

The Manager  
Consumer Data Right  
Australian Competition & Consumer Commission  
GPO Box 3131  
Canberra ACT 2601

By email: [ACCC-CDR@accc.gov.au](mailto:ACCC-CDR@accc.gov.au)

SUBMISSION PAPER:

## Consultation Paper Facilitating the participation of intermediaries in the Consumer Data Right regime

*This Submission Paper was prepared by Prospa Advance Pty Limited (47 154 775 667). [www.prospa.com.au](http://www.prospa.com.au)*

Prospa Advance Pty Limited (“Prospa”) welcomes the opportunity to provide feedback on the ACCC’s consultation on the participation of intermediaries in the Consumer Data Right (‘CDR’) regime.

### 1. A little about us – “Prospa”

Prospa is currently Australia’s #1 Online Small Business Lender<sup>1</sup>, operating out of our Sydney headquarters. Prospa has supported small businesses with funding of more than \$1.35 billion and employs over 250 people in Australia.

Prospa offers Small Business Loans between \$5,000 to \$300,000 and a Line of Credit for up to \$100,000. All customers of Prospa are small businesses with all funding decisions achieved by

---

<sup>1</sup> Market position for online balance sheet lenders to Australian small businesses, based on Prospa’s volume as a percentage of total market volume in 2017 as reported in KPMG “The 3rd Asia Pacific Region Alternative Finance Industry Report”, November 2018; USDAUD FX rate of 0.767.



assessing well over 450 data points, including turnover, profit & loss, business tenure, size and industry sector.

Prospa uses a sophisticated risk-based scoring methodology developed over our more than seven years of lending to small businesses. We verify the specifics of every small business applicant using data from sources such as (but not limited to): ASIC's website, Equifax, bankstatements.com and the Australian Tax Office.

The use of online small business lenders such as Prospa by Australian small businesses is increasing, due to our ability to provide online application processes, timely credit decisions and funding, unsecured finance, repayment flexibility and an excellent customer experience.

## 2. Impact Prospa has on the Australian economy

A recent independent study conducted by RFi Group and the Centre for International Economics on behalf of Prospa, revealed the positive economic impact of Prospa's lending to small business in Australia. See full report here: [https://howto.prospa.com/rs/317-LRS411/images/PRO028\\_EconomicImpactReport\\_FA03\\_Digital.pdf](https://howto.prospa.com/rs/317-LRS411/images/PRO028_EconomicImpactReport_FA03_Digital.pdf).

The research showed Prospa lending between 2013 and 2018 contributed \$3.65 billion to Australian nominal GDP and helped maintain 52,500 annual FTE positions. These findings demonstrate that by providing small business owners with fast, simple access to finance, Prospa is not just directly contributing to its customers' revenue and jobs, but to the wider Australian economy.

## 3. General observations and feedback

Prospa is strongly supportive of the ACCC's efforts to accommodate intermediaries into the Consumer Data Right (**CDR**) framework. Prospa is also of the view that in order for the benefits of open banking reforms to be enjoyed as widely as possible, the reforms should maximise participation across the economy. We believe that adequate and appropriate provision for

# prospa

intermediaries and other third party service providers will ensure that fintechs at all stages of maturity, will be able to participate in the regime and pass on the benefits of doing so to consumers.

We believe that the trust and confidence of consumers and small businesses in the CDR regime is crucial to its successful implementation, universal acceptance and rapid take-up. This requires robust privacy, consent and security safeguards, including the appropriate regulatory oversight of key participants. We believe that, particularly given that the CDR is a novel regime, trust and confidence in the regime can be quickly lost if even a single participant acts in a way that undermines the privacy or security of data or best practices relating to consent.

With this in mind, we recommend that regulatory permissions governing intermediaries, and data recipients that use intermediaries, be modelled as follows:

- The regime should provide for both outsourcing and accreditation models.
- In general, a high level of accreditation should apply to *both* the data recipient and the intermediary. Specifically, they should both be accredited to the same standard.
- An exception should apply to a data recipient that is simply acquiring anonymised data (and not personally identifiable data) from an intermediary. In this case, the data recipient should have access to a lower tier of accreditation. The intermediary should (still) be accredited at a high level in this case.

Prospa generally supports the following positions expressed in FinTech Australia's submission to this consultation:

- The view that intermediaries will adopt a range of business models and will provide a range of services. As such, the regime for them needs flexibility.
- The view that intermediary services generally create economic efficiencies and can increase participation in Open Banking.
- The view that the regime should enable the efficient transfer of CDR data to the overseas offices of Australia fintechs.

