Commonwealth Bank

Group Submission to ACCC Consultation on proposed changes to the CDR Rules

29 October 2020

Submission – Proposed changes to the CDR Rules

Section 1: Introduction

The Commonwealth Bank appreciates the opportunity to make this submission in response to the Australian Competition and Consumer Commission's ('ACCC') consultation on proposed changes to the Consumer Data Right ('CDR') Rules, published 30 September 2020. We have endeavoured to provide feedback across a number of the proposals, however due to the large number and materiality of proposals put forward, we would welcome further consultation to support the ACCC's consideration of the next version of the CDR rules.

The CDR is a reform that has the potential to drive significant economic benefits for consumers for decades to come. As one of the first organisations to be delivering the CDR for our customers, the Commonwealth Bank is committed to building trust in the regime and maximising its benefit for all Australians.

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

The Government's intention, as stated in the Consultation Paper, is *'to encourage the growth and functionality of the CDR, meet the objectives of promoting competition and innovation in the data economy, and empower consumers' choices about their data*[1]*.'* The Commonwealth Bank is fully aligned with these objectives.

In considering proposed amendments to the CDR Rules, the Commonwealth Bank believes that the following common principles should be adhered to:

Firstly, CDR reforms should result in Australia and Australians 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 customer outcomes that result from non-permissioned use or inadequate operational processes. Amendments to the accreditation system and consent model to increase Accredited Data Recipient participation in the CDR regime should not be to the detriment of consumer protections or the safety and security of the regime.

Secondly, the Commonwealth Bank 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

[1] ACCC, Consultation Paper – CDR rules expansion amendments, September 2020, p 4.

continue alongside the Open Banking regime will result in 'dual schemes' being 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 complexity and material risks of introducing expanded scope and functionality into Open Banking cannot be understated. As such, any consideration and design of future CDR policy should be informed by data-driven findings of a post-implementation review conducted after the full implementation of the current CDR (Open Banking) regime as recommended in the *2017 Final Report for the Review into Open Banking in Australia*[2] and previously committed to by Government.

We acknowledge the work done to date by the ACCC, Office of the Australian Information Commission ('OAIC') and Data Standards Body ('DSB') in drafting the proposed rule changes for the CDR. These proposed draft rules represent a significant expansion of the CDR regime.

We agree with the finding of the Maddocks Privacy Impact Assessment[3] ('PIA') that the proposed amendments *'will significantly add to the already complex legislative framework underpinning the CDR regime'* by introducing *'a number of new definitions, concepts and information flows, all at the same time'*[4].

The proposed amendments introduce a complex set of new roles associated with tiered accreditation (e.g. enclave provider, sponsor etc.), new information flows (e.g. Accredited Person to Accredited Data Recipient), new non-accredited participants (e.g. Trusted Advisors, CDR Insight Recipients), while adding further complexity to core terms such as consents (i.e. divided into collection, use and disclosure consent). 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 viable.

We also agree with the PIA's risk finding that '*there are several inconsistencies and incomplete provisions in the proposed amendments, which may make it difficult to understand the application and intention of those amendments*'[5]. For example, consumers may not be able to provide informed consent; it will be difficult to know whether their privacy rights have been breached; there may be an increased risk of harm to consumers through diminution of consumer protections; and an increased risk that participants may not understand or meet compliance obligations.

Informed consumer consent is a critical tenet of the CDR regime, and there should be no relaxation of the existing consumer protections. As such, we support the PIA's recommendation[6] for the ACCC and DSB to conduct consumer research on the best approaches to ensure consumers can provide informed consent for all of the varied consents envisaged by the proposed draft rules. In particular, we recommend the consumer research considers the needs of all consumers, including vulnerable consumers.

---

[2] Australian Government, Final Report, Review into Open Banking in Australia, December 2017, Recommendation 6.6 (available at https://treasury.gov.au/consultation/c2018-t247313)
[3] Maddocks, Update 2 to Privacy Impact Assessment ('PIA'), 29 September 2020 (available at: https://www.accc.gov.au/system/files/CDR%20-%20Update%202%20to%20privacy%20impact%20assessment.pdf)
[4] Maddocks, PIA, page 44
[5] Maddocks, PIA, page 44
[6] Maddocks, PIA, page 47

In September 2020, the OAIC released the Australian Community Attitudes to Privacy Survey 2020[7]. The results indicate that now more than ever, Australians are concerned about their data privacy. One observation is that Australians want privacy policies that are easier to understand, and feature standard, simple language (87%) a plain English summary (86%), and use of icons as visual prompts (73%)[8].

