The Treasury
Langton Crescent
PARKES ACT 2600
March 2018
AUSTRALIA

Reference: Review into Open Banking in Australia – Final Report

22 March 2018

To the Treasurer,

We write to you on behalf of Moneytree Financial Technology Pty Ltd in relation to the 'Review into Open Banking in Australia – Final Report,' (the Report) released in February 2018 for public consultation, and to submit our comments on Open Banking policy and regulation in Australia.

Background on Moneytree

Moneytree is a financial data aggregation platform, operating in Japan since 2013 and in Australia since 2017. We aim to bring financial institutions and their customers closer together through a permission-based platform composed of three parts:

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 also submitted comments for the initial consultation period on Open Banking, between August and September 2017, which can be reviewed here.

Assessment of the Report

Upon review of the 50 recommendations contained in the Report, it is clear the views of all parties were deeply considered and weighed. We applaud this. Based on the Report, we believe the goal of establishing a fair, equitable, and representative regulatory Open Banking framework in Australia is well within grasp.

Nevertheless, it is our view that some of the recommendations in the Report in current form may lead to unintended negative consequences and should be carefully reconsidered.

From our direct experience with Open Banking in Japan (both as a contributor to policy and regulatory discussions, as well as a market participant) and with additional reference to the UK and EU models, we make the following comments from the perspective of ensuring the Australian market remains in step with emerging Open Banking global standards.

It is in this spirit that we submit seven comments for consideration.

Comments regarding specific recommendations from the Review

We highlight the following recommendations from the Report, and comment on what we believe should be amended.

Comment 1

Re. recommendation 2.5 – the Standards (p. 20-21)
The Standards should include transfer, **data**, and security standards. Allowing supplemental, non-binding, standards to develop (provided they do not interfere with interoperability) will encourage competitive standards-setting and innovation.

Setting standards for **transfer** and **security** is primarily a technical discussion and agreeing on these aspects is readily achievable.

However, the setting of **data standards** may add significant lead time to the introduction of Open Banking in Australia. On the other hand, with many diverse stakeholders involved, prioritising the introduction of data standards within a limited timeframe could lead to innovation gridlock, whereby participants are disincentivised to go against a monolithic data standard, and simultaneously left waiting for standards to be updated in order to meet emerging needs.

It is our view that the suggested list of specific products to be included in the scope of Open Banking (table 3.1 of the Report) suffices as a definition of shareable data.

Given these considerations, the most important role of the Standards Body would be to ensure that the agreed transfer and security standards keep pace with real world needs. In setting these standards, the Standards Body should give recourse to all use-cases and types of data currently used within industry.

In summary, we think the setting of comprehensively defined **data standards** is overly prescriptive and risks significantly considerably delaying the realisation of the benefits of Open Banking.

Comment 2

Re. recommendation 3.2 – transaction data (p. 37)
At a customer's (or former customer's) direction, data holders should be obliged to share all transaction data in a form that facilitates its transfer and use. The obligation should apply for the period that data holders are otherwise required to retain records under existing regulations. **Table 3.1** describes the list of accounts and other products to which this obligation should apply

Table 3.1: Proposed list of banking products

Deposit products	Lending products
Savings accounts	**Mortgages**
Call accounts	Business finance
Term deposits	Personal loans
Current accounts	Lines of credit (personal)
Cheque accounts	Lines of credit (business)
Debit card accounts	Overdrafts (personal)
Transactions accounts	Overdrafts (business)
Personal basic account	Consumer leases
GST and tax accounts	Credit and charge cards (personal)
Cash management accounts	Credit and charge cards (business)
Farm management deposits	Asset finance (and leases)
Pensioner deeming accounts	
Mortgage offset accounts	
Trust accounts	
Retirement savings accounts	
Foreign currency accounts	

We agree with the list of products prescribed for inclusion in the scope of Open Banking. However, from our experience with Open Banking in Japan, it has been our experience that some products (e.g. home loans) are at times not connected to core banking information systems, and not visible in internet banking. This makes it impractical for those banks to share this data via early versions of their APIs.

We advise Treasury to give consideration to this and similar practical limitations. In cases where certain products on the prescribed list are not able to be provisioned electronically, we propose allowing a phased approach to implementation.

Comment 3

Re. recommendation 3.9 – reciprocal obligations in Open Banking (p. 43-44)
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**.

Moneytree believes the principle of reciprocity is generally fair, as applied to the exchange of non-value-added data. If participants engaged in bank-like behaviour are receiving value from Open Banking, they should be required to make available their raw data to other participants in a similar way.

However, one interpretation of reciprocity obligations requires participants to on-share raw data they have received. We believe this creates significant technical and operational risks that could compromise the viability of Open Banking.

