Consumer Data Right
ACCC Consultation on proposed changes to the CDR Rules

Response to consultation paper

29 October 2020

We appreciate the opportunity to contribute to this important discussion and welcome further dialogue on the topic.

https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-cdr-rules

As an accredited Data Recipient (DR) and a customer-owned Authorised Deposit-taking Institution (ADI) with Data Holder (DH) obligations, Regional Australia Bank is uniquely positioned to offer a balanced, practical and consumer-centric perspective on many of these proposed changes.

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 and specifically, as an ADI.

Rather than respond to every consultation question posed, we have elected to comment only on matters where we feel qualified to provide an opinion, and have prioritised responses to proposed Rule changes that appear to have potential material impact on participants, consumers, or the overall CDR ecosystem.

Q01	We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

While the setting of timelines will be contentious, we believe it is important that the rollout of CDR does not extend unnecessarily. Significant time has already elapsed and lack of appetite for further change, recently voiced by some ADIs, is not necessarily reflective of consumer sentiment, or the stated desire of government to foster innovation and competition to fuel the digital economy.

Concerns have already been raised by representatives of some ADIs that implementation of the existing Rules is challenging enough, and that further change might be too much at this time. We accept this view, but do not subscribe to it.

Appetite exists for those who recognise the strategic value of CDR, and Regional Australia Bank is not alone as an ADI aiming to publish Consumer data in advance of legislative obligations.

Existing and prospective ADRs, primarily fintechs, have lobbied effectively and are keen for many of these new rules to be made. With the barrier to entry currently too high for some, their participation is effectively stalled until new rules are adopted.

If an ADI is in the process of developing a DH solution right now, it could be more efficient to employ resources to do so once, on a single set of updated rules.

There would be more work (and risk) associated with building to the current standard and then subsequently having to retrofit a production platform to accommodate new rules, update processes, policies, frameworks, consumer dashboards, consumer agreements and other operational assets.

A partial solution to this tension might involve prioritising implementation of rules that do not require any further action by Data Holders, but which open up participation to new ADRs. These include restricted accreditation options and simplified information security obligations covered in Section 3 of the consultation paper.

Independent ecosystem service providers are now offering solutions that can directly assist with, and accelerate, DH participation. DH PaaS offerings are available in the general market, indeed several ADIs were recently able to use these to publish PRD ahead of schedule. The ACCC and the DSB could publish a directory of such services to broaden awareness of them without endorsement. This could provide a rapid ecosystem knowledge uplift and diminish the perceived burden on DH participation.

It is also worth noting that the resource constraints many smaller ADIs are impacted by, are offset to some degree by the simpler core banking system architectures they use. There is little difference in publishing consumer data for individual transaction accounts and loan accounts stored in the same underlying database. The need for an additional 4 months between publication of Phase 1 and Phase 2 products is therefore questionable for many ADIs.

Perhaps therefore, a compromise could be struck with lower-tier ADIs to compress or combine these phases to create capacity while still achieving overall delivery within original published timelines.

While implementation of many of the proposed rules would not directly impact DHs, there would appear to be significantly more complexity associated with items explored in Section 6 of the consultation paper. The expanded scope for management of authorisations and dashboards associated with extending the CDR to more consumers may require more lengthy development time.

Recommendation:

- Accelerate implementation of rules that facilitate broader ADR participation
- Prioritise rules that have limited impact on DHs
- Assist DHs in accessing CDR solution providers through a published directory
- Consider compressing the product phasing table timeline to create capacity

---

Q02	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.

These creative options certainly provide for improved flexibility, and would likely encourage more organisations to become ADRs, broadening ecosystem participation with consequential availability of improved consumer outcomes.

We found understanding and then differentiating between the different kinds of restricted accreditation proposals challenging. It was not a straightforward exercise, and this could impact market awareness and diminish the appeal for some.

This issue could perhaps be addressed by developing an accompanying Rules Interpretation Guide that provides overarching context. This context could explain that in order to access CDR data, organisations must become accredited and that there are a number of options available. Where accreditation relies on a third party, a CAP arrangement will need to be in place etc.

Appropriately positioned, the various options do have merit and responses are provided for each further on in this submission.

Recommendation:

- Implement simplified / tiered / alternate accreditation options
- Develop Guidelines to assist with comprehension

Q03	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.