If we anticipate Australians would like similar things from their CDR consents, adding complexity to consent through 'categorisation' will make the level of simplicity Australians desire highly unlikely. As such, and in keeping with the principles outlined above, the Commonwealth Bank is supportive of the PIA's recommendation that the ACCC take additional time to *'continue to refine the drafting of the CDR Rules'*, and *'issue detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules, as amended by the proposed changes'*[9]. This will help to provide greater clarity for implementation teams, help avoid rework and duplication of effort in the longer term and assist overall with the planning for and understanding of the scope of work required, including practical timeframes. It will also enable greater engagement with consumer advocacy groups on the proposed reforms to the regime.

Reciprocity obligations are fundamental for consumers, innovation, and competition

For the consumer benefits of the CDR to be fully realised, it is critical that Accredited Data Recipients 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 to meet the existing accreditation requirements, we strongly recommend adopting the recommendation of the *2017 Final Report for the Review into Open Banking in Australia*[10] that all Accredited Data Recipients 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 Accredited Data Recipient, the Data Recipient Accreditor (the ACCC) 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 2020 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 to consumers. Limiting the CDR regime such that it only enables consumers to share their data from Data Holders to Accredited Data Recipients (but not similarly requiring Accredited Data Recipients to send data the other way in response to a consumer's request) will considerably lessen the opportunity for consumers to leverage the potential of data sharing. There would be significant benefit for consumers if they were able to choose to exchange their data between

[7] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2020, September 2020, (available at: https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf)
[8] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2020, September 2020, page 5 (available at: https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf)
[9] Maddocks, PIA, page 45
[10] Australian Government, Final Report, Review into Open Banking in Australia, December 2017, Recommendation 3.9 (available at https://treasury.gov.au/consultation/c2018-t247313)

Data Holders and Accredited Data Recipients; however, currently there is no reason for companies in non-designated sectors to enable this consumer benefit.

Section 2: Timeline for proposed rules to take effect

The proposed draft rules represent a significant expansion of the CDR regime and will introduce additional complexity and risk to the current regime. As recommended in our submission to the Australian Treasury's *Inquiry into Future Directions for the Consumer Data Right*[11], any expansion of the CDR should not be considered until a post-implementation review is conducted 12 months after the full implementation of the current CDR (Open Banking) regime as recommended in the *2017 Final Report of the Review into Open Banking in Australia* and previously committed by Government.

Further refinement of the proposed draft rules and the development of proposed draft Consumer Data Standards ('the Standards') are required in order to understand the complexity involved in the implementation of these proposals. In particular, we welcome further clarification on the issues raised in the PIA.

Collaboration and cooperation across industry and regulators will be necessary to agree on practical implementation timeframes, and to facilitate appropriate planning and sequencing of multiple technological changes. The Commonwealth Bank recommends the compliance dates for any additional scope or functionality be subject to the final proposed draft of the Consumer Data Standards. It is not possible to determine build complexity and scale without assessing clearly defined technical requirements. However, having regard to the existing compliance milestones, we recommend that compliance dates for enabling sharing by non-individuals and business partnerships be introduced no earlier than July 2022.

We support a continuation of the phased implementation approach in the current Rules, with non-major ADIs having an appropriate additional period to the Major Banks to introduce new scope and functionality. In determining possible implementation dates for the next version of the CDR Rules, we request the existing delivery compliance timeline be taken into account. We note that the Major Banks, subsidiary brands and non-major ADIs are continuing to deliver significant compliance scope for existing CDR compliance milestones (Phase 3 Feb 2021; Phase 4 July 2021 (over 100 ADIs plus Major Banks' subsidiary brands); Phase 5 November 2021; and Phase 6 February 2021).

Section 3: Increasing the number and types of businesses that can participate in the CDR

The Commonwealth Bank 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.

[11] Commonwealth Bank of Australia, Submission to the Inquiry into Future Directions for the Consumer Data Right, May 2020 (available at: https://treasury.gov.au/sites/default/files/2020-07/cba.pdf)

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 breaches of their privacy and fraud.

We agree with the findings of the PIA that *'the complexities [of the proposed amendments] are particularly concerning in relation to the ability of entities to seek restricted accreditation, noting that such entities are less likely to be sophisticated providers of services who are familiar with handling important personal information and complying with complex legislative frameworks.'*[12]

We support the PIA's proposal to recommend that the ACCC *'continue to refine the drafting of the CDR Rules'*, and *'issue detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules, as amended by the proposed changes'.*[13] The Commonwealth Bank recommends further consultation with industry and consumer groups on the proposed models for restricted accreditation.

