SUBMISSION PAPER:

Submission to the Australian Competition and Consumer Commission Consumer Data Right - Consultation on proposed changes to the CDR Rules

November 2020

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 300 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 lead:

- Rebecca Schot-Guppy, FinTech Australia

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

- Adatree
- Afterpay
- Archa
- Banjo Loans
- Basiq
- Biza.io
- Credi
- Data Republic
- FinSS Global
- Firstmac
- Frollo Australia
- Joust
- loans.com.au
- MoneyPlace
- MoneyTree
- Prospa
- SideFund
- Tanggram
- True Layer
- Wisr
- Yodlee

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 and DLA Piper 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 the 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 further models into the CDR framework.

For ease of reading, we have incorporated the questions from the ACCC's Consultation Paper "CDR rules expansion amendments" dated September 2020 and included our responses inline below.

1. We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

While these changes will have build implications, including in relation to the way consent is dealt with in the data specifications, FinTech Australia considers these changes are vital to the effective functioning of the ecosystem and would support a swift timeline.

2. The proposed rules include three discrete kinds of restricted accreditation (i.e. separate affiliate, data enclave or limited data restrictions). We welcome views on this approach and whether it would provide sufficient flexibility for participants. In responding to this question you may wish to consider whether, for example, restricted accreditation should instead be based on a level of accreditation that permits people to do a range of authorised activities.

The three different models for restricted accreditation are a large step in the right direction and will facilitate participation within the ecosystem by participants who are not accredited to the unrestricted level.

However, a key concern that FinTech Australia has is that the three different forms of restricted accreditation, and the way they interact with the rules in relation to CAP arrangements and ADR-to-ADR transfers, introduce a high level of complexity into the environment. We consider that there are alternative ways to achieve the benefits of tiered accreditation (as discussed below) without the need for such complexity. FinTech Australia also considers that the terminology around intermediaries which has already been introduced into the Rules may be a preferable avenue than further complicating the CAP and ADR-to-ADR transfer concepts.

FinTech Australia considers a preferable approach may be to adopt a model similar to the AFSL holder / Authorised Representative model which is already familiar to the financial services industry. This could be adopted in place of the proposed sponsor / affiliate model. The restrictions in relation to an affiliate only receiving data from a sponsor (and needing multiple sponsors if data was to be received from multiple sources) could also be eliminated - there is no need to tie accreditation under this model to the method of accessing data. For the purposes of this paper, we will refer to this as a "Representative model" (rather than sponsor / affiliate).

FinTech Australia supports the concept of lower accreditation and compliance requirements for entities which only receive limited data, however questions whether it is necessary for this to be implemented as a separate accreditation model. Instead, this could be achieved through a concept similar to the product authorisations on an AFSL - not every AFSL authorises the same activities, nor does it entail the same compliance obligations.

Similarly, FinTech Australia supports the concept of a reduced burden for entities which only receive data through a data enclave. However, we consider that there is scope to significantly reduce the complexity associated with this. For example, FinTech Australia queries whether this could be simplified by either:

- incorporating this concept within the Representative model outlined above. The data enclave will, by definition, involve an entity receiving CDR data from an enclave provider. The recipient could be authorised by the enclave provider (or another accredited entity) to access the data; or
- adapting the concept of "CDR Insights" to provide an exemption for entities which only access data through a data enclave.

3. We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation.

FinTech Australia supports a risk based approach to accreditation, such that entities which pose a lower risk are subjected to lower accreditation and compliance requirements. However, we are concerned about additional complexity which would be introduced if further accreditation models were to be introduced.

If this approach were to be taken, FinTech Australia recommends that this risk based thresholds be converted to a technical definition, so that data holders could cascade down these restrictions in a way that integrates with fraud management systems.

