evel 4 & 5,
11 York Street, Sydney
NSW 2000, Au tralia

12 October 2018

To the Australian Competition & Consumer Commission (ACCC):

Reference: Consumer data right

We write to you on behalf of Moneytree Financial Technology Pty Ltd in relation to the ACCC's consultation for the proposed Rules Framework supporting Australia's Consumer Data Right (CDR) and its initial application to the banking industry (Open Banking).

Background on Moneytree

Moneytree is a financial data portability platform, operating in Japan since 2013 and in Australia since 2017. Our goal is to bring financial institutions and their customers closer together, enhance the digital banking experience, and improve visibility and transparency for customers via:

1. an API service for enterprises to obtain consensual access to customer data profiles,
2. a personal financial management mobile application for individuals, and
3. an expense tracking tool for small and medium-sized businesses.

Moneytree counts Japan's three megabanks and numerous regional banks among its clients and investors.

Our company submitted comments for the two consultation periods on Open Banking, between August and September 2017, and between February and March 2018; and for the 'Treasury Laws Amendment (Consumer Data Right) Bill 2018,' which was open for commentary between August and September 2018.

Moneytree Founder, Executive Director for Australia and Chief Technology Officer Ross Sharrott serves on the Advisory Committee for the Data Standards Body.

Comments

Our comments are submitted in three sections:

1. Rules we support and strongly recommend are maintained in the final Rules Framework;
2. Rules worth revising, including our suggested alternatives where possible
3. Rules requiring further clarification.

1. Rules we support

We highly commend the following rules proposed by the ACCC:

2.3 Sharing must not attract a fee (page 13)
... The ACCC proposes that in the first version of the rules, the sharing of the data outlined in the Open Banking review not be subject to fees...

Moneytree believes this is the right approach for the CDR to be successfully adopted in the banking industry, as the alternative (data holders charging a fee to data recipients) may deter the latter from participating in Open Banking due to the costs they would have to incur.

3. CDR consumer – who may take advantage of the CDR? (page 14)
... The CDR will therefore be available to both individuals and other entities, such as businesses and trusts ...

We support the idea that businesses (particularly smaller ones) and trusts should be able to take full advantage of Open Banking.

5.2. Derived data (page 18)
The Open Banking review recommended that data that re ult from 'material enhancement by the application of in ight , analy i or tran formation by the data holder' hould not be within cope of Open Banking The draft legislation provides that 'CDR data' can include data that is 'directly or indirectly derived' from underlying CDR data. The ACCC understands that the purpose of this inclusion is twofold: ● to en ure that the privacy afeguard and other protection continue to apply to data that ha been derived from the 'underlying' CDR data, and ● to provide scope for transformed or value-added data to fall within the CDR regime. The ACCC accept that the term 'tran formed' or 'value added' can encompa a pectrum of activitie , from imple tran formation of data (for in tance, imple arithmetic or collation)

through to sophisticated analysis. The proposed rules relating to data sets set out in the following sections seek to ensure that the data sets recommended by the Open Banking review are within scope, recognising that these data sets may include derived data, though not data that results from 'material enhancement' as contemplated by the Open Banking review.

We support the principle of not including data derived data through 'material enhancement' should be excluded from scope.

5.4. Reciprocity (page 21)

...The Consumer Data Right Booklet endorsed reciprocity as a principle, noting that the exact detail of reciprocity is yet to be settled and will be subject to further consultation. The Consumer Data Right Booklet also noted that the enabling legislation would incorporate a principle of reciprocity, allowing the ACCC to make rules regarding implementation, including rules regarding the timing of when accredited data recipients would become subject to reciprocity requirements...

...**The ACCC does not understand the principle of reciprocity to mean that a data holder is entitled to request or obtain data from an accredited data recipient before sharing data it has been directed to share by a CDR consumer. Reciprocity is not a 'quid pro quo' arrangement between data holders and accredited data recipients.** The CDR regime is consumer focused, and any approach to reciprocity would need to be based on a consumer directing and consenting to an accredited data recipient sharing their data.

In the ACCC's view the concept of reciprocity raises complex issues requiring further consideration. The ACCC therefore does not propose to make any rules regarding reciprocity in the first version of the rules.