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. The Commonwealth Bank has concerns regarding the proposed self-attestation approach for restricted accredited parties, particularly given the PIA findings[14] that there is no obligation on a sponsor to enforce the CAP arrangement and it unclear what would be required for a sponsor to have taken 'reasonable steps' to ensure a restricted accredited person's compliance with the information security standards.

At a general level, the Commonwealth Bank notes the proposed draft rules do not sufficiently address the accreditation management of restricted Accredited Persons in Combined Accredited Person ('CAP') arrangements. For example, the proposed draft rules are silent on mechanisms to suspend or revoke the restricted Accredited Person where the CAP arrangement is terminated, suspended, or expired. It is essential that there is no delay in the technical suspension or revocation of an Accredited Person's accreditation to ensure that Data Holders are provided with the most up-to-date information regarding participants' accreditation status.

To that end, we are supportive of the PIA recommendation to consider a requirement within the Rules and/or accreditation conditions that the Data Recipient Accreditor (the ACCC) is notified if the relevant CAP arrangement is suspended, terminated or revoked.[15] Further, we recommend that the proposed draft rules should explicitly require a data recipient to delete the CDR Data where it has been collected inadvertently during a suspension or following a revocation of accreditation. A data recipient should not be given the option to de-identify the data as this provides an incentive to collect the data inadvertently.

We also note the proposed rules do not address how Accredited Data Recipients will know if an Accredited Person is suspended or has their accreditation revoked. The proposed rules do not include an obligation on the Accredited Data Recipient to check the accreditation status of an Accredited Person before sharing data with the Accredited Person.

[12] Maddocks, PIA, page 45
[13] Maddocks, PIA, page 45
[14] Maddocks, PIA, page 73
[15] Maddocks, PIA, page 74

In particular, we are concerned by the potential difficulty in determining the application of rules to the various parties in a CAP arrangement for different information flows; and determining when parties have collected, disclosed, or hold CDR Data.

1. The same entity may be described several different ways in different clauses of the CDR Rules. For example, a Data Enclave Accredited Person may be described in different rules as 'a person with data enclave accreditation' or as an 'Accredited Person', or as 'the Principal', or as the 'Accredited Data Recipient'. This creates ambiguity, adding to the difficulty in navigating compliance with the Rules for all CDR participants, but particularly for start-ups and small to medium enterprise ('SMEs'); and
2. It is unclear in CAP arrangements when a party has collected, disclosed or holds CDR Data. This lack of clarity will have compliance implications given different requirements apply to an 'Accredited Person' versus an 'Accredited Data Recipient'.

We agree with the PIA finding that further complexity will arise where a party undertakes transactions in multiple capacities, increasing the difficulty for entities and the regulators to determine which CDR Rules apply[16]. As noted in the PIA, *'the further complexity of the CDR Rules as a result of the proposed amendments increases risks of non-compliance, particularly by restricted Accredited Persons, with the important privacy protections contained in the legislative framework... [which] may increase reliance on the regulators to take additional investigatory and/or legal action for noncompliance'.*[17]

The Commonwealth Bank recommends further consideration on how to solve problems around data collection, use and on-sharing, consent models, accreditation tiers and information security standards.

3.1 Restricted level: limited data restriction

We are firmly of the view that the limited data restriction model is not appropriate for inclusion within a 'restricted' tier of accreditation within the Open Banking regime. It is our view that it is not possible to select subsets of 'less sensitive' banking data sets, and we do not support the concept of 'lower risk' datasets within Open Banking. We agree with the finding of the PIA that banking data is likely to be 'inherently sensitive'.[18]

In serving customers at scale, we see how devastating the impacts of fraud, cyber and privacy issues can be for customers. Protecting our customers' data is a responsibility we do not take lightly, and each year we invest significantly in continuously improving our cyber security controls. We disagree with advice the ACCC has received that suggests these data sets are unlikely to be the subject of cyber-security attacks.[19] The OAIC's Data Breach Report for Jan-June 2020[20] shows that the financial sector accounts for 14% of all breaches in Australia for that period, and that malicious or criminal attacks account for 59% of data breaches in the finance sector. The key information involved in those data breaches include contact information, identity information and financial details.

