Commonwealth Bank

Group Submission to the proposed CDR Rules amendments (version 3)

30 July 2021

1. Introduction

The Consumer Data Right ('CDR') is a reform that has the potential to drive significant economic benefits for Australian consumers for decades to come. As one of the first organisations to deliver the CDR for our customers, and as the first major bank to become an Accredited Data Recipient ('ADR'), the Commonwealth Bank (CBA) is committed to building trust in the regime and maximising its benefit for all Australians.

CBA re-affirms its view that for the CDR to deliver positive outcomes and increase benefits to consumers, the Rules, Standards, and implementation approach must prioritise data security and customer privacy rights.

The primary consideration of the CDR regime must be ensuring that consumer trust and confidence in the regime is not reduced through a weakening of the consumer protection mechanisms in the CDR framework. This means ensuring:

1. consumer data is protected appropriately by robust security practices;
2. privacy protections are retained at every step in the process;
3. consumer consent is voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn; and
4. appropriate controls, oversight, monitoring and governance of entities collecting, holding, and transmitting CDR data is conducted.

These guiding principles were agreed for the implementation of Open Banking, and should be maintained moving forward. In considering proposed amendments to the CDR Rules, the Commonwealth Bank believes that the additional following common principles should be adhered to:

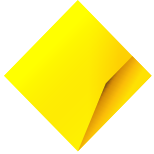
Firstly, CDR reforms should result in Australians and Australian businesses being better off. This means making sure solutions provide consumers the productivity benefits associated with greater access to data without increasing their exposure to misuse or mishandling of data. To achieve this, reforms must be designed with a view to raise consumer awareness and place consumers in control over access to their data.

Ensuring customer data can only be accessed through the CDR in a manner that puts consumers in control and provides them with both privacy and financial protection will be critical to ensuring both uptake of the regime and the reduction of poor consumer outcomes that result from non-permissioned use or inadequate operational processes. Amendments to the established accreditation system and consent model to increase ADR participation in the CDR regime should not be to the detriment of consumer protections or the safety and security of the regime.

Secondly, CBA is firmly of the view that the CDR's data sharing framework should be based on principles of safety, security, and reciprocity. Participants seeking access to consumer data should be prepared to (i) meet high levels of operational integrity and (ii) be prepared to share data when requested by consumers.

Thirdly, the current implementation of Open Banking is critical to build consumer and participant confidence in the safety, stability, and resiliency of the ecosystem. Further, allowing screen scraping to continue alongside the Open Banking regime will result in 'dual schemes' remaining in operation, to the detriment of consumers as well as take up and participation in the broader CDR regime. Increased planning and coordination across the distributed governance structure of the CDR is required to support the development and implementation of a robust, secure, and consumer-focused CDR regime and ecosystem.

The proposed amendments introduce a complex set of new roles associated with tiered accreditation (e.g. sponsor-affiliate, CDR Representatives etc.); new non-accredited participants (e.g. Trusted Advisors, CDR



Insight Recipients, unaccredited OSPs); and reverses the current express consent model (i.e. changing to an opt-out, or default pre-approval for joint accounts). The complexity and material risks of introducing this reversal to core tenets of the CDR cannot be understated, and the simultaneous introduction of these proposed changes to the regime will considerably increase the overall technical complexity of the ecosystem. There are substantial functional, security and customer experience design challenges to be solved in order to make the proposed changes feasible.

Reciprocity obligations are fundamental for consumers, innovation and competition

For the consumer benefits of the CDR to be fully realised, it is critical that ADRs participating in the CDR regime are subject to reciprocity obligations. This will ensure all ecosystem participants can compete and innovate, without a distortion of the competitive landscape.

Before introducing new tiers of accreditation for entities that may not be able or willing to meet the existing accreditation requirements, we recommend adopting the recommendation of the *2017 Final Report for the Review into Open Banking in Australia*[1] that all ADRs who wish to ingest CDR data be subject to reciprocal obligations as a part of the minimum accreditation criteria (regardless of whether they fall within a designated sector). That is, once an entity applies to become an ADR, the ACCC as Data Recipient Accreditor would conduct a review to consider whether the company collects any datasets that may be considered 'equivalent' that should be subject to a reciprocal data obligation. We also recommend a general exemption for these reciprocity obligations for start-ups and small businesses, as defined by the 2021 Banking Code of Practice, to ensure the barriers to entry are not prohibitive.

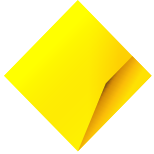
The principle of reciprocity is fundamental to the CDR regime's ability to promote innovation and to maximise the benefits of the regime for consumers. Limiting the CDR regime such that it only enables consumers to share their data from Data Holders to ADRs (but not similarly requiring ADRs to send data the other way in response to a consumer's request) will considerably lessen the opportunity for consumers to leverage the full potential of data sharing. There would be significant benefit for consumers if they were able to choose to exchange their data between Data Holders and ADRs; however, currently there is no reason for companies in non-designated sectors to enable this consumer benefit.