On page 44, the Report states:

> *"An Open Banking system in which all eligible **entities participate fully — both as data holders and data recipients** — is likely to be more vibrant and dynamic than one in which non-ADI participants are solely receivers of data, and ADIs are largely only transmitters of data. On the other hand, this proposal is essentially about banking data and any concern for fairness that leads to a principle of reciprocity **should not be allowed to unduly extend the scope of the system by stealth**".*
>
> *"This concern for balancing obligations of participants has led the Review to the conclusion that, **in principle, any non-ADI entity that participates in Open Banking as a recipient of data should also be obliged to provide equivalent data in response to a direction from a customer**. Equivalent data would consist of: **data received from another participant in Open Banking**; any customer-provided data (subject to the exclusions discussed above); data relating to the lending of money on credit; and data relating to the payment of monies to which they are either a party or that they are facilitating".*

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.

Comment 4

Re. recommendation 5.6 – persistent authorisation (page 88)
Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. **All authorisations should expire after a set period**.

Moneytree agrees with almost the entirety of this recommendation. However, we believe that is important for users to have the option to specify that third-party services may retrieve data on an ongoing basis and without expiring access.

In our experience, as a provider of financial data aggregation to nearly 2M bank customers in Japan, we are well aware of the high hurdle involved in requiring users to connect multiple financial institutions just to enjoy a new service. Enforcing expiry after a set period in all cases will lead to confusion among users as services simply stop functioning after unclearly defined periods. This would have the unintended effect of enforcing the status quo, and undermining the competition objective of Open Banking.

Instead, we recommend a more user centric approach, requiring data recipients to periodically notify users of continued access, and providing a readily accessible method to review and revoke connections.

Comment 5

Re. recommendation 5.10 – access frequency (p.91)
The Data Standards Body should determine how to **limit** the number of data requests that can be made.

Third party initiated data requests should not be any less frequent than the current standard in the European Union, which is four times a day. Different business models require more frequent access to data, and setting the maximum frequency too low could hamper the development of some existing, and yet to be discovered future, business models.

Comment 6

Re. recommendation 5.11 – transparency
Customers should be able to access a record of their usage history and data holders should keep **records of the performance of their API** that can be supplied to the regulator as needed.

We request clarification on what constitutes "records of the performance of their APIs." Does this definition include usage history? In the case that this is a list of 'who' an Open Banking participant has authorised for 'what' and 'when', this should be easy to develop and maintain.

However, if the recommendation requires a complete list of every API level access for each bank customer (presumably subject to seven years data retention) being delivered via API (which we presume under 'subject to the Customer Data Right and capable of being shared with third parties'); there would be a heavy burden on participants, and thus suggest the elimination of such obligation.

Comment 7

Additional considerations on the data transfer mechanism (Chapter 5)

On page 84, the draft proposal on Open Banking says:

> *"This Review does not make any recommendation that the Government should endorse screenscraping. However, banning it would remove an important market-based check on the design of Open Banking".*

Our company strongly agrees with this approach. In Japan, Open Banking is setting a 2-year transition period from the commencement date, by which time banks must comply with providing an approved method of access. From a practical viewpoint, we believe this period is too short a period for all banks to comply.

In Australia under the proposals, an overly aggressive transition schedule could lead to banks pushing for short cuts or exclusions in the data standards in order to meet the deadline. Such actions would necessarily limit the scope of data available, and thus limit third-party business optionality. Once again, phasing the implementation would mitigate the risks of this occurring.

Conclusion

It is Moneytree's view that the majority of the recommendations contained in the Report are well considered and headed in the right direction. In our comments above, we elected to focus on specific recommendations from the Report that should be reconsidered as a priority prior to implementation.

As a company with operations in Japan and Australia, we are privileged to participate in two Open Banking frameworks concurrently. The Japanese government passed legislation establishing an Open Banking framework in mid 2017, and it is due to commence from April 2018. In the lead up to this, Moneytree has providing its API service to more than 30 parties in Japan, including megabanks (the equivalent of Australia's Big Four Banks), regional banks, Fintech companies, major accounting software providers and ERP providers.

In addition to our experience and expertise in data management, we have considerable experience in the design of single-screen, customer consent mechanisms and developing a consistent customer-consent taxonomy (Safeguards contained in Chapter 4). We are happy to share this knowledge for the benefit of all participants in Australia. Given our relevant experience and expertise, as well as our neutral stance as a company working closely with banks and Fintechs alike, we welcome the opportunity to formally participate in the Data Standards Body in Australia.

Sincerely,

Mr Paul Chapman
Chief Executive
Moneytree Financial Technology Pty Ltd

Mr Ross Sharrott
Chief of Technology
Moneytree Financial Technology Pty Ltd