---

[16] Maddocks, PIA, pp 70-71
[17] Maddocks, PIA, pp 71-72.
[18] Maddocks, PIA, page 78
[19] Maddocks, PIA, page 78, referring to advice the ACCC has received about the risks associated with the types of CDR Data that may be held for the banking sector.
[20] Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January-June 2020, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/#kinds-of-personal-information-involved-in-breaches-all-sectors

The data sets proposed by the Consultation Paper (i.e. bank accounts, basic customer data, payees and regular payments) contain data fields that are currently used as part of existing bank identity verification processes. If these data sets were to be compromised or mishandled, the consumer's details could be used by malicious actors to perpetrate fraud and identity theft, causing significant consumer harm. Further, any compromise or mishandling of payee data could result in significant consumer harm, including malicious actors perpetrating fraud and identity theft of many individuals. We also note regular payments will include transaction data.

Access to customer data, including transaction history, should be considered the most sensitive category of data to share under the CDR framework and should naturally require the highest tier of accreditation for data recipients.

In prior submissions[21], the Commonwealth Bank recommended further consideration be given to the privacy and security risks of sharing payee details and counter-party identifiers, which commonly include name, BSB and account numbers of persons other than the CDR consumer. In line with industry practice, Commonwealth Bank recommends that sensitive data of third parties (e.g. a counter-party to a transaction) be obfuscated or tokenised as part of security standards defined by the Data Standards Body.

We agree with the Consultation Paper's acknowledgement that *'the risk of particularly CDR Data is highly contextual and that data can have a cumulative risk when combined with other data (whether publicly available data or not)'*[22]. This risk affects both consumers and the ecosystem.

We support the Australian Banking Association's recent recommendation[23] that the Australian Prudential Regulation Authority (APRA) is consulted on the implications of the proposed intermediary models and tiered accreditation within the Consultation Paper on the obligations of Approved Deposit-taking Institutions (ADIs) to comply with data standards per CPS234.

Section 4: Expanding how Accredited Persons can work together

4.1 Combined Accredited Person arrangements

The Consultation Paper states the Combined Accredited Person ('CAP') arrangements are intended to enable a restricted Accredited Person to work with an unrestricted Accredited Person to (a) support the data enclave restricted accreditation; or (b) to support affiliate restricted accreditation.

As noted above, the Commonwealth Bank recommends further consultation on the restricted level of accreditation and kinds of restricted Accredited Persons is required before the proposed rules can be finalised. We recommend any implications for the proposed draft rules for CAP arrangements are also considered as part of that consultation.

---

[21] Commonwealth Bank's submission to the ACCC's Exposure Draft for the *Competition and Consumer (Consumer Data Right) Rules 2019*, May 2019.

[22] ACCC, Consultation Paper – CDR rules expansion amendments, September 2020, page 12

[23] In their recent submission to the Treasury Consultation on the exposure draft of the *Treasury Laws Amendment (measures for a later sitting) Bill 2020: amendments of the consumer data right.*

We are supportive of the PIA's view[24] that further guidance about the proposed CAP arrangements be provided to ensure that all entities participating in the CDR regime understand their obligations.

In particular, we are concerned by the potential difficulty in determining the application of rules to the various parties in a CAP arrangement for different information flows; and determining when parties have collected, disclosed, or hold CDR Data. We agree with the PIA finding that further complexity will arise where a party undertakes transactions in multiple capacities, increasing the difficulty for entities and the regulators to determine which CDR rules apply[25]. As noted by the PIA, *'the further complexity of the CDR Rules as a result of the proposed amendments increases risks of non-compliance, particularly by restricted Accredited Persons, with the important privacy protections contained in the legislative framework... [which] may increase reliance on the regulators to take additional investigatory and/or legal action for noncompliance'.*[26]

Liability and accountability for resolving incidents and consumer complaints must be clear to participants and consumers, and it must not be unduly onerous for participants or consumers to seek remedies where multiple data recipients are involved in the collection, use and disclosure of CDR Data.[27] We suggest incident management requirements be defined under CAP arrangements to ensure consumer enquiries and complaints are managed and resolved in a timely manner.

Additionally, as noted in Section 3 of this submission, the proposed draft rules do not sufficiently address the accreditation management of restricted Accredited Persons in combined Accredited Person (CAP) arrangements. For example, the proposed draft rules are silent on mechanisms to suspend or revoke the restricted Accredited Person where the CAP arrangement is terminated, suspended, or expires. It is essential that there is no delay in the technical suspension or revocation of an Accredited Person's accreditation to ensure that Data Holders are provided with the most up-to-date information regarding participants' accreditation status.

