SUBMISSION PAPER:

Submission to the Australian Competition and Consumer Commission Consumer Data Right - Participation of third party service providers

January 2020

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 170 FinTech Startups, VCs, Accelerators and Incubators across Australia.

About this Submission

This document was created by FinTech Australia in consultation with its Open Data Working Group, which consists of over 150 company representatives. In particular, the submission has been compiled with the support of our Working Group Co-leads:

- Rebecca Schot-Guppy, FinTech Australia
- Alan Tsen, FinTech Australia

This Submission has also been endorsed by the following FinTech Australia members:

- Moneytree
- Basiq
- Biza.io
- TrueLayer
- Proviso
- MoneyPlace
- Zip Co
- SideFund
- Nudge
- Certified By
- Harmoney Australia
- ID Exchange
- Banjo

Submission Process

In developing this submission, our Open Data Working Group held a series of Member roundtables to discuss key issues relating to the Data Standards.

We also particularly acknowledge the support and contribution of K&L Gates to the topics explored in this submission.

Context: Open Banking in Australia

FinTech Australia has been a consistent advocate for policy reform to drive the implementation of an Open Financial Data framework in Australia. We have made numerous submissions to Federal Treasury, the Productivity Commission, Open Banking Inquiry, the Australian Competition and Consumer Commission (**ACCC**) and Data 61 on the need for a framework for the sharing of financial data and on the details of that framework.

We are strongly supportive of the ACCC's efforts to accommodate intermediaries into the Consumer Data Right (**CDR**) framework.

Throughout this process, we have emphasised the need for a regime which is flexible enough to enable participation by third party service providers. Without this, we are concerned that the CDR regime will be under-utilised and may not generate the anticipated advancements. Such advancements have the potential to drive innovation, competition and consumer choice, through giving consumers increased control over their data. Allowing for fulsome participation by intermediaries and other service providers will pave the way for innovative CDR use cases. Without this, any entity looking to provide consumers with a CDR-powered tool would face the significant costs of accreditation and integration. For many, these costs will be prohibitive.

The experience of other equivalent regimes around the world has also been that the greatest efficiencies can be gained by a small number of intermediaries providing the rails for data aggregation and sharing. Existing data aggregators (such as Proviso, Basiq, Yodlee, TrueLayer, Plaid etc) already fulfil this intermediary role using existing technology. Without creating the framework for intermediaries to operate within the regime, aggregators may continue to use existing technology or create their own “closed-loop” data platforms.

Participation of third party service providers

FinTech Australia welcomes the opportunity to put forward its position on behalf of members in relation to the participation of third party service providers in the CDR regime.

Our responses to the questions in the ACCC's December 2019 Consultation Paper are set out below.

A. Intermediaries

Question 1: ***If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that Consultation on how best to facilitate participation of third party service providers 4 intermediaries can bring to the CDR regime and for consumers?***

(a) Services to be provided by intermediaries

FinTech Australia anticipates intermediaries will adopt a range of business models and will provide a range of services. As such, the regime for their participation needs flexibility.

Based on input from our members, we expect some intermediaries will perform a primarily infrastructure role, providing a technical solution to data recipients to interface with the open banking APIs, without having to build this themselves. Such intermediaries may not store any CDR data and may not provide any enrichment.

Alternatively, intermediaries may step in to provide discrete or end to end components of implementation. For example, an intermediary may provide a consent management service, handling the aspects of open banking which relate to obtaining consent, consent dashboards, managing revocations, monitoring and prompting for expiry, etc.

At the other end of the spectrum, an intermediary may play the role of aggregating multiple sources of data (CDR data from multiple data holders, together with other data that is not covered by the CDR regime), storing that data, enriching the data in various ways (performing

analysis, generating insights, etc) and providing tools for the ultimate data recipients to deploy this data into their own products and services. This model may even involve intermediaries aggregating the data and anonymising it, to enable data recipients to gain insights from the data without accessing individual personal information.