We agree with the position that data holders should not be entitled to request or obtain data from accredited data recipients for free, as this would work against the CDR's objective to promote data-driven innovation (page 9 of the proposed Rules Framework).

As described in our second submission to the Treasury in March 2018 (link), as part of the 'Review into Open Banking in Australia – Final Report,' we believe the principle of reciprocity is generally fair as applied to the exchange of non-value-added data (produced by data holders).

This means that, if accredited data recipients are providing bank-like services (e.g. providing any of the payments, deposit or lending products within the scope which data holders normally

provide), they too should be required to make available the non-value added data generated by those services to other CDR participants.

Several significant issues arise from requiring accredited data recipients to share, on a quid pro quo basis, non-value added data they have previously received from a data holder. These include:

a) Accredited data recipients would incur a high operational burden, especially non-ADIs, as the on-sharing of data from data holders would force them to duplicate the APIs of CDR participants providing them with that original data. This would add significant cost and operational complexity for all CDR participants, and divert significant resources away from innovation toward compliance.

b) CDR participants would be forced to assume potential legal liability for data they have received but did not create. In addition to the burden of having to provide duplicate APIs to on-share information from data holders, CDR participants would have to assume liability for the accuracy of data they did not originally create, and which they may not have any way of verifying (i.e. where they received data from a participant other than the original source, there may be no way to compare it against "the source of truth").

c) Given the greater costs and risks outlined in (a) and (b) above, there would be hesitation to participate, especially among Fintech companies. Given the added overhead arising from this interpretation of reciprocity, participants would be incentivised to side step Open Banking, perhaps favouring other channels with less burdensome rules for participation (e.g. bilateral agreements).

d) Data integrity and trust in the system could be severely compromised over time. As the same data passes from one participant to another, there is an increasing risk of data integrity errors. This can occur due to software bugs, data transformation processes, or the peculiarities of different database systems. The more times data is shared by a participant who is not "the source of truth", the greater the risk of errors being introduced. In the event of legal or regulatory action, unwinding the chain of custody to determine liability would, at best, be costly and time-consuming, and at worst would be impossible (e.g. if participants in the chain of custody were no longer operational).

e) ADI's core banking systems are designed to hold internal data, and have no facility to store raw data received from other ADIs. Core banking systems used by ADIs are generally not designed to store the raw data conceived under Open Banking. In order to satisfy the above interpretation of reciprocity, ADIs will have to purchase or

upgrade information systems in order to support storing raw data received from third parties. Their holding of this data would be subject to equivalent duties of care and compliance obligations, making the true costs of Open Banking much higher than intended. Additionally, the issues identified in (a), (c) and (d) above would adversely apply to ADIs too.

8.1.1. Joint accounts and complex authorisations (page 33)

The Open Banking review con idered joint account , where more than one per on i the relevant CDR con umer **The Open Banking review recommended that authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from that account**

The ACCC notes that while this proposal may address issues with simple joint accounts, it may not necessarily resolve all issues for accounts that allow multiple parties to view and/or transact on the account, or that otherwise entail complex account arrangements.

Further, the ACCC is conscious of particular risks that can arise in relation to vulnerable consumers, including those at risk of financial or other exploitation by other account holders.

The ACCC proposes to make rules to the effect that where consumers with a joint account hold individual authority to transact on that account (that is, they do not require the consent of the other joint account holder(s) to transact), they will be able to apply for the CDR data in their joint accounts.

The rules may require that each joint account holder is notified of any data transfer arrangements initiated on their accounts, consistent with privacy safeguard 5 (see section 13), and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

We support this principle, in line with the recommendations of the Open Banking review and the ACCC's suggestion.

8.3.1. Nature of the consent to be provided (page 37)

Consent should be specific as to use

… In addition, the ACCC proposes to make a rule that accredited data recipients should only seek consent to access the minimum data necessary for the uses agreed to. This will help ensure consent is specific as to purpose, and that consent is express and informed…

This is in line with one of the key principles of 'Privacy by Design' which the GDPR (General Data Protection Regulation) is based on, and has become the emerging global standard for the responsible handling of personal information. We strongly support this proposed rule.