To that end, we are supportive of the PIA's proposed recommendation to consider a requirement within the Rules and/or accreditation conditions that the Data Recipient Accreditor (the ACCC) is notified if the relevant CAP arrangement is suspended, terminated or revoked.[28] Further, we recommend that the proposed draft rules should explicitly require a data recipient to delete the CDR Data where it has been collected inadvertently during a suspension or following a revocation of accreditation. A data recipient should not be given the option to de-identify the data as this provides an incentive to collect the data inadvertently.

We note there is no requirement for the provider to comply with a direction from the principal in relation to the deletion of redundant data. We agree with the PIA finding that this creates a risk that a CDR consumer's data will not be de-identified or deleted.[29]

The proposed draft rules only require the principal (restricted level Accredited Person) to keep records about the CAP arrangement and its operation. We note the PIA considers there may be benefits for

[24] Maddocks, PIA, pp 45, 48., 72, 77
[25] Maddocks, PIA, pp 70-71
[26] Maddocks, PIA, pp 71-72.
[27] As proposed in the ABA's submission to the ACCC's Consultation on facilitating participation of intermediaries in the CDR regime, February 2020, p 3.
[28] Maddocks, PIA, page 74
[29] Maddocks, PIA, page 76

broadening Rule 9.3(2)(i) to apply to providers in a CAP arrangement, to ensure that the ACCC and/or OAIC have access to information critical to effectively enforcing compliance with CDR privacy obligations.[30]

4.2 Transfer of CDR Data between Accredited Persons

The Consultation Paper notes proposed draft rules have been developed to permit transfer of CDR Data in a manner that has not previously been considered, i.e. Accredited Persons would be enabled to transfer CDR Data between themselves in order to offer consumers distinct goods or services requested by consumers.

In particular, the proposed draft rules do not adequately address critical data security requirements and would create additional barriers for consumers seeking to stop data sharing. For example, the proposed approach would not enable consumers to manage their consents from the Data Holder dashboard. Under the proposed draft rules, a consumer would need to log into multiple Accredited Persons dashboards to stop sharing.

Of particular concern, is the lack of any requirements for the Accredited Data Recipient to ensure the consumer is informed about, or able to choose whether they consent to, the selling of their CDR Data. We also recommend further consideration of the proposed approach that would enable Accredited Data Recipients to charge fees for transferring CDR Data.

The Consultation Paper notes that there would be no technical data standards that govern how the CDR must be transferred. The Commonwealth Bank is firmly of the view that the transfer of CDR Data must be governed by technical data standards and should not be left to commercial arrangements. We recommend the technical standards that govern the transfer of data between a Data Holder and an Accredited Data Recipient should also apply to transfers of CDR Data between an Accredited Data Recipient and an Accredited Person. 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.

The Commonwealth Bank is not supportive of the proposed draft rules to enable transfer of CDR Data between Accredited Persons due to the risk of consumer harm and diminution of existing privacy and security protections. We strongly support the PIA's proposed recommendation that the ACCC continue to refine the drafting of the CDR rules with respect to this particular issue.

Section 5: Greater flexibility for consumers to share their CDR Data

5.1 Disclosure to trusted advisors

The Commonwealth Bank 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 Commonwealth Bank 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

[30] Maddocks, PIA, page 78

in the CDR regime. The Accredited Person is not required to comply with the CDR Rules or Data Standards when transferring CDR Data to a Trusted Advisor. This will increase the risks of loss or unauthorised access and disclosure during that transfer.

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 and Privacy Safeguards. As noted in the PIA, the proposed classes of Trusted Advisors may not have any obligations under other privacy legislation, such as the Privacy Act (including the Australian Privacy Principles).[31] We support the PIA's recommendation that there be a requirement that CDR Data only be disclosed to non-Accredited Persons that comply with the Privacy Act (including the Australian Privacy Principles).

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 entities risks undermining the consumer protections that the accreditation process is designed to provide.

In the event the ACCC intends to proceed with amendments to enable disclosure of CDR Data to non-Accredited Persons, the Commonwealth Bank recommends further consultation with industry and consumer groups to address the concerns raised in the PIA. For example, Commonwealth Bank agrees 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 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.

5.2 Disclosure of CDR insights

The proposed rules would permit Accredited Data Recipients to disclose an insight derived from a specific individual's CDR Data, to any person with a consumer's consent. The Accredited Person is not required to comply with the CDR Rules or Data Standards when transferring CDR Insights to an Insight Recipient. This will increase the risks of loss or unauthorised access and disclosure during that transfer.

We note the 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'*[32]. The 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 Persons proceed, disclosures of CDR Data 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 Data insights with consumers' informed, express, and time-bound consent.

