Raiz Invest Limited
ABN 74 615 510 177
Level 11, 2 Bulletin Place
Sydney NSW 2000
T 1300 754 748
www.raizinvest.com.au

17th February 2020

Senate Select Committee on Financial Technology & Regulatory

Dear Chair and Committee Members,

Thank you for the opportunity to provide our thoughts on how the Commonwealth, through its policies and laws, can create an ecosystem which promotes and encourages innovative products and start-ups to flourish and incentivises large businesses to collaborate or, at the least, play fair with smaller businesses.

Having had an opportunity to consider this in more detail, our view is that the issue needs to be taken back to basics.

All the innovative products, new start-ups and technology are all (fundamentally) aimed at data and the better use and analysis of data.

Therefore, it is critical for an ecosystem to recognise:

1. The ownership of that data; and
2. That the data has value.

In a retail banking ecosystem, the data accumulation by the large banks and financial service providers is massive. If the data is viewed as belonging to the individual bank client and the intrinsic value this data has is recognised by law – then, in our view, the ecosystem has a strong foundation for fostering innovation.

If this principle of data ownership and its value is accepted as a fundamental principle, then it follows:

a) access to the data should be controlled by the person who owns it; and
b) the owner's data may be held by a custodian (such as a bank) – but that party should be viewed merely as a custodian of that data (and not control or own that data); and
c) if the owner grants access to their data to a third party, that third party's access should be on the terms that the owner has agreed – and not prevented or restricted by the data custodian.

This then leads to the conclusion that all FinTech's, banks and financial service providers should have equal access, when granted, to the customers data, and that access should be on the same terms and subject to the same rules and regulations.

There should be no special, or streamlined regulations applying to one set of banks/financial services providers over another. The data belongs to the owner of the data (in our case, the individual retail bank customers) – and it should be that person who controls and decides how their data is used, who has access to it and what value it has. Their data custodian (i.e. in our case, the banks) should not have an ability to restrict their autonomy in making this decision, but like all custodians, should act on the instructions of their customers.

This fundamental principle of data ownership and equal access to data was recognised in Europe when Open Banking was introduced there. Under the European and UK version of the Open Banking Rules, the incumbent banks, financial service providers and FinTech's were all subject to the exact same rules in relation to data, privacy safeguards and obtaining consent. The incumbent banks did not have the benefit of streamlined accreditation or lesser consent requirements from their customers. It was this recognition of data ownership, and the creation of a level playing field for all participants that then led to the European model determining that screen scraping was not necessary (since the FinTech's otherwise had equal access to data).

In Australia, this is currently not the case or approach we have taken. Two examples draw out the differences and that the fundamental principle of data ownership does **not** underpin our rules. Under our CDR rules:

i. the banks have streamlined accreditation processes, while other financial institutions (particularly FinTech's) must go through full accreditation process; and

ii. The incumbent banks are the original custodians of customers' data. As such, the consent they must obtain from customers is governed by the Privacy Act. This consent obligation is a significantly less onerous burden than the obligation that applies to FinTech's under the CDR Rules who seek to be a data recipient. Such FinTech's must obtain double consent (consent by the customer to the FinTech itself *and* consent to the bank sharing the customer's data), on an annual basis under the CDR privacy safeguards – ironically a much higher bar that has to be met by the data custodians themselves.

This is an issue because it provides a significant competitive advantage for the large banks, Google and Apple (the later also collect large amounts of transaction data which can be married with other data in their data base).

For example, CBA recently reported that over 35% of the Australian population uses them as their primary bank – this means CBA gets access to the data of over 35% of the Australian population without having to obtain their explicit or ongoing consent for what the data is used for. It means that CBA can share this data, without their customer knowledge or consent (relying on the Privacy Act and their Privacy Policy), with their FinTech ecosystem, such as Klarna, even though CBA's customers may not be customers of these start-ups, as confirmed in the recent letter to the committee from CBA.

If FinTech's in the CBA ecosystem, such as Klarna, were to start off without the benefit of their relationship with CBA, then they would be subject to the same requirements as other FinTech's – i.e., they would first have to go through full accreditation under the CDR rules to access customer data, and they would need to obtain double consent (consent by the customer to the FinTech itself *and* consent to the bank sharing the customer's data). This double consent would need to be renewed annually.

However, by being part of the CBA ecosystem, FinTech's, such as Klarna, will be able to 'piggy-back' off the CBA arrangements and rely on the Privacy Act to access 35% of the Australian population's banking data *without* being fully accredited under the CDR Rules (instead getting the benefit of streamlined accreditation) and *without* having to obtain the annual double consent.

It is apparent from this example how uneven the playing field currently is, and that the current rules have a material and adverse impact on the viability and ongoing commerciality of conducting innovative FinTech business in Australia, particularly against an incumbent bank, Google or Apple – or any FinTech that they own.

Is this really what the owners of the data (i.e. the customer) wants?

Large businesses (like Apple and Google) and the large banks (like CBA) already collaborate with (and invest into) a few handpicked FinTech companies. These FinTech's are carefully chosen to either expand the incumbent's market share or drive greater revenue to the incumbents.

Given this investment and collaboration is already occurring by the large banks, in our view, if the Commonwealth wants to foster an ecosystem that encourages innovation and enables new product to get to market, then it needs to ensure that the playing field is fair and level for all participants. The single best policy that the Commonwealth can implement in this regard is to recognise who owns the data and that the data is valuable. These two fundamental principles require the Commonwealth to safeguard the data of individuals and to give control over that data back to the individuals who own it – and not allow it to be held captive by the incumbent banks who happen to have an unfair advantage because they were there first.

Yours Sincerely,

Brendan Malone
Chief Operating Officer
Raiz Invest Limited