2. Increasing pathways to participation

CBA supports a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with read access activities, without relaxing the existing obligations concerning security, privacy, and consumer consent.

To accelerate the creation of a safe and efficient ecosystem, consumers must have confidence in the security of the ecosystem and its participants. The accreditation model should be treated as the single most critical process within the CDR regime in ensuring the safe and secure sharing of CDR Data. The instantaneous nature of data sharing via Application Program Interfaces ('APIs') within the CDR regime means that a consumer's sensitive CDR data can be requested and shared within a matter of seconds and there is no opportunity to recall an erroneous data share. Consumers and participants rely on the accreditation model to have confidence that recipients of CDR data have been appropriately 'vetted' as suitable entities to handle CDR data.

[1] Australian Government, Final Report, Review into Open Banking in Australia, December 2017, Recommendation 6.6 (available at https://treasury.gov.au/consultation/c2018-t247313)



The objectives of increased competition and innovation must be carefully balanced with the need for adequate consumer protections and information security. We support the CDR being developed with the appropriate safeguards in place to minimise the exposure of all consumers to potential breaches of their privacy and fraud. However, we are concerned that the proposed draft rules do not provide the minimum information security controls and privacy safeguards required for consumers to safely and securely share their CDR data.

CBA is firmly of the view that the transfer of CDR data must be governed by technical data standards. We recommend that entities who wish to handle CDR data (i.e. Affiliates, CDR Representatives, OSPs and Trusted Advisors) are subject to the existing information security standards of the CDR for the transmission and storage of CDR data. It is vital that all links in the chain of custody for CDR data have the same levels of protection. Without end-to-end security standards being mandated, the security and privacy of the CDR data cannot be guaranteed. We support the proposed draft rules which require Affiliates to be subject to all of the CDR Privacy Safeguards. We recommend an independent Privacy Impact Assessment is conducted and considers which Privacy Safeguards should apply to CDR Representatives, OSPs and Trusted Advisors.

3. Disclosure to Trusted Advisors

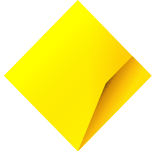
CBA is not supportive of the transfer of CDR data to non-accredited persons. The proposed draft rules reflect a fundamental departure from the findings of the two expert reports to Government on the CDR regime. It is a core tenet of the regime that CDR Data can only be received by Accredited Persons who are subject to the CDR Rules, Standards, and Privacy Safeguards.

The significant privacy and security risks of allowing disclosures of CDR data to non-accredited persons via the CDR regime negate the potential benefits provided to consumers. Allowing CDR data to be disclosed to non-accredited persons risks undermining the consumer protections that the CDR accreditation process is designed to provide.

CBA is firmly of the view that if Accredited Persons were able to transfer data to non-accredited persons, even where directed by a consumer, this would weaken the integrity and trust in the CDR regime. This is due to non-accredited Trusted Advisors not being required to comply with the CDR Rules, Standards or Safeguards. We are pleased to see that the proposed draft rules state that the transfer of CDR data from an ADR to a non-accredited Trusted Advisor is covered by the information security controls in Schedule 2 of the CDR Rules. However, we note there are no obligations regarding how the consumer's CDR data is stored once received, which will increase the risks of loss or unauthorised access and disclosure. CBA does not support this proposed change to the level of information security required to handle consumers' banking data.

Critically, there is a material risk that consumers will not understand or be appropriately made aware that their data will no longer be subject to the protections within the CDR Rules, Standards and Privacy Safeguards. Further, the proposed classes of Trusted Advisors may not have any obligations under other privacy legislation, such as the Privacy Act 1988 (including the Australian Privacy Principles).

In the event Treasury proceeds with amendments to enable disclosure of CDR data to non-accredited persons, CBA recommends further consultation with industry and consumer groups to address the concerns raised in the 2020 Maddocks Privacy Impact Assessment (2020 PIA). For example, CBA agrees with the 2020 PIA that the CDR regime should prevent participants from operating as mere conduits for CDR to non-accredited persons and would recommend that only the Data Holder for the CDR banking data be enabled to securely provide access to specific professional classes, with consumer consent. This would mitigate the risk of predatory behaviours towards consumers without placing a threshold burden on the



consumer to obtain an unnecessary good or service. Alternatively, other non-CDR methods of secure read-only access could be considered.

If the proposed draft rules proceed, we recommend CX Standards apply to Trusted Advisor disclosure consents, and that these CX standards explicitly advise consumers that they will not have the same rights or protections as consumers who share their CDR data with unrestricted ADRs. This is an important disclaimer, as under the proposed draft rules there is no Privacy Safeguard obligation for Trusted Advisors to delete or de-identify the consumer's CDR banking data; nor any information security obligations for how the consumer's CDR banking data is stored. As noted above, we recommend an independent Privacy Impact Assessment give consideration to which Privacy Safeguards should apply to Trusted Advisors; and recommend that entities who wish to handle CDR data (such as Trusted Advisors) are the subject to the information security standards of the CDR for the transmission and storage of CDR data.