4. What are your views on the low to medium classification of risk for the data set out in Table 1?

FinTech Australia broadly agrees with the risk classification set out in Table 1. However, it appears that there are certain scopes which are not addressed in the table (such as more specific financial information). If this is because it has been concluded that this information is of higher risk, it would be useful for that to be confirmed.

5. Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?

FinTech Australia believes that the accreditation criteria that apply to individuals accredited to the restricted level are appropriate.

6. Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?

FinTech Australia considers that this data set would enable existing and future CDR use cases and would therefore encourage participation in the CDR.

However, as noted above, the current implementation is likely to lead to increased complexity which could have the opposite effect.

7. Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.

FinTech Australia believes that the data enclave restriction would increase participation in the CDR for existing and future use cases. For example, it may allow credit scoring / assessment by running algorithms within the data enclave. It may also enable platform operators to allow third party applications / plugins to run on the data and derive valuable insights.

8. Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?

In light of the updated approach to accreditation, FinTech Australia questions the ongoing need for CAP arrangements within the rules. This concept was an attempt at allowing multiple parties to collaborate to provide services, however the level of prescription involved in CAP arrangement is unnecessary and restrictive. We also note the possibility of using the Intermediary concept to provide a simpler framework here.

Specifically in response to this question, on the assumption that the CAP arrangement concept is retained, we do not see the need for the CDR Rules to prescribe incident management arrangements between the parties. In many respects, the level of prescription involved in the CAP arrangements concept should be reduced. We do note the complexity of shared responsibility reporting obligations.

9. Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?

FinTech Australia believes that it would be appropriate for entities managing data enclaves to demonstrate appropriate data leakage protections are in place. It would also be prudent to have additional requirements around the bulk export of data.

10. Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.

As noted above, FinTech Australia believes that the affiliate restriction level would increase participation in the CDR significantly. We do however have concerns around the complexity of the current implementation and, in particular, the interaction with this model and the CAP arrangements concept. In order for the CDR to be utilized by the largest number of entities possible we believe it is necessary to have an ecosystem which is clearly understood and this affiliate restriction level, while welcome, does appear to add a layer of complexity when viewed alongside the CAP arrangements. We have outlined above possible mechanisms for simplifying this.

11. Should there be additional requirements under Part 1 of Schedule 2 for sponsors?

FinTech Australia has concerns around the need for an affiliate to have multiple sponsors in the CDR environment. It is not clear why an affiliate is required to only receive data from a sponsor and why, where the affiliate receives data from multiple sources, that each source would need to be a sponsor. Not only does this create additional complexity, it also creates the issue of there being confusion around who would have liability if there was a breach or data incident.

12. Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?

As noted above, in light of the updated approach to accreditation, FinTech Australia questions the ongoing need for CAP arrangements within the rules. This concept was an attempt at allowing multiple parties to collaborate to provide services, however the level of prescription involved in CAP arrangement is unnecessary and restrictive.

Specifically in response to this question, on the assumption that the CAP arrangement concept is retained, we do not see the need for the CDR Rules to prescribe incident management arrangements between the parties. In many respects, the level of prescription involved in the CAP arrangements concept should be reduced.

13. The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.

> *Example level 1: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems.*
>
> *Example level 2: affiliate is able to access all data sets, but uses some of the sponsor's systems and applications to access or manage the data.*
>
> *Example level 3: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor's systems and applications to access or manage the data.*

FinTech Australia believes that these distinctions may be useful in reducing the controls which need to be imposed on an affiliate. As outlined above, if this concept were addressed through a Representative model (in a similar way to the current AFSL regime), this could be achieved by the sponsor granting authorisations to the affiliate which are a subset of the authorisations held by the sponsor.

However, if this model is to involve different requirements based on the scope of data and the type of access, it would significantly overlap with the limited data restriction and the data enclave restriction. This is undesirable.

Finally, we do again have concerns around the level of complexity being introduced with multiple levels of tiering.

14. We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.

FinTech Australia agrees with this position but is keen to see technical guidance on this matter to enable us to better understand how this will practically work.

