Submission on discussion document: *Options for establishing a consumer data right in New Zealand*

Your name and organisation

Name	Josh Daniell | Carlos Chambers
Organisation	ākahu | Common Ledger

Background

ākahu and Common Ledger believe in the merits of data rights for New Zealand consumers. We see CDR as the optimal legislative vehicle to enable the potential benefits, and this joint submission outlines our shared views.

ākahu

ākahu is a consumer data sharing platform which is focussed on serving the New Zealand market. We build and maintain data integrations with bank, kiwisaver, investment, utility, and telco providers. We bundle those integrations into a SaaS product for developers.

For consumers: The purpose of ākahu is closely aligned with the objectives of CDR. ākahu puts consumers in control of their personal data. We make it simple for a NZ consumer to access the data that organisations hold about them, and to share that data with trusted third parties of their choice.

For data recipients: Using kahu integrations, a data recipient can enable its consumers to seamlessly share their data held by other organisations. Consumers can choose to share their identity, usage, balance, and transaction data. They can also initiate payments directly from the data recipient's app. No one else provides this depth of consumer data sharing functionality in New Zealand.

Common Ledger

Common Ledger is a business data sharing and insights platform which is focussed on serving the New Zealand and Australian markets. We build and maintain integrations with accounting and accounting software providers, banks, credit bureau providers, and some government agencies.

For (business) consumers: The purpose of Common Ledger is closely aligned with the objectives of CDR. Common Ledger puts business owners in control of their data. We make it simple for business owners to access data that organisations hold about them, and to share that data with trusted third parties of their choice - including advisors and lenders. Business owners can choose to share their entity's identity, usage, balance, journal data (categorised accounting data), reports, and accounting behavioural data. We also use this data to provide simple, understandable insights to business owners and their advisors, enabling them to make smart, timely decisions, and simplify and improve the accounting and loan application processes.

For data recipients: Our data recipients include accountants and advisors. Using Common Ledger's integrations, a data recipient can enable its business consumers to share their data held by other organisations.

Common Ledger is engaged in ākahu's data recipient accreditation process, and plans to use ākahu's integrations to fill gaps where consumer data is required for business consumer use cases.

Responses to discussion document questions

Does New Zealand need a consumer data right?	
1	*Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?*
	Key problems have been accurately identified, and we add one more below. **Traditional methods for consumers to access their data** We note MBIE's comment around traditional methods of enabling a consumer to access their data. These methods commonly include non-sanctioned "screen scraping" of a provider's web app, and non-sanctioned use of a provider's mobile APIs. These practices are widely used by banks, brokers, accounting software providers, fintechs, and payment providers. For example, in markets where Xero does not have direct integrations with banks or a regulated framework to adequately access bank data, a Xero customer can choose to share their bank transaction data with Xero via these traditional methods. While a well-designed and mature CDR framework is preferable to traditional methods, some large markets like the US have a flourishing range of consumer products like Venmo, PayPal, and TransferWise that rely on these traditional methods. As discussed throughout the development of CDR in Australia, there is no evidence of consumer harm from traditional methods and they have proven themselves to be functional solutions for over a decade. These traditional methods should be allowed to continue, at least until a CDR framework is mature and able to deliver better access to data without undue barriers or limitations. Traditional methods of data access help to achieve the objectives of the proposed CDR regime. Any restrictions on traditional methods would lead to poorer immediate consumer outcomes. Explicitly acknowledging the use of traditional methods in NZ, and encouraging data holders to refrain from attempting to block these methods, will provide the opportunity to start working towards the objectives of CDR while the proposed legislative framework is developed and reaches a mature state. This would help to allay a current problem with data portability in NZ, which is the threat that data holders could attempt to block the existing traditional methods, or stoke concern with their customers around the use of such methods.