[31] Maddocks, PIA, page 65
[32] Maddocks, PIA, page 67

Section 6: Extending the CDR to more consumers

6.1 Proposed approach to enabling CDR Data sharing by non-individuals

The Commonwealth Bank is supportive of the principles-based and non-prescriptive approach to designing the proposed draft rules for enabling business consumers within the CDR.

We firmly support the 'opt-in' model, where business consumers will nominate persons as 'nominated representatives' who can share and manage CDR on the CDR consumer's behalf. We welcome further clarification on what the regulator considers 'valid credentials in relation to the non-individual consumer's account'[33].

We recommend the proposed draft rules not be prescriptive regarding which channel is used to enable business customers (non-individual consumers) to authorise the sharing of CDR Data. This approach would provide greater flexibility for Data Holders with regard to implementation. The same outcome can be achieved through stipulation of in scope customer types and product sets.

The Commonwealth Bank recommends the proposed draft rules for the introduction of business consumers be staged, and commence with business partnerships followed by small businesses (as defined in the 2020 Banking Code of Practice). In making this recommendation, we refer to lessons from other jurisdictions, including the United Kingdom, whose Open Banking regime has focused on enabling retail customers and small to medium-sized enterprise.

We are firmly of the view that large customers (including large enterprise and institutional customers) should be out of scope for the CDR. There are existing commercial incentives for banks to provide direct to consumer data sharing for large corporates and institutional banking (IB). We support allowing the market to serve this need, as it enables proper consideration of the risks, regulatory and legal ramifications of sharing this data outside the regime (which will be too difficult to solve for within the CDR regime). Once IB clients have ingested their own data, they can set up the appropriate legal contracts to on-share this data with third parties (including participants in the CDR regime). Industry experience shows these customers are unlikely to use the CDR regime to share data, and we have previously expressed concern about potential inadvertent consequences resulting from the inclusion of large corporations as CDR consumers. Examples of these concerns are outlined below.

Compliance with other legal and regulatory obligations: the current CDR regime does not address the conflicts of laws issues arising from competing regulatory and contractual obligations, and in particular, does not consider the implications that the CDR regime may have in relation to Data Holders' regulatory obligations in other jurisdictions. For example, Data Holders should be able to refuse to comply with a direction to transfer CDR Data where a Data Holder holds a reasonable belief that to transfer the CDR Data would Breach the Data Holder's legal or regulatory obligations that are specific to institutional banking (IB), such as conflicts management, prevention of market abuse, price signalling, etc. or with confidentiality obligations with customers and other IB partners (e.g. syndicates and agents). The ACCC must also ensure that competitively sensitive information is not disclosed in a manner that could substantially lessen competition in a relevant market. The bank's interactions with IB customers are not extensions of the interactions with retail clients and some IB customers are larger than the banks that serve them.

[33] ACCC, Consultation Paper – CDR rules expansion amendments, September 2020, p 33

Privacy Safeguards: It is not clear how the Privacy Safeguards will operate in practice with regards to institutional clients, particularly given the conflict between the provisions in the *Consumer and Competition Act 2010* (Cth) (CCA), which extends the safeguards to business, and the interpretation issued by the OAIC, which restricts the safeguards to personal information of an individual. Irrespective of the Privacy Safeguards, the Commonwealth Bank will continue to meet common law and equitable obligations, such as the Banker's Duty of Confidentiality, with respect to the confidentiality of institutional client information.

With respect to concerns regarding the confidentiality of IB consumer data, for example, transaction data is high value data. This data directly exposes business and transactional relationships. While personal data exposes risk of identity theft, transaction data in aggregate can expose confidential relationships and valuable market data, potentially including data suggestive of trends that could be pertinent to financial markets. One potential scenario could be that a firm with many data customers in a foreign jurisdiction may look to mine the data for market sensitive information.

Confidentiality: An ADI and an IB customer may be subject to contractual confidentiality obligations set out in the overarching facility agreement. These agreements may involve more parties and therefore cannot simply be bilaterally amended to allow for disclosure to a third party. Mandatory disclosure may have downstream impacts for both the customer and the ADI when entering into multi-party arrangements. The CDR regime should offer protection for Data Holders where a non-individual consumer requests information that may be in breach of confidentiality of a third party whose information may be contained in the payload.