Specific comments supporting the position of FinTech Australia will be set out in relation to relevant sections of the consultation paper.

# prospa

Prospa's submission differs from FinTech Australia's submission on three key points:

- We believe that the ACCC's framework for intermediaries should contemplate, in addition to the models set out in FinTech Australia's submission, additional models, including intermediary services that may transfer aggregated, anonymised data (and not CDR data) to the data recipient, as well as intermediaries that may provide 'white-label' services.
- We believe that, in addition to regulating data flows, the regime should include a bespoke consent framework for intermediaries. This should regulate, amongst other things, the flow of a consumer's consent information with respect to CDR data, as between intermediaries and data recipients. This, as well as the rest of the compliance framework, should be tailored and appropriate to the range of possible intermediary models.
- We disagree with FinTech Australia's position that data recipients that acquire CDR data through intermediary services should have access to lower tiers of accreditation. Rather, we believe that only those data recipients that acquire anonymised data should be accredited at a lower tier. Similarly, we believe that transfers of CDR data between accredited persons and non-accredited third parties should also be subject to a bespoke consent and compliance framework, within the CDR regime.

Prospa's points of departure from FinTech Australia's submission will be specified in this submission, in relation to the relevant sections of the consultation paper.

## Part A: Intermediaries

### 4. Question 1: Services provided by intermediaries

***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 and intermediaries can bring to the CDR regime and for consumers?***

In addition to the models set out in FinTech Australia's submission, we note that in some cases, whilst the intermediary service may be *receiving* CDR data, it could be transferring aggregated, anonymized data (and not CDR data) to the data recipient. That is, the intermediary may process

# prospa

data (CDR data, non-CDR data or a combination of both), to generate aggregated, anonymized data or insights, which it then shared with data recipients.

We also note that some intermediaries may wish to provide ‘white-label’ services. These are products or services provided to the data recipient by the intermediary and offered to the consumer under the data recipient’s brand (and not the intermediary’s brand).

Further, some intermediaries may simply facilitate the data recipient’s compliance with the consent framework, for instance by collecting and/or managing consumer consents.

We anticipate that some intermediaries will only collect CDR and/or consumer consents and pass them on, whereas others will both collect and use that CDR data and/or customer consents. For instance, in the case of an intermediary that is transferring aggregated, anonymized data (and not CDR data), we believe that the data recipient should be accredited but should not be subject to the CDR privacy and consent obligations with respect to the CDR data. Those obligations should apply only to the intermediary.

We recommend that the ACCC’s regulatory framework (including the compliance and consent framework) should contemplate these models, in addition to those set out in FinTech Australia’s submission. We have made additional recommendations with respect to the rules that are appropriate for these specific models, in other sections of this submission.

We note that, despite using an intermediary to collect and/or use CDR data and/or consumer consents, data recipients may still need to store and manage consents. This is particularly the case where they need to make multiple uses of CDR data under a particular consumer consent (provided for a period of time not exceeding 12 months). We believe that the points made by FinTech Australia on the economic efficiencies of using intermediaries should be qualified in this regard.

## 5. Question 2: Models for capturing intermediaries

***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.***

In addition to points raised in FinTech Australia's submission, we see a need for appropriate safeguards to be provided for consumers and data recipients where intermediaries are providing the technical infrastructure for compliance and consent.

We have provided specific comments on the application of the accreditation model to the various possible business models, in other parts of this submission. We also reiterate our view that it is crucial that an appropriate and tailored consent and compliance framework be included in the rules for intermediary services.

## 6. Question 3: Obligations that should apply to intermediaries

***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**

We would support an accreditation model which:

- a) requires intermediaries to comply with, at minimum, the obligations that currently apply to 'unrestricted' accredited data recipients;
- b) additionally, requires intermediaries to comply with a bespoke consent framework; and
- c) allows intermediaries to seek a consumer's consent to sell CDR data, as an exception to rule 4.12(3)(a) of the CDR Rules.

We believe that only those data recipients that are acquiring anonymized data should be permitted to have a lower tier of accreditation. We disagree with FinTech Australia's submission in this regard.

- i) Obligations

# prospa

We consider that the risks (in relation to privacy and security of consumer data) 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, evidence of the fact of accreditation should allow them to deal with an intermediary without having to independently satisfy themselves that the intermediary has complied with its obligations.

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.

## ii) A bespoke consent framework

We emphasise that there is a wide range of possible intermediary business models. Some may only provide the technical infrastructure for consent and compliance. Others may provide the technical infrastructure for the data recipient to access CDR data using the data holder's APIs.