12.1. Disclosure of consumer data to other parties (pages 48 51)

...the ACCC also recognises that there may be legitimate reasons for data to be disclosed to non-accredited entities, and that by doing so the security, practicality and utility of the CDR to consumers may be increased. Certain applications of CDR data may depend on the ability to disclose to non-accredited entities, and if the CDR regime does not allow this to occur these applications will be unavailable to consumers, limiting the value of the CDR. A prohibition on disclosure of data to other entities is also at odds with the CDR's strong focus on consumer choice and freedom...

We support the idea of accredited data recipients sharing data with non-accredited entities at the request of customers, in line with the CDR's focus on creating consumer benefit. accredited data recipients

12.1.3. To an intermediary through whom the data passes on its way to the data recipient (page 51)

The ACCC under tand that one propo ed alternative model for the operation of a CDR arrangement i u e of an intermediary For e ample, an accredited data recipient may offer it ervice to and directly interact with it con umer but rely on an intermediary to directly receive CDR data in the fir t in tance, that i , the intermediary would be the entity calling the API and receiving data from the data holder

While the second scenario above in section 12.1.2 involves an accredited data recipient directly receiving CDR data by calling the API then outsourcing parts of its service to its own outsourced providers, the intermediary model relies on an intermediary, while not necessarily interacting with the customer directly, receiving CDR data and passing it (or a subset of it) on to the accredited data recipient. This could, to the extent that a tiered system of accreditation is ultimately adopted (see section 6), allow smaller accredited data recipients to qualify for a lower level of accreditation by relying on the stronger security and privacy protections provided by an intermediary accredited to a higher level.

As an intermediary would directly participate in the disclosure process flow it would need to be accredited should this model be provided for in the rules. Without accreditation an intermediary would not be listed in the Register and would therefore not be able to access a data holder's API. These technicalities notwithstanding, **the ACCC considers it appropriate**

that the primary collector of a consumer's CDR data be accredited in every case.

Like in cenario two, the CDR protection would continue to apply and the con umer' data will not 'leave' the CDR y tem, a the intermediary and the accredited data recipient would both be accredited entitie ubject to CDR obligation Thi model may al o allow for CDR data to be proce ed within the environment of the intermediary, and for the accredited data recipient to obtain in ight from the data without ever ' eeing' or toring the data In uch a ituation it may be appropriate for the accredited data recipient to hold a lower level of accreditation

This is a complex issue which would have significant impacts on the consent, authorisation and authentication processes in particular, and would require careful development as part of the standards-setting process. The ACCC welcomes stakeholder comment on this issue, to assist in determining to what extent the utility of the CDR would be limited without the ability to operate in this way. The Open Banking review and government response both clearly emphasised that the CDR should be flexible enough to allow the development of alternative business models, and the ACCC supports this to the extent that it does not significantly impact on the security or privacy of consumers' data.

For reasons of protecting the privacy and security of consumers, and also in order to earn consumer trust in Open Banking, we strongly agree with the ACCC's suggestion that intermediaries should require to be accredited as CDRs.

2. Rules worth revising

5.3.2. Transaction data (page 19 20)

...The ACCC proposes to make rules to the effect that transaction data include, at a minimum:

- the opening and closing balance of an account for the period specified
- the date on which a transaction was made
- the relevant identifier for the counter-party to a transaction
- the amount debited or credited pursuant to the transaction
- the balance on the account prior to and following a transaction
- any description in relation to the transaction, whether entered by the consumer or the data holder
- any identifier or categorisation of the transaction by the data holder (that is, debit,
- credit, fee, interest, etc.).

...The ACCC is considering whether the metadata associated with each transaction should be

included as part of the transaction data to be shared in the first version of the rules. 'Metadata' is data about data, and in relation to transactions could include information such as geolocation data on where a transaction occurred, or the time when a transaction took place. The ACCC welcomes submissions from stakeholders on what metadata could be within scope, what benefits to consumers it could deliver if it was in scope and what risks would arise and need to be managed...

We agree with the definition of transaction data proposed by the ACCC in proposal 5.3.2.

