regional australia bank

Consumer Data Right
ACCC Rules Consultation

Response to Draft Rules and accompanying Explanatory Note
(both published 22 June 2020)

19 July 2020

Regional Australia Bank provides this submission in response the ACCC's request for views on the proposed draft Consumer Data Right (CDR) Rules that would authorise third parties, accredited at the 'unrestricted' level, to collect CDR data on behalf of another accredited person.

As the first accredited CDR Data Recipient (DR) and a customer-owned Authorised Deposit-taking Institution (ADI), Regional Australia Bank offers a practical and consumer-centric perspective on the proposed changes. We appreciate the opportunity to contribute to this important discussion and welcome further dialogue on the topic.

While CDR will ultimately serve multiple sectors of the economy, it is today still restricted to the financial services sector. Effort has been made to consider the needs of other sectors within this submission however, it is primarily written from the perspective of a Financial Services organisation, specifically as an ADI and an accredited DR.

1. Context

Although it is not stated in the Explanatory Note, it is assumed that the proposed inclusion of intermediaries within the Rules is, at least in part, intended to facilitate and accelerate broadened and more diverse participation in the CDR. This would assist with the over-arching principles identified in the 2018 Farrell Report, specifically that Open Banking should encourage competition, be customer focussed, efficient and fair and create opportunities.

Today, the accreditation bar remains high, effectively presenting a barrier to entry for smaller organisations wishing to participate as Data Recipients.

The proposed changes to the Rules would permit intermediaries with no direct consumer relationship to operate within the CDR ecosystem on behalf of an ADR. This would provide real and immediate benefit for smaller ADIs who could avail themselves of the current streamlined accreditation process with relative ease. These ADRs would be able to use the CDR infrastructure and services of an accredited intermediary acting as a Provider to them (the Principal), while they retain the direct consumer relationship.

However, the majority of ADRs will not be ADIs. Therefore, the CAP arrangement cannot reasonably be viewed as something that will facilitate and accelerate broadened participation on its own. To achieve this objective, a simplified or lesser form of accreditation, potentially a series of accreditation tiers, may be required.

2. Accreditation

There is currently only one defined level of accreditation. Tiered accreditation implies levels of access to CDR data, although accreditation could also be restricted by type and sensitivity of data. Alternate dimensions, such as industry or economic sector, might also be worthy of consideration as accreditation differentiators.

While the observations and comments in this submission relate primarily to the proposed CAP arrangements, it is suggested that tiered accreditation should also be addressed at this time, particularly if increased participation and the associated economic and consumer benefits of that are deemed a priority.

A word of caution is also offered on the matter of blanket or unrestricted levels of CDR accreditation. While ADIs may be trusted to handle financial data in a secure and appropriate manner, their detailed knowledge of the nuances of energy and telecommunications sectors will likely be incomplete. This may present some consequential risk to those additional sectors. The same principle applies in reverse; energy or telecommunications providers may not be familiar with financial data management matters, such as PCI DSS.

Recommendation:

- Prioritise definition of rules for tiered accreditation
- Recognise the nuances of cross-industry accreditation
- Consider type and sensitivity of data as accreditation differentiators

---

3. Transparency Mechanisms for Consumers

Under current rules, if they elect to use an Outsourced Service Provider (OSP), DRs are required to identify that fact in their CDR policy, naming the OSP and the role they have in the CDR arrangement. It would seem appropriate to also require that DH and DRs extend this publication obligation to include any active CAP arrangements.

Participants will need to make modifications to their CDR Policy documents to reference CAP arrangements where these are used. To diminish the comprehension burden on consumers, it would seem appropriate to provide this information alongside existing OSP details in the same section, perhaps entitled Third Party Arrangements.

The explanatory notes indicate that a consumer should additionally be shown the name and accreditation number of a Provider under a CAP arrangement (and presumably also be provided some associated contextual copy). There is already a significant cognitive load placed upon consumers as a result of the current pre-consent and consent processes. There is a point at which consumers view these processes as overly burdensome and simply skip over or bypass the content, missing

out on the information that is intended to protect them. Worse still, confidence in the ecosystem is diminished in favour of simpler sharing mechanisms such as screen-scraping. We caution further adding to this load.

Will this additional obligation be worthwhile? Will it provide any further value to the consumer? From their perspective, they have a relationship with the Principal, and should they require more detail, they could find information on CAP arrangements described within the DR CDR policy.

The expectations on consumers are already high with DH, DR, Consumer and OSPs, without adding Principal and Provider under CAP arrangements. Perhaps this needs to remain an obligation on DRs but not be publicly communicated.

Recommendation:

- If CAP arrangements are to be communicated, do so via the CDR Policy
- Group CAP and OSP arrangements together as Third Party Arrangements
- Avoid further burdening consent messaging with reference to CAP arrangements
- Consider if there is any value in communicating CAP arrangements to consumers

---

4. Dashboard Implications

The explanatory notes indicate that changes will be required to the consumer dashboard where collection has been facilitated by a Provider. This will also require additional and prescriptive updates to the current CX Guidelines. The date of February 2021 seems achievable, although it should be recognised that software development companies and potentially core banking Providers may have already built (and are no doubt attempting to deploy to their clients) dashboard products that will not yet have this capability.

This further serves to illustrate a disadvantage of the distributed consumer dashboard architecture. While there are challenges associated with creating a single consumer identity, an alternate centralised consumer dashboard would provide consumers with a single location from which to administer all their consents. This would also enable the multiple inevitable evolutionary adjustments to Rules to be accommodated and deployed more readily and consistently.