We believe that there should be sufficient safeguards in the rules to ensure that a data recipient has accurate and complete consumer consent information pertaining to any CDR data under the data recipient's control, at all times. In particular, where a data recipient's goods or services require multiple uses under each consumer consent, it would be impracticable for the data recipient to have to verify consents with the intermediary prior to each use.

Further, in some cases, it may be most appropriate the consumer to provide consents directly to the data recipient; the data recipient would store and manage consents. In other cases, it may be more appropriate for the consumer to provide consents to the intermediary. The rules should be flexible enough to allow for both options.

These objectives can best be achieved if government creates a bespoke regulatory framework for consents, for intermediaries. It is important that this consent framework is introduced at the same time as any other rules providing for intermediary services (and not at a later stage).

We have commented in more detail on the content of the consent framework in our response to Question 4.

## **(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.

## 7. Question 4: Disclosing the use of intermediaries to consumers

***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.***

### **(A) Notification**

We support FinTech Australia's submission with respect to notification.

### **(B) Consent**

We note our previous comment, in this submission, on the need for a bespoke consent framework for intermediaries.

Specifically, we recommend that the consent framework for intermediaries cover (at minimum):

- An intermediary's duties with respect to the provision of information as to the consumer's consent ('consent information'), as CDR data flows between the intermediary and the data recipient. On this point, we believe that consent information should flow with the data, such that if an intermediary is providing CDR data to a data recipient, the intermediary has a corresponding duty to provide accurate and complete consent information pertaining to that CDR data. It may be appropriate for any non-CDR data (including aggregated, anonymized data) to be carved out of such obligations.
- Related to this, the duties, as between the intermediary and the data recipient, with respect to the consumer dashboard. For instance, the data recipient should have ready access to and control over the relevant consumer dashboard at all times.

The rules should permit consumers to provide consents directly to data recipients. They should also permit consumers to provide consents to an intermediary that is sharing the relevant CDR data with a data recipient.

## 8. Question 5: Disclosure of CDR data between accredited persons

***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.***

We support FinTech Australia's submission in response to this question 5.

## 9. Question 6: Lower tiers of accreditation

***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?***

We believe that only those data recipients that are acquiring anonymised data should be permitted to have a lower tier of accreditation. We believe that the data security and privacy risks that may arise when an entity is integrating with a data holder's open banking API could arise in the same way for data recipients who receive information through an intermediary. This is because the same CDR data, consent and/or consent information would be transferred between an intermediary and data recipient, in the same manner that it would be transferred between a data holder and an intermediary.

For data recipients that are acquiring anonymised data, we agree with the specific options proposed by FinTech Australia in its submission, in relation to the lower tiers of accreditation. That said, we believe that where intermediaries are providing accreditation, the criteria should include that the data recipient is able to understand the nature of the consent(s) given and can store, manage and delete data (to the extent required by the Privacy Safeguards).

We emphasise our view that intermediaries should be subject to a bespoke consent framework, as detailed in other parts of this submission.

## Part B: Disclosure of CDR data to non-accredited third parties

### 10. Question 7: Possible applications

***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.***

We generally agree with FinTech Australia's submission in response to this question 7. However, we note that an online small business lender accessing *business* transaction history, specifically, is an example of how consumers share their banking data with non-accredited third parties. Another example is access to personal accounts and credit card history for responsible lending assessments by consumer finance or buy-now-pay-later providers.

### 11. Question 8: Permissions to receive CDR data

***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?***

We generally agree with FinTech Australia's submission in response to this question 8.

### 12. Question 9: Privacy and consumer protections

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

We disagree with FinTech Australia's submission 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.

We believe that that in some cases, the intermediary service provider may be the accredited person receiving CDR data and the fintech that is engaging the intermediary and using the CDR

data may be non-accredited third party. With this in mind, it is important that the CDR privacy, consent and compliance framework apply to both the collection and use of the CDR data.

## 13. Question 10: Degree of transparency for consumers

***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?***

We disagree with FinTech Australia's submission in response to this question. Given the possibilities set out in our response to question 8, we believe that a bespoke consent and compliance framework under the CDR regime should apply.

Kind regards,



p.p.

Anna Fitzgerald

Group Head of Corporate Relations, Prospa

If you would like more information regarding our submission, please contact:

**Anna Fitzgerald** / Group Head of Corporate Relations [REDACTED] Or

**Deevya Desai** / Regulatory Affairs Manager [REDACTED]