If the CDR regime enables full participation by intermediaries, they may also facilitate emerging personal data sharing services, including by way of "Me2B" consumer centric models with a focus on privacy and security by design where the consumer is treated as the custodian of their own data. Allowing intermediaries to deliver these services (rather than having individual fintechs build their own tools) will provide significant costs savings, as well as fast tracking innovation. To build such Me2B infrastructure would typically be out of the realm of start-ups who during early stage product innovation can ill afford the investment to build at-scale commercially robust infrastructure required to meet the necessary levels of security and privacy compliance. Me2B models would also necessitate a tailored approach to which entity is responsible for obtaining and managing customer consents.

The use of intermediaries could also open the way for the collation of data between jurisdictions. FinTech Australia members would like to see a regime for intermediaries which is flexible enough to allow sharing of data to overseas entities, where supported by appropriate consents and equivalent consumer protections.

(b) Services to be provided to consumers using intermediaries

Any use case for CDR data could be delivered by a data recipient using an intermediary. In addition, the use of intermediaries may allow for the aggregation of disparate data sets which would be more difficult without the involvement of an intermediary.

(c) Collect and use

We anticipate some intermediaries will collect CDR data and pass it on, whereas others will both collect and use that data. Intermediaries may also process data to generate insights and share that derived data with data holders. As noted above, some intermediaries may pass data on to data recipients in an aggregated, anonymised form.

Finally emerging technologies (such as those referred to as "Me2B") may involve intermediaries effectively providing rails between CDR Data Holders and end users without the intermediary every having visibility of the data in transit. This may involve the consumer acting as the custodian of the returned data, with the intermediary facilitating analysis to be conducted on the consumer's data in order to offer tailored or new services.

(d) Economic efficiencies

Our members anticipate that there will be significant costs involved in building systems which can effectively collect and use open banking API data, and/or collect and manage consents, in a way which is secure and compliant. Depending on the level of internal development involved and the use of third party tools, our members anticipate costs of between $100,000 to $250,000 in order to achieve accreditation. These costs are not being deployed towards developing, and realising, their use case, but on building the underlying infrastructure and compliance. This will stifle the innovation which could otherwise be unlocked by the CDR regime. Using intermediaries enables these costs to be shared or significantly reduced. An intermediary whose costs can be shared in this way is also likely to be able to make a bigger investment into developing robust, quality systems which will provide better outcomes for consumers. Data recipients who can use the services of an intermediary will also be able to focus on how they can deliver value.

Allowing the use of intermediaries will also mean data recipients are saved from investing considerable time designing and building their own infrastructure. For a start-up with a potentially limited capital runway, this would be a significant benefit.

Question 2: ***How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.***

The rules currently provide for data recipients to outsource certain activities to third parties. We have always supported the inclusion of this ability in the rules, as it enables data recipients to adopt a range of business models.

For the reasons outlined throughout this submission, we consider an accreditation model is also required for intermediaries. That is, we see a need for intermediaries to have direct access to the open banking APIs in their own right, under their own accreditation, in order to provide their services for data recipients.

Where an intermediary is integrating with the APIs and aggregating data, we expect this would be most efficient through the intermediary's own accreditation, rather than supervision by a data recipient. In practice, data recipients who use the services of an intermediary are unlikely to be in a position to assess and supervise an intermediary's compliance with the relevant requirements. Indeed, a large part of the benefit of engaging an intermediary is not needing to engage with those requirements.

***Question 3:** What obligations should apply to intermediaries? For example, you may wish to provide comment on:*
a. if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;
b. if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;
c. if the obligations should differ depending on the nature of the service being provided by the intermediary.

(a) Accreditation model

FinTech Australia would support an accreditation model which requires intermediaries to comply with all of the obligations which currently apply to 'unrestricted' data recipients. We consider that the risks attaching to an intermediary are broadly equivalent to those of a data recipient which has itself integrated with the open banking APIs.