Furthermore, we question whether the CAP arrangement concept is still required in light of proposed developments to the accreditation model and the existing intermediary concept (adjusted as necessary).

15. Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data?

Fintech Australia does not believe that this approach is necessary. It would be preferable to link the consent process as closely as possible to the relevant action, so that a consumer provides consent to disclosure at a separate point to the time of providing consent to collection / use.

a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate?

b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the consumer and, if so, to what extent?

In line with usual business practice, Fintech Australia would maintain that commercial arrangements between ADRs remain confidential where they have no bearing on or impact upon the rights or freedoms of the consumer.

We appreciate and acknowledge the rationale for proposed changes to the consent models (including separate collect, use and disclosures consents, duration of consents etc.), and to the authorisation processes for amending, withdrawing consents etc under Rules 4.3.2 A-C and related. However, as a general note, concerns are raised on the increasing complexity of the regime's consent model, including the technical challenges presented by these proposed changes and the resulting potential for negative impacts to the overall customer experience - and take-up.

By way of clarity, our members are of the view that there needs to be a common set of standards that apply to consumer consents, to ensure a level of consistency and consumer understanding on the various consent and authorisation methods being proposed. Previous submissions have confirmed that a form of 'open source' consent model is required to ensure a level of traction in the system, such that similar technical standards, consent management protocols and customer experience applies throughout the entire CDR process. Members therefore repeat their request for an overarching consent management model to be developed, using open source standards, in parallel with and alongside any changes to consents under the Rules. Without such a consent model in place, the risk of inconsistent methods of communications of consent, and consumer mistrust, is high. Our members do not view proposed changes to the Rules as operating in isolation from the technical standards that must address such changes - and in fact it is the technical standards themselves which should dictate the scope of change to the Rules as regards consumer dashboard display information, including on consents.

Some of our members have previously provided separate submissions to ACCC/Treasury as regards the recommended adoption of a proposed data consent model, accommodating recommended sets of standards, which we would be happy to re-provide and explore further with the ACCC/Treasury.

Similar considerations - as regards the technical challenges and the need for a broader consent management model – are raised on the proposed Rules revisions with regard to the sharing of CDR data on joint accounts and the setting of consumer preferences as part of the broader authorisation process. Our members also recommend that the process for amending authorisations be further simplified for consumers under Rule 4.3.2A-C., taking account of the complexities raised by the additional processes proposed.

It may be that the workability of the mechanisms and consent model proposed under these revised Rules would benefit from an experimentation or test period, to challenge some of the assumptions made under these proposed Rule changes (a test period, in a similar manner to, for example, FS regulatory sandbox environments) – which would allow for areas of issue to be properly identified and remediated prior to full live roll-out.

A specific concern is that the more detailed and nuanced the consent process is at the outset, the more likely it is the consumers will not understand it - resulting either in poorly informed consent or opt out. This is undesirable. It would be preferable to link the consent process as closely as possible to the relevant action - for example, it would not be a good CX design to ask consumers at the time of giving their consent how they wished their data to be dealt with if, in the future, they revoked their consent. This should be asked at the time of any future revocation.

16. To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession's regulatory regime in your response.

We welcome the proposed amendments to the Rules that allow ADRs to disclose CDR data to trusted advisors and to disclose limited 'insights' derived from CDR data to any nominated persons.

Our members also agree that the obtaining of a specific consent with regard to the disclosures to such trusted advisors is helpful, but queries how in practice these types of consents will in fact be implemented. Our earlier comments as regards the technical specification challenges associated with obtaining consents more broadly are repeated here.

As regards the classes of trusted advisors currently proposed, our members suggest that a broader method in which to define classes may be appropriate to be considered in the Rules. For example, defining by reference to the holder of an AFS licence, credit licence or other professional service licence may be a reasonable conditional approach.