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?*
	Yes we broadly agree, with one addition below. **Monopolies and competition in NZ** NZ is a small, isolated market, with natural monopolies and less competition than larger, more connected markets. While NZ has a strong history of regulation of natural monopolies, new tech business models are harder to regulate. CDR would provide a powerful regulatory environment and tool to reduce the likelihood and risks of negative impacts of these natural monopolies. In designated sectors, CDR can encourage innovation and competition, and empower consumers with visibility, choice, and control. Compared to the large, lumpy cost and ambulance at the bottom of the cliff approach of regulatory intervention, CDR would be a more proactive, iterative, and less expensive method of addressing competition concerns. Relative to the binary decision of “regulate”, or “do not regulate”, CDR provides an appropriate mechanism for the current era.
3	*Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?*
	Where work is underway, and sector-specific thinking on data portability is already advanced, consideration should be given to how that work can be folded into the CDR regime to avoid losing momentum, duplication, and wastage of resources.
4	*What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?*
	CDR should codify the idea that a consumer has on-demand access to, and control of, their customer data in designated sectors. This principle should be independent of the type of entity. The scope of consumers should be broad and enshrined as all legal entities in the primary legislation. We acknowledge that there may be an increased cost to data holders in managing authentication, consent, and permissions for more complex customers. This increased cost should be addressed through carefully defining "CDR data" for each designated sector, and/or by phasing the introduction of complex customers into a designated sector. Complexity of managing consent is a topic that many data holders are already required to address through other legislative obligations like AML/CFT, and shouldn't be a barrier that prevents complex entities from enjoying the benefits of consumer data rights.
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’)?*
	Identity data Consumer identity data should be included (if not already implicitly included within the proposed scope). At a minimum, this should include any name, date of birth, and address

	data which is held by a data holder. The inclusion of identity data is aligned with the Privacy Act principle that individuals should have access to their personal information. Identity data supports numerous CDR use cases. For example, the portability of identity data would enable faster onboarding to a new provider, and faster and cheaper compliance processes in relation to AML/CFT obligations. **Avoid an incentive to cram for the test** If the CDR regime is successful in promoting competition through mandated access to "product data", it's likely that consumers will use comparison products to facilitate the ongoing selection of appropriate products. CDR data would be used to populate comparison products, so data holders would be incentivised to evolve their products in a way that improves their ranking in that specific context. While this is likely to lead to positive outcomes in the short term, there is a risk of unintended consequences. For example, a data holder may not be incentivised to innovate in areas that are excluded from the definition of CDR data, and are therefore less visible to consumers through comparison products. MBIE should carefully consider the definition of CDR product data in order to decrease the risk of unintended negative consequences. In particular, the scope of CDR product data, and any standards around product data, should retain a level of flexibility in order to avoid stifling innovation.
6	*What would the costs and benefits be of including both read access and write access in a consumer data right?*
	Write access supports numerous CDR use cases. For example, faster switching between products, opening and closing accounts with providers, and cheaper payments. It's critical for write access to be included in the CDR regime.
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?*
	We broadly agree with the proposed outcomes.
8	*Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?*
	We broadly agree with the criteria.
9	*Do you have any comments on the discussion of Option one: Status quo?*
	None.
10	*Do you have any comments on the discussion of Option two: A sectoral-designation process?*
	We agree that option 2 is optimal.

11	*Do you have any comments on the discussion of Option three: An economy-wide consumer data right?*
	None.
12	*Do you have any comments on the discussion of Option four: Sector-specific approach?*
	None.
13	*This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?*
	None.
14	*Do you have any comments on our initial analysis of the four options against our assessment criteria?*
	We broadly agree with the analysis.
15	*Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?*
	Yes we agree.
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?*
	Data standards MBIE should avoid allocating significant resources to the process of developing highly specific data standards. The most important part of the designation process will be defining "data holders" and "CDR data" for each sector. That will enable participants to understand the scope of data that will be unlocked, and work can begin towards the objectives of CDR in that sector. It is less important to include rigid standards specifying the format of CDR data. Data recipients are typically able to receive data in slightly different formats and still derive significant value so long as the data is accurate, documented, and the full scope of data is exposed by each data holder. Data recipients will always need to process data to some extent before it is utilised or made available to consumers. Rigid data standards would require more time to develop by policy makers, and require more time and cost for data holders to meet those rigid standards, with little value for other CDR participants. It is also likely that rigid standards would become outdated as products evolve. For example, a new feature of an insurance product could become desirable for consumers, but if it's excluded from rigid data standards, then it may be less visible to consumers.

