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

12 October 2018

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

Reference: Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking

We write to you on behalf of Moneytree Financial Technology Pty Ltd in relation to the Treasury's second stage consultation on Treasure Laws Amendment (Consumer Data Right) Bill 2018 and Designation Instrument for 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. a personal financial management mobile application for individuals;
2. an expense tracking tool for small and medium-sized businesses, and;
3. a standardised API of aggregated financial customer data for enterprises.

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. We've also submitted comments to the ACCC on the consultation of the draft rules for the implementation of the CDR, which closes today.

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

Comments

Our comment focuses on only one of the proposals considered in this second stage of review to the Treasury Laws Amendment (Consumer Data Right) Bill 2018: the proposal 3 on reciprocity.

Proposal 3: Reciprocity (page 7, CDR proposals for further consultation)

Submissions acknowledged that s56BC(1) of the exposure draft was capable of achieving the principle of reciprocity as stated in the Open Banking Review that

> 'entities participating in Open Banking as **data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking**, plus any data held by them that is transaction data or that is the equivalent of transaction data.'

However, many also expressed the view that the that the Bill could highlight the principle of reciprocity to a greater extent for the lay reader. Treasury is therefore seeking views on amended sections which try to highlight the principle of reciprocity and how it can operate:

- Reciprocity operates to allow the ACCC to write rules requiring data recipients to provide customers access to data, or the ability to request disclosure of data to accredited parties:
  - **Equivalent data – designed entity**: Data of a class within a designation instrument that an accredited recipient has generated or collected themselves, where the accredited recipient themselves falls within a designated class, but there is no rule requiring that accredited recipient to provide access to that designated data. An example of this would be that a rule could be written to require a small ADI to disclose banking information at a consumer's request before 1 July 2020, if the small ADI had received CDR data [***s56AG(3)***]; and/or
  - **Equivalent data – not designated entity**: Data of a class within a designation instrument that an accredited recipient has generated or collected themselves, where the accredited recipient themselves does not fall within a designated class. An example of this would be that a rule could be written to require a non-bank lender who is an accredited recipient to disclose lending information at a customer's request [***s56AG(3)***]; and/or
  - **Received data**: Data that recipients have received through the CDR [***s56BC(1)(a)***]
- Where reciprocity has the effect that an accredited recipient is required to provide customers the right to access equivalent data, they are able to be treated as a data holder for the purpose of the rules and Privacy Safeguards.

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.

However, 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.

In summary, we believe further clarification on reciprocity is required for the success of Open Banking to prevent confusion and additional high operational costs to all participants in the regime which work against the innovation that all participants and stakeholders are expected to introduce. We look forward to the ongoing consultation process with Treasury, ACCC and various stakeholders for the success of CDR implementation in Australia.

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