Specifically our members have recommended including individuals that provide assistance in relation to commercial credit (i.e. brokers that are not mortgage brokers) in the prescribed list of trusted advisors. This would ensure that advisors assisting small businesses in relation to small business credit products that are not secured by mortgages, are included within the regime. It would, in turn, promote the financial inclusion of small businesses and their greater participation in the CDR regime.

17. Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?

We anticipate that there could be difficulty to distinguish between an ADR which is providing a good or service, as compared to an ADR which is operating as a conduit. If a consumer wishes to make their data available to a trusted adviser, it could be argued that an ADR which facilitates that data being made available to the trusted adviser is, by doing so, providing a good or service to the consumer.

18. Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding 'raw' CDR data as disclosed by the data holder)?

The disclosure of CDR 'insights' is viewed as valuable data and the definitions as proposed are agreeable (though the definitions would be assisted with illustrative examples).

There may, however, be difficulties drawing a distinction between raw data and derived data - for example, bank transaction data which are turned into entries in an accounting system appear to be intended to be derived data for this purpose, however the level of processing may be minimal.

19. What transparency requirements should apply to disclosures of CDR data insights? For example, should ADRs be required to provide the option for consumers to view insights via their dashboard, or should consumers be able to elect to view an insight before they consent for it to be disclosed to a non-accredited person?

On the consumer transparency requirements applicable to the disclosure of CDR data insights, our members express the view that 'consent fatigue' and overloading the consumer is highly likely to occur – and whilst the option to view permissions via consumer dashboards may be helpful, as raised, the technical standards that apply to 'how' these disclosures arise, and consistency across the eco-system, continues to be a key area of risk / concern.

20. We are seeking feedback on the proposal for enabling business consumers (both non-individuals and business partnerships) to share CDR data.

This is a concept of which FinTech Australia approves.

21. In particular, we welcome comment on the proposal to require a data holder to provide a single dashboard to business consumers which can be accessed by any nominated representative to manage CDR data sharing arrangements.

FinTech Australia is in favour of this concept however we await further technical information to understand how this would work.

22. Are there other implementation issues the ACCC should be aware of in relation to the proposed rules for CDR data sharing by non-individuals?

Our members have recommended the introduction of rules to the effect that where an individual identifies themselves as a nominated representative of an entity, third parties may rely on this representation for the purposes of the CDR Rules (including consents, authorisation and activities undertaken through the customer dashboard) without having to verify its accuracy.

Without seeing further technical materials, FinTech Australia does not have any further view on this matter.

23. We welcome comment on the proposed approach to require data holders to treat business partnerships in line with the approach for dealing with business consumers? Do you foresee any technical or other implementation challenges with taking this approach for business partnerships that the ACCC should take into account?

FinTech Australia supports a consistent approach being taken for all non-individual customers, regardless of entity type.

24. Should additional protections be introduced for personal information relating to business partners who are individuals?

We do not consider that this is necessary. Such information could be dealt with in line with whatever consents have been provided by the partnership.

25. Are there other aspects of the rules that may require consequential changes as a result of the enablement of business consumers? For example, are the internal dispute resolution requirements appropriate for business consumers?

Again without seeing technical material FinTech Australia does not have a particular view on this matter.

26. We welcome feedback on the proposals for enabling authorised users to share CDR data.

This is a very broad question. Without a properly defined architectural outcome, it is difficult to assess whether the proposed model is feasible.

27. Should persons beyond those with the ability to make transactions on an account be considered a person with 'account privileges' in the banking sector?

FinTech Australia's preliminary view is that persons with account privileges would be sufficient.

28. How should secondary users rules operate in a joint account context?

FinTech Australia does not have a strong view on this matter. The key concern here is again that this level of detail may lead to unnecessary complexity.

29. As well as having the ability to withdraw a 'secondary user instruction', should account holders be able to have granular control and withdraw sharing with specific accredited persons that have been initiated by a secondary user?

FinTech Australia's preliminary view is that this appears to be appropriate.