Regarding the que tion of metadata, we upport the inclu ion of information uch a the time and geolocation of tran action , a well a highly relevant and related data uch a intere t rate , foreign currency tran action amount from over ea purcha e and product maturity date Accredited data recipient can u e thi metadata to improve tran action categori ation, merchant identification, provide u eful alert and other feature to the con umer In turn, thi enable a greater range of new feature & ervice that can benefit con umer

6.2. Proposed rules for accreditation model and criteria (page 24 - 26)

In the first version of the rules, the ACCC proposes to provide for a general tier of accreditation that will entitle an accredited data recipient to receive and hold any type of CDR data in scope for Open Banking, subject to compliance with the draft legislation, the rules, and the standards. The accreditation criteria relating to this general tier of accreditation, and the ongoing obligations of accredited recipients, are discussed in the sections below.

The ACCC al o upport the development of lower tier of accreditation in the fir t ver ion of the rule , to the e tent that thi can be implemented from 1 July 2019 Lower tier of accreditation may limit acce to particular type of CDR data (or have other re triction) and have reduced requirement for accreditation For e ample, the intermediary model (ee 12 1 3) i a cenario where it may be appropriate for the rule to provide for a lower level of accreditation for entitie that will not collect CDR data but will be able to acce and u e ub et of CDR data or in ight from CDR data collected by an intermediary to provide ervice to con umer The ACCC welcome the view of takeholder about thi i ue and the type of lower tier that would be u eful and practical to implement, having regard to e i ting bu ine model and likely u e ca e for CDR data The ACCC eek view about the ba i on which lower tier could be re tricted and the way in which the e limitation would reduce ri k relating to the collection, torage or u e of CDR data and therefore provide a ba i for reduced accreditation requirement

6.2.1. Criteria for general level of accreditation

The ACCC considers that the criteria for accreditation should be objective, to the extent possible, related to the security and integrity of the CDR regime and primarily directed towards ensuring that applicants demonstrate their capacity to manage CDR data in accordance with the privacy safeguards. In developing the proposed criteria for accreditation, as noted above, the ACCC has had particular regard to the requirements for registration as an AISP in the UK, and the requirements to be met by ADIs, in relation to risk management and the applicant's history of compliance with relevant laws. The ACCC also recognises that an objective of the CDR regime is to encourage data-driven innovation and that an appropriate balance needs to be struck to ensure that the criteria for accreditation do not impose unnecessary barriers to entry. The ACCC seeks the views about the practical implications of the proposed criteria for general accreditation in this context.

The proposed criteria for accreditation assume that in most cases an applicant will be a corporation. However, the ACCC acknowledges that individuals and other legal entities may apply for accreditation and proposes to accommodate this in the first version of the rules.

The ACCC proposes to make rules that the Data Recipient Accreditor grant accreditation to an applicant to be a 'data recipient' of CDR data if the Data Recipient Accreditor is satisfied that:

1. The applicant is a 'fit and proper' person to receive CDR data. Relevant information that will need to be provided with an application, and which may be taken into account by the Data Recipient Accreditor for the purposes of this assessment, is expected to include:

    - whether the applicant (or its directors) has been charged with or convicted of a serious criminal offence, or an offence of dishonesty, against a law of the Commonwealth or of a State or Territory
    - whether the applicant (or its directors) has been found to have contravened, or civil proceedings have been commenced against the applicant alleging contravention of, a law relevant to the management of CDR data including the Competition and Consumer Act 2010 (Cth) (CCA) (including the Australian Consumer Law), the Australian Securities and Investment Commission Act 2001 (Cth) (ASIC Act) and the Privacy Act 1998 (Cth) (Privacy Act)
    - whether any directors of the applicant have been disqualified from managing corporations
    - whether the applicant or its directors has a history of bankruptcy or insolvency

- any other relevant matter.