Genuine Consent: The *2017 Final Report for the Review into Open Banking in Australia* recommends that the transfer and handling of data under Open Banking should require the customer's informed, express, and time-bound consent. Consent arrangements for non-individuals need to be considered, these go beyond receiving delegated authority and permissions to ensure that consent is provided by the relevant people with the appropriate capacity, given the complexity of large businesses. There are often requirements to maintain confidentiality within divisions of legal entities, not simply within the organisation as a whole. The parameters for managing information flows are usually set out within confidentiality agreements and conflicts management policies and procedures, where permitted recipients of information are specified according to their role within an organisation and the nature of the information being shared. Information is often only shared on a "need-to-know" basis. The Data Holder should be able to rely on the authority of the 'nominated representative' of the non-individual consumer, to the extent the correct verification checks have been performed. There should be immunity for the Data Holder if there is a disclosure based on a 'nominated representative' who holds themselves out as having authority to consent on behalf of the non-individual consumer. We request clear guidance from the ACCC regarding how it expects Data Holders to verify nominated representatives, including whether Power of Attorney or signatory lists would suffice.

The 'opt-in' model with nominated representatives envisaged by the ACCC does not address the above issues of genuine consent, particularly where different staff members may be authorised to transact on different accounts with no commonality across the breadth of a large institution. The model also does not address the conflict between a CDR consumer who is subject to contractual confidentiality obligations, authorising a third party, that being an Accredited Data Recipient, to request information that is subject to the confidentiality requirements.

Further, we appreciate the recent guidance the ACCC provided in relation to guidelines to determine if products are in scope under the CDR. We recommend this guidance is incorporated into the Rules, especially in determining if a product is "publicly available". We further recommend that wholesale and institutional clients are specifically excluded as being eligible under the Rules.

Nominated Representative – Dashboard

We are supportive in-principle of the proposal to require a Data Holder to provide a single dashboard to non-individual consumers, which can be used by their nominated representatives to manage CDR Data sharing on the non-individual consumer's behalf. We agree in-principle that multiple nominated representatives should be able to view and manage the same sets of consents, however they should not necessarily be able to view all of the consents a non-individual consumer may have. For example, the visibility of the existence of some consents may breach Chinese Walls. The rules should allow sufficient flexibility to cater for these circumstances.

We note that an inadvertent outcome of allowing only one nominated representative to share data on behalf of a non-individual consumer means that only one individual's credentials would need to be compromised to share data once an individual has been nominated. We recognise that the rules are principle-based to provide flexibility in implementation approaches; however, we recommend the proposed draft rules are amended to enable Data Holders to optionally implement additional controls to ensure the security of the consumer's CDR Data. We expect many of our business customers will be interested in controls equivalent to those we have already implemented for them on their business banking accounts. For example, two-factor-authentication to verify individuals, and two-to-authorise for transactions.

6.2 Specific rules for business partnerships

The Commonwealth Bank supports the proposed approach to treat business partnerships in line with the approach the ACCC is proposing for non-individual consumers, noting our recommendation above that the rules should not prescribe which channel is used to enable data sharing.

6.3 Secondary users

The Commonwealth Bank recommends that further consultation be undertaken regarding the introduction of secondary users. We specifically welcome consideration of the potential impacts for vulnerable consumers, and the implications for deletion/de-identification of CDR Data.

It is our view that enabling persons beyond those with the ability to make transactions on an account should not be considered, as it would introduce additional risk of data being shared by unauthorised persons.

It is our view that to enable data sharing by a secondary user, each account holder must consent to enabling the account/secondary user to share CDR Data. That is, once the Rules are expanded to include joint accounts held by more than two individuals, all account holders should be required to enable any authorised users to share data.

Further, if secondary users are to be enabled, it is unclear whether it is feasible to implement only transactions restricted to the secondary user.

It is our view that the primary account holder should be able to 'remove' an account from a data sharing consent initiated by the secondary user. This ensures consistency with the current joint account model whereby both account holders can revoke the authorisation to share data with a specific Accredited Data Recipient. This granular control benefits both the account holder and the secondary user – it provides the primary account holder with the ability to remove sharing with a specific Accredited Data Recipient (triggering deletion/de-identification), while continuing to provide flexibility for the secondary holder to share account data with other Accredited Data Recipients.

We would welcome further consideration of the practical implications in scenarios where secondary users shared data through the 'transfer of CDR data between Accredited Persons' approach described in section 4.2 of the Consultation Paper. Our understanding of the proposed rules is that the primary account holder(s) will not have further visibility or control over the CDR Data shared by the secondary user when shared in this manner. This could result in adverse impacts for consumers, particularly vulnerable consumers.

Section 7: Facilitating improved consumer experiences

7.1 Sharing CDR Data on joint accounts

The proposed draft rules raise additional questions that we request the ACCC give consideration to during further consultation with CDR participants, including disclosure options, implications for the joint account management service, and joint account definition.