Recommendation:

- Update CX guidelines with prescriptive details on disclosure of CAP arrangements
- Reconsider the benefits of a centralised consumer dashboard architecture

---

5. Liability

Australian ADIs are regulated under CPS 231 – Outsourcing. This standard governs outsourcing arrangements involving material business activities entered into by an APRA-regulated institution. Under this prudential standard 'All risks arising from outsourcing material business activities must be appropriately managed…'.

Consistent with these outsourcing arrangements, CDR liability rests with the Principal as an accredited person. Therefore, under a CAP arrangement, one might question the need to place onerous accreditation obligations on the Provider when no additional protection is afforded. It is in the interest of the Principal to ensure that they only engage with capable Providers.

Extending this thought process, an ADI is today able to use services from any public or private cloud provider. Many smaller ADIs use such providers to manage core banking activities. The risk and obligation rests firmly on the ADI to ensure any such outsourcing arrangements are appropriately structured, especially in respect of information security, privacy, operational stability, performance and risk.

Should an ADI become an ADR, the applicable minimum information security controls in Schedule 2 of the Rules would also apply (under CPS 231) to any outsourcing arrangements they have in place, including CAP arrangements. Once again this suggests that placing additional formal CDR accreditation obligations on a Provider may be unnecessary, at least where the arrangement is with an ADI.

Where the Principal is not an ADI, it still seems wholly appropriate that liability should rest with them, even when using the services of a Provider. The Provider would need to demonstrate how their services enable the Principal to meet their CDR obligations.

The requirement to issue a receipt to consumers who have provided consent offers an example of how this might work in practice. Under the proposed CAP rules, both the Provider and Principal are responsible for sending the receipt, yet liability rests with the Principal. Rather than attempt to define dual responsibilities, the Principal may select a Provider that is able to deliver this service on their behalf. An appropriate legal agreement would be in place, the scope of which may include publication of performance metrics and testing and reporting of controls effectiveness, to ensure obligations continue to be met.

A small number of specialist CDR providers will be motivated to build resilient and richly featured functionality. At scale, this would be economically viable. Equivalent capability is unlikely to be viewed as a justifiable investment for an individual DR.

Recommendation:

- Reconsider the requirement for a Provider to be accredited
- Clarify that a Principal always bears all liability
- Require Principals to have outsourcing arrangements in place with Providers
- Consider certification of Providers rather than onerous accreditation
- Consider annual ASAE3402 (or equivalent) certification for Providers

6. Affiliate Data Recipient Option

If the prudential regulator is comfortable that an ADI is able to use a banking licence to allow a third party fintech to offer direct-to-consumer products and services under a B2B arrangement, would it not be reasonable to allow that same ADI to extend the scope of those services to encompass CDR data?

Once accredited, could a DR allow carefully selected partner organisations to benefit from their accreditation through an affiliate service, without that partner organisation having to achieve full accreditation at the unrestricted level?

The risk and obligation for this model would remain with the ADI, but a new accelerated pathway for fintech and other third-party access to CDR could be provided through the accreditation of a bank partner.

Just as a bank remains responsible for KYC and information security today, the bank would similarly need to ensure that any third-party handling CDR data, did so appropriately, adhering to the Rules. In fact, the bank may choose to impose its own tiered CDR consumer data access policy, in keeping with its own risk appetite.

This approach could allow lower-risk consumer data such as a balance of a single account, to be consumed by a third-party business without the requirement for that business to become accredited at the unrestricted level.

It is possible this could be extended to other sectors of the economy, however the immediate, pressing need from fintech seeking simplified participation into the CDR ecosystem appears largely unique to financial services.

Recommendation:

- Enable ADRs to offer affiliate CDR participation to selected partners
- All liability rests with accredited data recipients
- Potentially combine with participation as a certified recipient with low risk data

7. De-Risking of Intermediary Participation

The proposed adjustments to the Rules, and the requirement for a Partner to achieve unrestricted accreditation to operate as an intermediary, seem largely founded on the assumption that intermediaries are able to access the CDR data they are collecting on behalf of an ADR.

While this assumption is valid with the current CDR architecture, there is an alternate option that could reduce the risk of an intermediary accessing CDR data. Potentially this could also lower the bar for intermediary participation in the ecosystem.

If the CDR ecosystem supported a similar concept to the world wide web (HTTPS/TLS) where the recipient (browser) and the holder (server) used public key encryption to encrypt the data between holder and recipient, then the intermediary would not be able to access the data.

A workable solution would likely still require metadata to remain visible to the intermediary. Items such as API endpoints being requested, the target data holder, consent authorisation details (for managing consent lifecycles) and attributes required to be used within a dashboard would all be visible to the intermediary, but the actual CDR data itself would only be visible to the accredited holder and the recipient.

With such protections in place, and a subsequent reduced accreditation effort, the barrier to entry for intermediaries would be significantly lower, and broader participation may be more readily achieved and accelerated. Some intermediaries may still wish to become accredited so they can offer value-add services using CDR data. This option does not preclude that.

This would not be a trivial adjustment to the CDR ecosystem. Such a solution would need the DR to incorporate some specific technology to be able to handle the encryption/decryption independently of the intermediary. However, in relative terms, this would be a small effort compared to implementation of the entire ADR stack and one that could be solved through the release of open-source software solutions. Now would be the time to consider such an option, before CDR adoption becomes more widespread.

Recommendation:

- Consider de-risking the role of intermediaries via an adjusted ecosystem design
- Consult with CDR stakeholders to determine appetite for such a change

Head Office
Technology Park, Madgwick Drive, Armidale NSW 2350
PO Box U631, University of New England NSW 2351
Telephone 132 067 **Email** enquiries@regionalaustraliabank.com.au
Web regionalaustraliabank.com.au