2. The applicant has appropriate and proportionate systems, resources and procedures in place to comply with the legislation, the rules and the standards, including in relation to the management of risks relating to CDR data in compliance with the privacy safeguards. As noted at section 6.9, the ACCC seeks stakeholder views on certification against industry standards that may be appropriate to recognise in the rules as evidence of this criterion in the accreditation process. The applicant will need to provide:

- a business plan, including a detailed description of the services the applicant intends to provide to consumers using CDR data and examples of the relevant consent screens
- evidence of the applicant's internal control mechanisms, including:
    - if applicable, the details of outsourced activities relating to CDR data (see section 6.8 below) and of the policies and procedures in place to manage those arrangements
    - information about business continuity arrangements, including clear identification of critical operations, effective contingency plans, and procedures for testing and reviewing of the adequacy of such plans
- evidence of the applicant's risk management processes, including:
    - effective procedures to identify, manage and monitor any risks to which it might be exposed with respect to CDR data
    - adequate procedures and processes to comply with the privacy safeguards including a copy of the policy about the management of CDR data required by privacy safeguard 1
    - the applicant's procedures for monitoring, handling, and following up security incidents and security-related customer complaints
    - the applicant's measures and tools for the prevention of fraud and illegal use of CDR data
    - descriptions of security control and mitigation measures and procedures for the mandatory reporting of incidents, and notification processes to consumers in the event of a security incident.

> 3. The applicant's internal dispute resolution processes meet the requirements specified in the rules and the applicant is a member of an external dispute resolution body recognised by the ACCC (see section 15)...

For accreditation purposes, we believe the "appropriate and proportionate systems, resources and procedures in place to comply with the legislation, the rules and the standards, including in relation to the management of risks relating to CDR data in compliance with the privacy safeguards" mentioned in the draft rules should be accredited by an independent auditor.

In many industries, there are existing security standards reviewed by external auditors that certify acceptable governance and best practices. Recognition of acceptable standards by external auditors will make CDR compliance easier for data recipients to understand and prepare for, and also reduces the operational burden on the ACCC in auditing and accreditation. Furthermore, this will reduce the cost of participation for recipients who have already invested in the security and audit required to achieve such standards and avoid creating unnecessary barriers to entry, such as long lead times for receiving accreditation.

We recommend that SOC 2 or ISO 27001 certifications be accepted as equivalent to, or better than, the proposed standards for full CDR accreditation.

We also recommend these highly known and accepted standards for full accreditation of data recipients should also satisfy any lower tiers of accreditation that might be established by the ACCC (i.e. accreditations should ladder down, so that higher levels of accreditation encompass all the levels *below* them). This was not explicit in the draft rules.

8.3. Consent provided to accredited data recipients (page 34)

> The ACCC proposes to make rules to the effect that an accredited data recipient must obtain a consumer's consent to collecting and making use of specified data, for specified purposes and for a specified time. A consumer will be able to specify and/or limit their consent to the scope of the data provided (including the types of data and the period of time covered by the data), the uses to which the data is put, **and the duration of time over which the data is made available and held**.

The proposed rule described here treats as one and the same the consumer's consent for an accredited data recipient to access their data, and the consent provided to hold retrieved data. This could lead to undesirable situations where accredited data recipients must delete historical

data simply if a consumer is less than proactive in updating their consent, or where consent is revoked due to closing an account, regardless of the consumer's actual intent. In a very broad range of use cases (e.g. accounting, personal financial management, credit scoring, etc) consumers may want accredited data recipients to hold historical data for an extended or indefinite period. We strongly recommend clarifying this point to avoid undesirable consequences.

8.3.1. Nature of the consent to to be provided (page 37)	**9.5 Duration of authorisation (page 43-44)**
Con ent hould be time limited… ...In relation to the second i ue, the ACCC propo e to make a rule that would limit the period of authori ation provided to data holders to **90 days**	The ACCC propo e to make rule to the effect that con umer may grant authori ation for a pecific, one off reque t, or may grant authori ation that per i t over time In term of per i ting authori ation , the ACCC propo e to make a rule that will limit the period of authori ation to 90 day , con i tent with EU requirement under the PSD2 that al o limit the period of authori ation to **90 days** The ACCC propo e to make a rule that re authori ation will then be required if the accredited data recipient eek continuing acce to the con umer' data The re authori ation may be a implified ver ion of the proce initially undertaken to authori e the data holder to hare the data (while till requiring trong con umer authentication) Again, the ACCC' e pectation i that the re authori ation proce hould not add undue friction to the u er e perience Re authori ation proce e hould therefore be included in the authori ation tandard , which participant mu t comply with Tho e tandard would al o be ubject to u er te ting a outlined previou ly