30. We are seeking feedback on our proposals relating to sharing CDR data on joint accounts, including:

a. the proposed approach to require data holders to allow consumers to set their preferences (a disclosure option) as part of the authorisation process

b. the proposed approach of allowing 'joint account holder B' to withdraw an approval at any time

c. the expansion of the rules to include joint accounts held by more than two individuals

d. the proposal that joint account holder B does not have to 'approve' amendments to authorisations

e. the proposed approach that the rules do not require (but do not prohibit) the history of disclosure option selections being displayed to consumers as part of the joint account management service or data holder consumer dashboard.

FinTech Australia does not have a strong view on this matter. The key concern here is again that this level of detail may lead to unnecessary complexity.

31. Do the benefits of requiring data holders to display on-disclosures to 'joint account holder B' outweigh the costs?

FinTech Australia does not have a strong view on this matter. The key concern here is again that this level of detail may lead to unnecessary complexity.

32. Should accredited persons be required to offer consumers the ability to amend consents in the consumer dashboard, or should this be optional?

Again FinTech Australia does not have a strong view on this as we have not been able to view the requisite technical information which would enable a clear view on this matter.

33. We are seeking feedback on the proposed rules about the way accredited persons are able to invite consumers to amend their consents. Should a consumer be able to amend consent for direct marketing or research in the same way as amending consent for use of data in the provision of goods and services?

We believe that this would be appropriate however it does again raise concerns about the complexity of the consent model.

34. Should the authorisation process for amending authorisations also be simplified?

FinTech Australia does not see any issue with this suggestion.

35. We are seeking feedback on the proposed approach of separating the consent to collect from the consent to use CDR data (rather than combining consent to collect and use).

As previously stated while this model certainly has advantages and may enable more entities to enter into the CDR framework, we have serious concerns about the level of complexity in the consent process and fear that this complexity may deter consumers from engaging with the CDR framework.

36. Should accredited persons be able to offer disclosure consents only after an original consent to collect and use is in place (with the effect that combining a use and collection consent with a disclosure consent would be prohibited)? See also the consultation questions in section 7.2 above.

The key concern here is again that this level of detail may lead to unnecessary complexity.

37. We are seeking feedback on the 'point in time' redundancy approach.

FinTech Australia sees value in a point in time redundancy approach to consents. However there are still a wide range of concerns about how this would operate in practice and how it would interact with the proposed consent models. In order to have an appropriate view on this, we would first need to know how the consent model will work with the above comments that we have made in relation to the complexity of the model.

38. We are seeking feedback on the proposed approach where a consumer withdrawing their authorisation for a data holder to disclose their CDR data results in removal of the ADR's consent to collect only.

While FinTech Australia agrees with this fragmented approach to the removal of an authorization there is again the broader issue of the entire consent framework being potentially too complex to allow broad use by consumers.

39. We are seeking feedback on the collection consent expiry notification and permissible delivery methods.

FinTech Australia believe that it would be appropriate for these notifications to be done through existing channels with consumers.

40. We welcome any comment on the proposed rules to improve consumer experience in data holder dashboards.

Given the dearth of technical detail FinTech Australia is not in position to provide comments on the data holder dashboards.

41. We are seeking feedback on whether the proposed amendments place the obligation on the party best placed to meet the obligation.

FinTech Australia believes that the requirements are currently placed on the correct parties.

42. Are there any technical or other implementation issues of which the ACCC should be aware?

Broadly speaking the technical and implementation issues are as stated above. These are that the proposed consent model is convoluted and may potentially deter use of the system and that the lack of technical detail provided so far by the ACCC makes it difficult to ascertain what the actual technical issues will be.

Conclusion

FinTech Australia thanks the ACCC for the opportunity to provide inputs and recommendations on the development of the draft rules. 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:

- DLA Piper
- King & Wood Mallesons
- K&L Gates
- The Fold Legal
- Cornwalls