For data recipients dealing with intermediaries, accreditation should allow them to deal with an intermediary without having to independently satisfy themselves that the intermediary meets all of the relevant requirements.

An adjustment to the accreditation process may be required in relation to the revocation of accreditation of an intermediary. As many data recipients (and their consumers) may be relying on an intermediary to access the APIs, revoking an intermediary's accreditation could have a significant impact on many consumers. As such, it would be preferable for the basis for such revocation to be heightened and for transition arrangements to be put in place to give data recipients time to make alternative arrangements.

(b) Outsourcing model

We support the continued ability for data recipients to outsource activities to third parties. As the accredited data recipient remains responsible for the performance of those activities, we do not see a need for prescribing the manner in which data recipients contract with their service providers.

(c) Different levels of obligations

As it would be preferable for the intermediary regime to be principles-based to provide flexibility, we anticipate that it would be difficult to introduce different layers of obligations which would apply to different types of intermediary. This is something which could be explored during later iterations of an intermediary regime.

Question 4: ***How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.***

Fintech Australia supports full notification to consumers of any intermediaries being used. We consider that consumers should be fully aware of not just the data recipients who will ultimately receive their data, but also the intermediaries which will be used to obtain that data.

In order to enable consumers to understand the role of intermediaries, a broader education campaign may be needed.

The various use cases which could be involved, including multiple intermediaries aggregating various aspects of the data and sharing it with multiple data recipients, may make it difficult to design a convenient consent process for all intermediary use cases. For example, in some instances it is most convenient for an intermediary to seek and obtain consent from consumers on behalf of a range of data recipients. Alternatively, if the data recipient has the relationship with the consumers, the recipient should initiate the consent process.

The ACCC may wish to explore whether intermediary information could be visible to consumers through the consumer dashboard contemplated by the current rules. This would facilitate a level of consumer awareness and control, without creating additional confusion.

We expect it will be necessary for the ACCC to examine existing research, and conduct further research, about how consumers engage with the consent process and how best to involve intermediaries.

Furthermore, the regime should allow for data recipients to engage the services of an intermediary (or outsourced service provider) to provide tools for managing the consent process itself.

Question 5: ***How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.***

Fintech Australia considers that data recipients who seek to share data with other data recipients should be regulated as intermediaries. That is, such data recipients would need consent from the consumer to share data in that way and would need accreditation as an intermediary.

Question 6: ***Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?***

FinTech Australia considers that data recipients who use the services of an accredited intermediary should be subject to a reduced set of accreditation criteria. The data security issues which arise when an entity is integrating with a data holder's open banking APIs do not arise in the same way for data recipients who receive information through an intermediary.

While data recipients will still be holding CDR data, this is not unique. Consumers already have the ability to obtain their own bank data (for example, in the form of downloaded statements) and share it with third parties. Where they do so, the third party recipient must simply hold that information in accordance with general privacy laws and any arrangements agreed between the third party and the consumer. Accordingly, we do not consider that it is necessary for all of the accreditation criteria to apply to a data recipient which receives information through an intermediary.

Our members have proposed that accreditation for data recipients who use an intermediary could be achieved by the ACCC adopting a subset of requirements for those data recipients. For example, depending on the business model involved (eg whether the data recipient holds / stores data), data recipients who use an intermediary could be exempted from some of the accreditation requirements, such as the need to maintain the specified level and type of professional indemnity insurance and dispute resolution membership. However, we anticipate all accredited data recipients would need to comply with all of the remaining aspects of CDR Rules, especially as they relate to consumer consent and other interactions with consumers.

An alternative would be to consider adopting rules for recipients obtaining data from intermediaries in line with those expected of general accounting firms notably adherence to the Privacy Act and its associated provisions for mandatory data breach notifications.

Finally, rather than requiring accreditation from the ACCC, accreditation for these data recipients could simply involve them satisfying the relevant accredited intermediary that they are a fit and proper person to receive CDR data. Intermediaries would need to make this assessment fairly and in good faith, having regard to criteria determined by the ACCC. In some

ways, this is an extension of the commercial due diligence intermediaries would already be conducting on technology vendors.