We believe a ma imum authori ation period of 90 day i too hort for a broad range of u e ca e If a 90 day limit i maintained, con umer will be required to re authori e data acce four time a year acro multiple data holder and multiple ervice In ome u e ca e , con umer may not yet have reali ed the full benefit of a particular ervice before being required to "reconnect"

We ugge t a ma imum of three year , with guidance given to accredited data recipient that the reque ted duration mu t be appropriate to the nature of the ervice offered, and proportionate to the benefit conferred on the con umer

Reminders to consumers that an authorisation is current, can and should be sent with greater frequency than the authorisation period. For example, for a three-year authorisation, reminders should be sent at least once a year, and for shorter authorisation periods reminders should be sent at least halfway through the period, and in all cases at a reasonable time before expiry.

Mandating a short maximum expiry on authorisations, though it would reduce the incidence of "zombie" authorisations, will hamper the effectiveness of Open Banking in driving innovation, as it adds unexpected friction and complexity to a framework that is currently not well understood by consumers. For example, consumers' experience of Open Banking would be negatively affected if connected services frequently stop working and require them to re-authorise numerous services four times each year. As for accredited data recipients, services offering monitoring of accounts for accounting, audit or solvency verification purposes face significant detriment at best, and at worst this approach risks making these use cases entirely unfeasible.

Whatever authorisation duration is ultimately decided by the ACCC, the authorisation renewal process is critical to the success of Open Banking. If consumers must re-enter authentication information in order to extend an authorisation, as opposed to clicking a confirmation link in an email or on a website, a barrier to the adoption of Open Banking will have been created.

8.3.1. Nature of the consent to be provided (page 38)

Consent should be able to be easily withdrawn with near immediate effect

Central to providing consumers with control over their CDR data is the capacity for consumers to withdraw consent. The ACCC proposes to make a range of rules which will help provide consumers with a straightforward withdrawal process. The proposed rules include:

- a consumer may withdraw consent at any time without detriment
- the ability to withdraw consent will be no more complex than giving consent in the first place
- accredited data recipients must inform consumers how they can withdraw consent
- withdrawal of consent must be able to be effected via both the accredited data recipient and the data holder (where it is withdrawal of authorisation; see section 9.9)90
- if a consumer withdraws consent through the accredited data recipient, the accredited data recipient must notify the data holder and any intermediary. Similarly, if consent is

withdrawn via an intermediary, it must notify the data holder and the accredited data recipient

- if a consumer withdraws consent, the consumer's data becomes redundant, whether it is held directly by the data recipient or is being stored by a contractor, see discussion above and section 13.

We concur with the first four points about customers' consent.

We request clarification on the definition of "notify" in the fifth point. What form of notice is imagined here?

We strongly disagree with the final point that data is no longer useful or becomes "redundant" after a consent is withdrawn. Access to historical data can be useful for many reasons, such as in accounting systems. We also recommend a separate consent for holding historical data be included, with revocation of the holding consent made available in the proposed consumer dashboard (section 8.3.2).

8.3.2. Consumer dashboard (page 38-39)

The Open Banking review recommended that con umer be provided with the ability to acce a record of their data u age hi tory

The Government confirmed consumers should be able to keep track of their authorisations and that these records will themselves be designated data sets under the CDR. The draft explanatory materials envisages that:

> *'The consumer data rules require all banks to provide convenient online access to a dashboard displaying all of the permissions the CDR consumer has granted '*

The ACCC proposes to makes rules that will require all accredited data recipients to have a system in place which allows consumers to readily manage their consents. This should allow consumers to view what they have consented to and to readily withdraw those consents if they choose.

Specifically, accredited data recipient will be required to provide a con umer facing online interface or da hboard that how the con umer' current and hi toric con ent provided to accredited data recipient , including

- which datasets the consumer has provided consent to be collected and used

- when consent was obtained
- the period for which data was requested
- the purposes or uses for which consent was obtained
- the name of any intermediary
- when the accredited data recipient's access to the data will expire and the period for which the accredited data recipient will hold the data
- whether any consents have been revoked and, if so, when.

