Levels 4 & 5,
11 York Street, Sydney
NSW 2000, Australia

Mr Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600
AUSTRALIA

Reference: Treasury Laws Amendment (Consumer Data Right) Bill 2018

Dear Mr McAuliffe,

We write to you on behalf of Moneytree Financial Technology Pty Ltd as part of the Australian Treasury's consultation for the Law Amendment Bill that will create the Consumer Data Right (CDR) in Australia.

Following our previous submissions to the Treasury in regards to the Open Banking and CDR (Sep-2017 and Mar-2018), we would like to reiterate our congratulations towards establishing an open data economy that is safe, private and transparent for consumers, and that allows for greater competition and innovation in the financial services industry, as well as the other industries in which the CDR will be implemented.

Having reviewed the documents for this current consultation, we have only a few observations. The most critical one is around **the reciprocity principle** contained in the Explanatory Materials of the bill.

On page 12 of the Explanatory Materials, point 1.46 considers the following:

> *1.46 When in possession of a consumer's CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants. This is known as the principle of reciprocity.*

While we were unable to find the amendment in the Exposure Draft that could be interpreted as above, having this in the Explanatory Materials is still problematic.

Below are our previous comments on this issue to the 'Review into Open Banking' lead by Mr Scott Farrell and published for consultation earlier this year.

The issue with the reciprocity principle, as considered in the Review into Open Banking:

One interpretation of these recommendations would make all participants of Open Banking **both data holders and data recipients**. As such, all participants would have to replicate the APIs of participants providing them with raw data so they can on-share this data (Recommendation 3.11). It is our view that this requirement is impractical in some respects and inapplicable in others. In particular, we have identified the following possible negative outcomes:

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

b) **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 raw data, participants would have to assume liability for the accuracy of data they did not originally create, and which they may not have any way to verify (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 incentivized to side step Open Banking, perhaps favoring 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.

In summary, we believe the challenges of duplicating raw data to on-share with other participants could jeopardise the Open Banking model, and heavily outweigh any potential benefits.

In regards to the Exposure Draft, our company has one comment on point **56AA** (page. 3), which states the following:

> The object of this Part is:
>
> (a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed:
> (i) to themselves; or
> (ii) to others in those sectors that they trust; and
> **(b) to enable any person to access any information in those sectors that does not relate to any identifiable, or reasonably identifiable, consumers; and**

(c) as a result of paragraphs (a) and (b), to create more choice and competition within those sectors.

We fully agree with the view that all financial data belongs to the customer and the customer should have the capability to retrieve them or to provide authorised secure access to this data. It is in this spirit that we suggest amending letter (b) in line of the following, instead:

(d) to enable any person to access any information in those sectors that does not relate to any identifiable, or reasonably identifiable, consumers, as long as the availability of the anonymised data has been previously disclosed with the data owners in a clear way; and

Beyond these written comments, our company remains open for further discussions with the Australian Treasury regarding any additional input it might need as part of this consultation.

Sincerely,

Mr Paul Chapman

Chief Executive 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