B. Disclosure of CDR data to non-accredited third parties

Question 7: ***If the ACCC amends the rules to allow disclosure from accredited persons to nonaccredited third parties and you intend to: a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.***

Some examples of how consumers currently share their banking data with non-accredited third parties are below. All of these scenarios may use an intermediary in the process:

- Rental applications - providing bank statements to a real estate office to prove income
- Budgeting software - help consumers understand their finances with bank transaction feeds
- Accounting software - help businesses manage, reconcile and understand their finances with bank transaction feeds
- Property management software - help property investors reconcile and manage rental payments with bank transaction feeds
- Payments providers - for AML obligations need to verify that a bank account name is connected to a BSB and Account number. Transaction data may not be required but bank account details are.
- Identity Verification requirements (variety of financial and non-financial services) generally result in the need to provide utility or bank statement for proof of address
- online small business lenders - accessing transaction history
- responsible lending assessments for consumer finance or buy-now-pay-later providers.

Many of the above use cases depend on speed of processing and the CDR regime, with appropriate inclusion of intermediaries, has the potential to greatly improve processing speeds.

Question 8: ***What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?***

Currently, consumers have the ability to share their own data freely with their own service providers (for example, through sharing bank statements). We consider that the CDR regime should not restrict the ability of consumers to continue to do so. Imposing restrictions on a

consumer's ability to deal with their own data would seem to be inconsistent with the aims of the CDR regime. Accordingly, FinTech Australia supports the ability for consumers to continue to share, and authorise the sharing of, their data with non-accredited third parties. As noted above, however, FinTech Australia supports the need for accreditation of Data Recipients who participate in the CDR regime.

Question 9: ***What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?***

FinTech Australia considers that the sharing of data obtained through the CDR regime with non-accredited third parties should be subject to the general privacy and consumer protection arrangements.

The CDR regime is designed to protect the interaction between data holders and data recipients. We do not consider that it is intended to afford special protection to financial data in general, in excess of the protections which apply to other forms of personal information. The privacy law already singles out data which warrants additional protection (ie sensitive health data). If there is a view that financial data, or all personal information, requires additional protection, this should be done through amendments to Australia's general privacy and consumer protection laws.

FinTech Australia is concerned by any attempts to effect broad reforms to Australia's existing privacy and data security laws by expanding the application of the CDR. If all data sourced through the CDR regime is subjected to greater privacy and other consumer protections, it is likely that many innovative businesses which would otherwise have used the CDR compliant APIs will find other ways to obtain that data (including through existing informal channels). We wish to highlight that there are an increasing number of emerging organisations worldwide which, while promoting "open banking" solutions are, in fact, proprietary in nature. If participating in the CDR regime data is beyond the reach of the majority of organisations, the market will likely be motivated to find alternative solutions (which may include proprietary APIs and/or legacy technologies). This may impact the stated intended goals of the CDR regime.

Question 10: ***What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?***

Given our comments above, we consider this question is more relevant to a broader assessment of whether Australia's general privacy regime remains appropriate.

We consider that the position under Australia's general privacy laws in relation to sharing this data should apply. We anticipate this would generally mean such data could only be shared after appropriate disclosure.

Conclusion

FinTech Australia thanks the ACCC for the opportunity to provide inputs and recommendations on the development of the Consumer Data Right, including in respect of the participation of intermediaries. We will continue to engage on the broader issues in relation to Open Banking.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech Industry, representing over 300 fintech Startups, Hubs, Accelerators and Venture Capital Funds across the nation.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to drive cultural, policy and regulatory change toward realising this vision.

FinTech Australia would like to recognise the support of our Policy Partners, who provide guidance and advice to the association and its members in the development of our submissions:

- Baker McKenzie
- Cornwalls
- DLA Piper
- Hall & Wilcox
- King & Wood Mallesons
- K&L Gates
- The Fold Legal