We are cautious of endorsing volume-based restrictions as a lower form of accreditation. Such an approach may create problems. Carefully designed controls would be necessary if hard data volume limits were to be implemented. Without such controls, ADRs may be working with partial datasets and incomplete information that could produce inaccurate recommendations, and result in inappropriate services being delivered to consumers.

Another potential accreditation option would be to restrict a DR to data related to an industry or economic sector. While ADIs are 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, yet current roles permit unrestricted access through the streamlined accreditation process. This may present some consequential risk to those additional sectors. The same principle also applies in reverse; energy or telecommunications providers may not be familiar with financial data management matters, such as PCI DSS.

Of course, one of the significant benefits of CDR over narrower Open Banking regimes such as the one now established in the UK, is the prospect of economy-wide access to consumer data. Creating industry accreditation silos would diminish the scope of potential use cases that could otherwise provide significant consumer value.

Perhaps this is where the proposed risk-based restriction in section 3.1 has particular merit. It could enable access to data across multiple industries or sectors, yet ensure that the highest-risk attributes of consumer data are only accessible to those adequately equipped to manage it.

There would appear to be some risk in offering multiple restricted accreditation options for ADRs. Aside from 'too much choice' and potential market confusion, there would be additional administrative burden placed upon the regulator, maintaining sector attribute risk ratings, overseeing compliance, and keeping pace with an ever-evolving ecosystem.

Recommendation:

- Assess the implication of volume-based restrictions carefully
- Recognise the nuances and risks of cross-sector accreditation
- Consider risk-based restrictions in combination with cross-sector accreditation
- Bear in mind the consequences of offering too many accreditation options

---

Q07	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

The data enclave restriction appears complex and although it has presumably been designed to meet a specific use case, it is not clear to us precisely what that might be. The associated capability of this restricted level of access is also not immediately clear through use of the 'enclave' label, which is not a commonly used term.

Would it not be possible to achieve the same outcome through an Outsourced Service Provider (OSP) with an associated CAP arrangement? The ADR achieves Indirect accreditation as a consequence of the OSP's unrestricted accreditation. Interaction with the DHs is undertaken by the OSP and all data remains within OSP systems.

A simpler term for this type of arrangement might therefore be 'Indirect OSP accreditation'.

This indirect/direct concept could also contribute to a Class of accreditation that could then be combined with the Data Access Level to form a simple accreditation matrix.

Such a matrix may assist with communication of the accreditation options to prospective ADRs.

In the table below, the cell shaded in green is the only scenario where an ADR would be accredited at the unrestricted level, all other combinations are a form of restricted accreditation with lower barriers to entry.

		Data Access Level	
		Limited	**Unlimited**
Accreditation Class	**Direct**	Collect and use limited data from DHs directly. Liability rests with ADR.	Collect and use any CDR data from DHs directly. Liability rests with ADR.
	Indirect Affiliate	Collect and use limited data from DHs indirectly through an accredited Sponsor. Liability rests with Sponsor who attests to capability of Affiliate	Collect and use any data from DHs indirectly through an accredited Sponsor. Liability rests with Sponsor who attests to capability of Affiliate
	Indirect OSP	Collect and use limited data from DHs indirectly through an accredited OSP under the terms of a CAP arrangement. Liability rests with ADR who attests to their own capability using an accredited provider.	Collect and use any data from DHs indirectly through an accredited OSP under the terms of a CAP arrangement. Liability rests with ADR who attests to their own capability using an accredited provider.

Potentially, this does raise the question of whether an indirect accreditation sub-class is actually required. Arguably, a sponsor-affiliate arrangement could be catered for through an OSP arrangement. Consequently, there would need to be some material difference in order to warrant a separate affiliate model.

Perhaps justification for a separate affiliate option stems from the associated accreditation process. This could certainly be more streamlined and less onerous than an OSP or direct accreditation arrangement, and would be reflective of the increased level of risk the sponsor is taking in return for the direct arrangement with the affiliate.

On balance, we believe there is merit in offering independent OSP and affiliate arrangements, however, if this was not to be the case, the accreditation options could be further simplified as follows

		Data Access Level	
		Limited	**Unlimited**
Accreditation Class	**Direct**	Collect and use limited data from DHs directly. Liability rests entirely with ADR.	Collect and use any CDR data from DHs directly. Liability rests entirely with ADR.
	Indirect	Collect and use limited data from DHs indirectly through an accredited OSP or Sponsor under the terms of a CAP arrangement. Liability rests with ADR who attests to their own capability and use of an accredited provider.	Collect and use any data from DHs indirectly through an accredited OSP or Sponsor under the terms of a CAP arrangement. Liability rests with ADR who attests to their own capability and use of an accredited provider.