17	*Do you have any feedback on our discussion of any of these key elements?*
	None.
18	*Are there any areas where you think that more detail should be included in primary legislation?*
	Making CDR the framework of choice over time MBIE should aim to make CDR the obvious choice for use cases that require consumer data portability. To achieve this, CDR will need to be more appealing than traditional methods of consumer data access that exist in the absence of CDR. So CDR will need to deliver better access to data, while ensuring that any potential barriers such as accreditation, pricing, reciprocity, and liability are right-sized. If CDR gets these settings right, participants will naturally migrate to the CDR framework as it rolls out and matures. If CDR does not get these settings right, we will end up with two separate consumer data portability environments over the long term. We consider that much of the detail of CDR should be contained at the designation level in order to establish a flexible and responsive regime. However, to the extent that the right-sizing of key components is appropriate in primary legislation, they should be addressed in primary legislation. If these key components such as accreditation, pricing, reciprocity, and liability are addressed appropriately in primary legislation, stakeholders will have more time and certainty to begin work towards the objectives of CDR. **Intermediaries** Data recipients have the choice of building and maintaining data integrations themselves, or outsourcing that part of their products to intermediaries. Most data recipients choose to use intermediaries. Intermediaries will help the CDR regime to flourish in a number of ways: ● Intermediaries specialise in building and maintaining integrations with data holders. The ability to outsource reduces the technical barrier for data recipients to utilise consumer data portability in their products. This is similar to the ability to outsource data storage and data processing to cloud providers. ● Intermediaries can spread the costs of accreditation, as well as the significant costs involved in building and maintaining a broad range of data integrations, so that data recipients have a cost-effective method of accessing CDR data. ● The cost of accessing CDR data will become commoditised over time, so intermediaries will be incentivised to carry out value-adding work of cleaning data, enriching data, categorising data, and delivering enhanced data to recipients and their consumers. The role of intermediaries should be explicitly enabled (or not restricted) through primary legislation, and considered when designing CDR components such as accreditation.

Non-accredited data recipients

MBIE should consider whether any elements of the CDR regime will apply to a non-accredited data recipient. For example, if an accredited intermediary retrieves CDR data from a data holder and sends that data (with the consumer's consent) to a non-accredited data recipient, it's important for all stakeholders to know whether any components of the CDR regime such as accreditation and liability will apply.

We consider that the objectives of CDR will be frustrated if any data recipient that comes into possession of CDR data is subject to the CDR regime. For example, if a consumer provides a cloud accounting provider with consent to access their CDR data from a bank, and then exports that data from the cloud accounting provider and delivers it to their accountant, it would be inappropriate for the accountant to be subject to the CDR regime.

In addition, if specific obligations remain attached to CDR data, that data may need to be siloed from other data, which would be operationally difficult and unnecessary.

MBIE should exclude non-accredited data recipients from the CDR regime, unless and until there is a clear rationale to extend specific elements of the regime.

Consumer consent and authentication

Primary legislation or designation rules should set minimum requirements for consumer consent and authentication to ensure an appropriate minimum standard, and to set a level playing field for participants.

Consumer control

Consumers should have visibility over any enduring consent that they have provided, and the ability to revoke any enduring consent.

Expiry of enduring consent

MBIE should consider setting a default expiry on any enduring consent provided by a consumer, with potential exceptions where:

- The consumer continues to actively use the product.
- Data accessed through the enduring consent is both necessary for the product and transparent to the consumer.

Bilateral agreements

If a data holder is able to require a bilateral agreement with a data recipient, the objectives of the CDR regime are likely to be frustrated. For example if bilateral contracts were allowed, they could delay a standardised regulatory liability regime from bedding in, and cause confusion for consumers if there were effectively two liability regimes.