In the event a consumer deletes their account with an accredited data recipient, the requirement to store 'historic consents' may be problematic. Do accredited data recipients have an obligation to continue holding these records after deletion? If so, for how long, and how much identifiable data about the consumer should be retained? An obligation such as this could make it impossible to 'forget' a consumer who no longer wants to use a service or product offered by the data recipient.

We recommend the ACCC scope this rule to enable data recipients to forget former consumers if the consumer so wishes.

12.1.1. To a specified entity as directed by the consumer (pages 49 - 50) 1

The ACCC recognises that there will be instances where a consumer wishes to have their CDR data disclosed to a non-accredited entity. For example, a consumer might want to have their data disclosed to their accountant to assist in the preparation of their tax return. Such instances should be facilitated by the CDR regime, recognising that consumers should be free to direct that their own data be shared with non-accredited entities for specific purposes as they wish.

The ACCC proposes to make rules **requiring** accredited data recipients to transfer data to a non-accredited entity if directed by a consumer and with their specific express consent. This is a situation where CDR data has been shared by a data holder with an accredited recipient, and the consumer is now directing that accredited recipient to share the data with a non-accredited recipient. The ACCC is not proposing to make rules that would permit the sharing of CDR data from a data holder to a non-accredited recipient.

A the con umer i directing that their data be di clo ed to a non accredited entity, the con umer' data will leave the CDR y tem and the CDR protection will no longer apply The accredited data recipient i not liable for mi u e once the data i tran ferred The CDR protection will not apply, however the Privacy Act and the APP may apply where applicable, although the Privacy Act will not apply to all third party recipient out ide the CDR y tem

A further rule would require that the accredited data recipient must notify the consumer that:

- the entity they are ending their data to i not accredited under the CDR and therefore the CDR protection no longer apply
- the non accredited entity' handling of their data may be covered by the Privacy Act
- di clo ure i at the con umer' own ri k

Accredited data recipients being "required" to share CDR data with non-accredited parties is a potentially troubling definition because it implies data recipients would not be able to charge for this service to companies outside of Open Banking. Treasury's 'Review into Open Banking in Australia – Final Report' recognised there is value in holding data on behalf of consumers. Furthermore, there is a cost in becoming accredited, connecting to Open Banking APIs and storing data. Allowing all non-accredited parties free and unfettered access to Open Banking data stored by accredited data recipients would destroy many of the economic incentives for services focused on storing data on behalf of consumers. Moreover, it would encourage the widespread adoption of advertising-led business models that could seriously jeopardise the privacy of consumers and undermine many of the objectives of Open Banking. We suggest this phrase to be amended as follows:

> *The ACCC proposes to make rules **to allow** accredited data recipients to transfer data to a non accredited entity if directed by a consumer and with their specific e press consent*

3. Rules requiring further clarification

2. Sharing data with third party recipients (page 12)

The ACCC proposes to make rules to the effect that:

...

- data haring mu t only occur where the con umer ha given relevant informed con ent to the accredited data recipient and authori ation to the data holder

The above statement indicates that data sharing could only happen within the regime which is seemingly at odds with 12.1.1., which allows data sharing at the customer request with non-accredited parties outside of the CDR system. We suggest replacing with the following:

- Data sharing must only occur where the consumer has given relevant informed consent to the accredited or non-accredited data recipient and authorisation of the data holder.

Final words

It is our intention that these comments can help the ACCC determine the best set of rules for all participants of the CDR system as it applies to the banking sector and others in which the new the CDR will be exercised in the future.

We remain open to any follow up questions or discussions with the ACCC on any of the comments submitted in this document and more broadly.

Sincerely,

Mr Paul Chapman

Chief E ecutive Officer and co founder
Moneytree Financial Technology Pty Ltd

Mr Ross Sharrott

Chief Technology Officer and co founder
Moneytree Financial Technology Pty Ltd

Member of the Advisory Committee for the Data Standards Body in Australia