A class of accreditation that permits the collection of CDR data to be undertaken by an accredited OSP would certainly be helpful, and encourage participation from smaller organisations. Any banking use case could then be considered by any organisation, levelling the playing field and increasing competition whilst still ensuring the safety and integrity of the ecosystem.

Recommendation:

- If retained, reconsider the labelling of the enclave accreditation option
- Consider a simplified set of accreditation options that provide access to limited or unlimited CDR data either directly or indirectly via an OSP or Sponsor

---

Q10	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 an ADI, we like and support the concept of affiliate accreditation, and believe it enables an important emerging service model whereby established institutions offer wholesale services to fintechs. The existing due diligence undertaken by banks, who take on regulatory risk through such partnerships, is significant, enabling them to confidently attest to the capability of an affiliate and retain liability for their conduct.

If liability does rest with the sponsor, this model would encourage fintechs to accelerate accreditation through partnership with an ADI under a trusted commercial arrangement, leveraging the ADI's existing accreditation and potentially removing the need for a further CAP arrangement. It is in the interests of the sponsoring ADI to

ensure that the affiliate complies with an extensive set of contractual requirements in order for them to retain their good standing as an unrestricted ADR.

In fact, the bank may choose to impose its own tiered CDR consumer data access policy, in keeping with its own risk appetite.

An annual attestation cycle would seem appropriate for such an arrangement and would fit well with existing prudential regulatory obligations of an ADI such as CPS 234 (Information Security), CPS 231 (Outsourcing) and CPS 220 (Risk Management).

In practical terms, under this model the affiliate would develop a consumer-facing application that called private end points exposed to them by the sponsor. Valid requests made by the affiliate of these end points, would in turn trigger subsequent requests of the relevant DH endpoints by the sponsor's DR platform, and resultant CDR data would then securely flow to the affiliate.

Although the sponsor will provide the underlying CDR infrastructure services, these are largely invisible to the consumer who has a relationship with the affiliate. The sponsoring ADR would therefore need to record the affiliate name and any associated CDR software applications under a sub-brand of the sponsor on the CDR register. This would ensure that the affiliate name is displayed during the DH authentication and authorisation processes, and in the DH and DR consumer dashboards.

Recommendation:

- Proceed with establishment of Rules to support streamlined affiliate accreditation
- Permit sponsors to register affiliate brands and associated software applications on the CDR register to benefit consumers

---

Q11	Should there be additional requirements under Part 1 of Schedule 2 for sponsors?

The obligations defined under 2.2(7) for a third-party management framework would appear to cover the high-level conditions well. We don't foresee the need for further requirements.

Q12	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?

Our interpretation is that incident management and other operational procedures necessary for compliance with ecosystem obligations would all be included as part of

the third-party management framework defined in proposed Rule 2.2(7) of Schedule 2. We have not identified a need for any additional requirements beyond this.

Q13	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.

While we recognise the intent to create more flexibility around accreditation, creation of additional sub-classifications may introduce undesired complexity and confusion.

The simple accreditation matrix suggested as part of our response to question 7 above does accommodate different levels of access to data while also recognising variations in associated assurance obligations.

Our understanding of the proposed affiliate model suggests that ultimate responsibility for conduct rests with the affiliate. This would not appear to reflect the inherently close and deep business partnership formed between an affiliate and sponsor, often over an extended period of time. This is in contrast with the more commercially minded, commodity-based service relationships that an ADR might have with an OSP.

Recommendation:

- Recognise the inherent conduct assurance and associated risk mitigation provided through the close nature of an affiliate-sponsor business partnership.

Q14	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.

We agree that the party with the immediate and direct consumer relationship should be responsible for delivery of customer-facing aspects of CDR. The consumer would expect this, indeed, they may be confused or concerned if the name of a different entity (the provider) was presented to them or referenced in communication.

The branding, communication style and tone of voice used by the provider would likely differ significantly from that of the principal, potentially leading to eradication of consumer trust in the CDR ecosystem if it were to be favoured.