MBIE should use regulation to address the key elements that would otherwise be included in a bilateral agreement (such as pricing, access, and liability).

Reciprocity

We don't consider that a rule of reciprocity is appropriate. For example:

- If a consumer provides an intermediary with consent to access their bank transaction data and provide it to a cloud accounting provider, it would be inappropriate for the intermediary to be deemed to be a data holder in relation to that bank transaction data.
- If a consumer provides a cloud accounting provider with consent to access their bank transaction data, and then exports that data from the cloud accounting provider and sends it to their accountant, it would be inappropriate for the accountant to be deemed to be a data holder.

Rather than a rule regarding reciprocity, we think that designation is the appropriate tool to ensure equitable rights regarding consumer data. If the definitions of "data holder" and "CDR data" are well-designed for each sector, the designation rules will rightly catch a data recipient that is offering a product that is subject to that designation. For example, if Xero allows its customers to share their bank data with Xero, that should not trigger Xero to become a data holder for the purposes of the CDR regime. However, if Xero decides to offer a financial product that is in-scope for a designated sector, such as an invoice financing product for businesses, Xero would then become a data holder under the banking sector designation for the purposes of the CDR regime.

To help encourage uptake of the CDR regime, the rules should allow for non-designated entities to voluntarily operate within appropriate elements of the CDR regime.

Pricing

It should be free for consumers to access CDR data (and to enable a third party to act as their agent in this regard).

- Individuals already have a right to access data that is subject to the Privacy Act for free. API services should be a more efficient way to comply with these access rights once they are set up (because each request can be served electronically).
- If there was a fee, that cost would have to be worn (in some way) by consumers, which would make it more difficult to achieve the objectives of CDR.
- If some data holders charge more than others, it could lead to data gaps for products that are built on top of CDR data.
- If CDR data is subject to fees, data recipients may be incentivised to use cheaper traditional methods of data access.

These principles regarding pricing should also apply to any government agencies that fall within a designated sector.

Accreditation

	We consider an accreditation regime to be an appropriate mechanism to set minimum standards for direct participants in the CDR regime. To ensure that accreditation does not create an undue barrier, it's critical that the costs and timeframes associated with accreditation are right-sized. ākahu's accreditation process has been designed with this balance in mind. As a point of reference, here's a link to ākahu's accreditation process, including the policies that a data receiver must comply with.
19	*How could a consumer data right be designed to protect the interests of vulnerable consumers?*
	We are happy with how this question has been covered in other submissions that we have reviewed.
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?*
	No comment.
21	*How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?*
	We are happy with how this question has been covered in other submissions that we have reviewed.
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?*
	We should pay attention to the development of regimes in other jurisdictions and align where appropriate, but compatibility should not be a priority.
23	*Do you have any comments on where a consumer data right would best sit in legislation?*
	CDR should sit in a new piece of legislation.
24	*Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?*
	We have considered, but do not yet have a strong view on this question.
25	*What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?*
	We have a preference for a single regulator. This should not prevent other regulatory bodies from having involvement or responsibility for elements of the CDR regime. However we should strive for simplicity and clarity, and this is best achieved with a single regulator that can build up the required capabilities.
26	*If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?*

A well-designed CDR regime will help to create an appropriate environment for consumer data access to realise the potential benefits described by MBIE. However regulations will not deliver those outcomes on their own. These outcomes will be unlocked through experiences that deliver real value to consumers. It will take time to build, test, iterate, and scale these experiences. In the short to medium term, effectiveness of the CDR regime should consider the extent to which data recipients (and potential data recipients) agree that the regulations enable an appropriate environment for the potential value to be unlocked.

In a similar vein, we note that many stakeholders support the idea of government-led consumer education around CDR. While the proposed education is well-intentioned, we consider that most consumers will not care about CDR until great experiences are available and they can see the value for themselves. Time and patience will be required for the regulations to bed in, and great consumer experiences to be built.