4. Disclosure of CDR Insights

The proposed rules would permit ADRs to disclose an Insight derived from a specific individual's CDR data to any person outside the regime (i.e. a non-accredited Insight Recipient) with a consumer's consent.

We note the 2020 PIA finding that *'CDR insights contain information that is more sensitive than raw CDR Data alone'* and *'may be as, or more, invasive than sharing a CDR consumer's raw CDR Data'.*[2] The 2020 PIA also notes vulnerable consumers may be pressured into disclosing insights or may not otherwise fully understand the negative consequences that their consent to disclose could have.

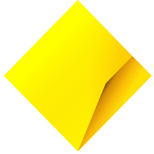
We would welcome further consideration of whether it is appropriate for CDR Insights to be generated and disclosed as part of the CDR regime, with specific consideration given to how risks to vulnerable consumers can be mitigated.

Should the proposed draft rules to enable disclosure of CDR Insights to non-accredited Insight Recipients proceed, disclosures of CDR Insights should be limited to derived CDR data only and should exclude any 'raw' CDR data. We are supportive of specific transparency requirements that apply to disclosures of CDR Insights with consumers' informed, express, and time-bound consent. In particular, the Rules should require the ADR to show the CDR Insight to the consumer prior to it being disclosed to the non-accredited Insight Recipient; should clarify a consumer's right to challenge the CDR Insight if they dispute the Insight; and should clarify the consumer's right to request deletion of the Insight.

5. Joint Accounts

CBA is not supportive of a default pre-approval, otherwise known as an 'opt-out' approach, for joint accounts. A default pre-approval approach does not align with the objective of the CDR regime, which is to give consumers more control over their data (which includes personal information). The CDR is a right for consumers to determine what data is shared, on what terms, and with whom. This is achieved by requiring the consumer's consent for the collection and use of their CDR data, and ensuring that their consent is voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn. A default 'pre-

[2] Maddocks, Update 2 to Privacy Impact Assessment ('PIA'), 29 September 2020, page 67, (available at: https://www.accc.gov.au/system/files/CDR%20-%20Update%202%20to%20privacy%20impact%20assessment.pdf)



approval' model for joint account holders would effectively take away that control, as it will result in data being shared without the prior consent of each account holder.

Further, transacting on an account is inherently different than data sharing – currency is fungible and recoverable; data is not. Transaction data reveals rich information about a person's location, their preferences, associations, who they are with, their income and liabilities. This data is inherently personal, and may include sensitive information under the Privacy Act 1988. In our experience, it would be out of step with customer expectations for this data to be shared without their explicit consent. As such, it is our view that the current opt-in approach must prevail as it ensures that data sharing can only occur on a joint account once all account holders are informed, have consented and enabled the account for data sharing.

CBA is concerned that the proposed draft rules do not provide a mechanism for the joint account holder who did not give their express consent for their data to be shared, to request their data be deleted by the relevant data recipient.

CBA also hold concerns about the implications for customer financial security and wellbeing if a default pre-approval approach is taken in the CDR, including for consumers experiencing vulnerability. We would therefore encourage further consultation with consumer advocacy and privacy groups on the design of any proposed deviations from the current 'opt-in' approach and consent model.

It is our view that the proposed default pre-approval approach is contrary to global privacy and data security trends, which would compromise the interoperability of the CDR, and is not aligned with recent recommendations by the ACCC and Office of the Australian Information Commissioner ('OAIC') on consent, including:

a) The ACCC's recommendation on strengthening consent requirements and pro-consumer defaults in the recently published *Digital Platforms Inquiry Final Report*, which stated:

> *"Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled."*[3]

In December 2020, the ACCC reiterated this recommendation in their submission[4] to the Review of the Privacy Act 1988 ('Privacy Act Review'). The ACCC also noted that allowing consumers to have meaningful control over their data is *'integral to maintaining the consumer trust necessary to continue the economic and social benefits of personal data flows'.*[5]

b) The OAIC's recommends in their submission to the Privacy Act Review that consent should be defined to *'require a clear affirmative act that is freely given, specific, current, unambiguous and informed'.*[6]

As such, CBA recommends retaining the existing opt-in approach for joint accounts data sharing, and proceeding with the introduction of in-flow election for joint accounts.

---

[3] ACCC, Digital Platforms Inquiry – Final Report, Recommendation 16(c), p35 (available at https://www.accc.gov.au/system/files/Digital%20Platforms%20Inquiry%20-%20Final%20report%20-%20part%201.pdf)
[4] ACCC Submission in response to the Issues Paper, December 2020, Review of the Privacy Act 1988, Annexure A, p16 (available at https://www.ag.gov.au/sites/default/files/2021-01/accc.PDF)
[5] 4.1 of the ACCC submission in response to the Issues Paper, December 2020, Review of the Privacy Act 1988, p7 (available at https://www.ag.gov.au/sites/default/files/2021-01/accc.PDF)
[6] OAIC Submission in response to the Issues Paper, 11 December 2020, Review of the Privacy Act 1988, Recommendation 34, page 77 (available at https://www.oaic.gov.au/assets/engage-with-us/submissions/Privacy-Act-Review-Issues-Paper-submission.pdf)