This matter could be potentially further complicated where the principal is consuming white labelled financial products and services from an ADI acting as a provider under a CAP arrangement. The prudential regulator would view the ADI (the provider) as having ultimate accountability for product service and customer conduct. The subtle difference between consumer relationship and accountability might benefit from further definition.

Recommendation:

- Communication with the consumer should come from the entity that has the direct consumer relationship
- Distinction between a consumer brand relationship and the entity with ultimate accountability for customer and service conduct may be required

---

Q35	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).

We support the proposed separation of consents for collection and use of CDR data and the associated benefits this will bring in terms of more flexible use case design and consumer trust. However, a note of caution and an associated request accompanies this support.

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 this as overly burdensome and simply skip over or bypass the content, missing out on 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.

The draft wireframes published at https://miro.com/app/board/o9J_kk5E-AY=/ provide insight into how a potential CX might accommodate separate consents. This looks encouraging, and if this proposed change is adopted, we encourage authors of the CX guidelines to permit a single combined consent action where the duration of both collection and use is the same.

This seemingly minor concession could help avoid the consumer frustration we have identified in our current CDR online lending use case, where a single consent action to select multiple data clusters is not permitted, even though the use case is not valid without all clusters.

Recommendation:

- The updated rules should support independent collection and use time periods
- CX guidelines should permit a single consent action where collection and use timeframes are the same
- CX guidelines should consider permitting a single consent action, irrespective of collection and use timeframes

---

Q41	We are seeking feedback on whether the proposed amendments place the obligation on the party best placed to meet the obligation.

We agree that white label products should be included in the CDR regime and we concur that the contractual relationship with the consumer generally rests with the white labeller.

There is also potential for non-ADIs to offer white labelled products and services and market these using their own brand. For example, a fintech may offer a transaction account under a BaaS relationship with an ADI. The fintech is the brand with whom the consumer interacts, while the ADI sits underneath and carries the contractual banking relationship.

While the consumer knows the brand, they may be unfamiliar with the underlying white labeller. This presents an issue if the consumer subsequently wishes to share their associated banking data, or is searching for product information using CDR. If the fintech brand is strong, they may search for that brand as the DH rather than the lesser known (to them) white labeller that is actually responsible for the underlying bank account.

Similarly, when providing consent to share data, the consent flow, authentication and authorisation dialogue may need to accommodate a combination of the white labeller and brand names in order to accurately reflect the data exchange and align with a consumer's perspective on where their banking relationship sits.

We see a growth in scenarios like this and the need to accommodate entries for potential DH brands brought about through BaaS and other white label partnerships.

Recommendation:

- Accommodate customer-facing brands offering white label products in consumer dashboards and consent flows

---

Additional Observations and Thoughts

CDR Policy adjustments

These will need to be considered and potentially, policies will be required to contain information on the level and type of accreditation an ADR is operating under. If an affiliate or OSP model is used to gain and maintain accreditation, this point of difference may be important to a consumer.

Accreditation Badge Adjustments

Should consideration be given to the style of the ADR Accreditation ID and CDR logo for different classes of accreditation? Should the consumer be made aware visually, that they are dealing with an ADR accredited at the restricted or unrestricted level?

Participation Accelerators

Given that many ADIs appear uncomfortable with the prospect of further changes to the rules and the associated demands that implementation would impose on them in terms of resource, it may be beneficial to offer them additional support.

Anecdotally, much of the concern raised to date seems related to the matter of reviewing, understanding and then acting upon, interpretation of the new rules. This concern could perhaps be at least partially addressed if the ACCC were to provide a dedicated support team staffed by rules, standards and CX experts, available at short notice to assist DHs in an informal manner.

In addition to on-demand support, DHs could schedule calls with subject matter experts and a knowledge base could be developed to build on the current DSB CDR Support Portal. Collaboration tools such as those favoured by the initial CDR participants, could be made available and access extended to a broader group.

This extensive support resource could be made available free of charge as an incentive to participants. Limiting access to a defined time period, perhaps 6 months, could encourage earlier engagement and participation, elevating comprehension, removing fear of the unknown and enabling challenging timelines to be viewed more favourably .

Recommendation:

- Consider whether information on the class of accreditation achieved by an ADR should be included within their CDR Policy
- Consider if the accreditation ID and CDR logo should reflect the class of accreditation achieved by an ADR
- Provide an extensive range of support services free of charge to DHs for a limited time as an incentive to embrace the new rules and accelerate participation.

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