We are supportive of the following proposed approaches for joint accounts:

- Requiring Data Holders to allow consumers to set their preferences (a disclosure option) as part of the authorisation process.
- Expansion of the rules to include joint accounts held by more than two individuals, provided that all parties will need to 'enable' the account for sharing; and any party can remove account(s) or disable sharing under the one-to-authorise model.
- The rules do not require, nor prohibit, the history of disclosure option selections being displayed to consumers as part of the Joint Account Management Service or Data Holder consumer dashboard (e.g. no requirement to display the consumer's history of one-to-authorise vs two-to-authorise).

We are concerned that the proposed draft rules mean that Joint Account Holder A could provide consent for an Accredited Person to disclose their CDR Data to other persons (non-Accredited Persons or Accredited Data Recipients) and Joint Account Holder B will have no transparency or notification of that disclosure. It is our view this creates risk of harm for consumers, particularly if banking data is being shared. We recommend further consideration of measures to increase transparency and consumer control over who their data is shared with. In particular, ensuring Joint Account Holder B has transparency of any further disclosures of CDR Data relating to their joint account, which will allow the consumer to make informed decisions and have better control of their data (e.g. Joint Account Holder B could decide to disable sharing on their joint account if they are uncomfortable with the on-disclosure).

We recommend further consideration be given to measures to improve consumer visibility and control before the rules are finalised.

7.2 Amending consents

The Consultation Paper asks for views on whether it should be mandatory or optional for Accredited Persons to offer consumers the ability to amend consents in the consumer dashboard. The Commonwealth Bank is supportive of an optional approach. It is our view this should be left to the competitive space of Accredited Persons to determine the customer experience i.e. customers could amend consent in the consumer dashboard, set up a concurrent consent or cancel consent and replacing with a new consent.

We support the PIA's proposed recommendation that considers a greater level of transparency (about any arrangements/monetary benefits the Accredited Data Recipient receives if they recommend the Accredited Person) should be provided to consumers before they provide Use Consents and Disclosure Consents for direct marketing.[34]

We are supportive of PIA's proposed recommendation that considers imposing limitations on the frequency and timing for Accredited Data Recipients inviting consumers to amend their consent in general and considers the appropriateness of presenting pre-selected options to the CDR consumer.[35]

It is our view that the authorisation process for amending authorisations could be simplified; however, the authorisation must include the Data Holder. We are supportive of a consistent technical approach be taken to amending use case, accounts, duration and data sets, and the customer experience be left to Accredited Persons.

7.3 Separate consents approach

The Commonwealth Bank is firmly of the view that the consumer should have control and complete visibility over how their CDR Data is shared and used. For this reason, we do not support the separation of consent to collect, consent to use, and consent to disclose CDR Data. It is our view that the separation of these consents introduces considerable complexity and risk to the ecosystem. Further, the proposed approach will make it challenging for consumers to understand the full implications of each of the separated consents.

The Commonwealth Bank is not supportive the transfer of CDR Data between Accredited Persons as proposed in the draft rules, and as such we are not supportive of the need for consent to disclose.

7.4 A 'point in time' redundancy approach and the impact of withdrawing authorisation

The Commonwealth Bank is firmly of the view that consumers should have control and complete visibility over how their CDR Data is shared and used. The proposed approach to separate consents would have the adverse outcome that visibility and management of both consents to use and disclose is spread across two dashboards. We support the need to delete redundant data when the consent to use is cancelled or expires.

We firmly oppose the Consultation Paper's proposed approach whereby consumers would not be able to terminate all consents with an Accredited Person via their Data Holder dashboard. In taking a consumer-led approach, and in keeping with the existing 'no wrong doors' principles, the consumer should be able to manage their consents in one location.

[34] Maddocks, PIA, page 63.
[35] Maddocks, PIA, page 55

We are not supportive of the proposed rules to require Accredited Persons to provide a notification to the consumer in writing and outside of the consumer dashboard. It is our view that this would be a poor consumer experience, and a preferable approach would be to require notification in the dashboard with the option to provide a notification digitally (e.g. in app or via email).

Further, it is our view that tagging CDR Data should occur from the point of collection, to ensure that a consumer's instructions to delete or de-identify data from a particular Data Holder are followed, which would assist regulators with compliance and enforcement activities.

7.5 Improving consumer experience in Data Holder dashboards

We welcome further discussion and examples on the rationale for requiring different fields in the dashboard, for example, brand, field presented in authorisation flow, field presented in consent management, and field presented for concurrent consent.

We are supportive of PIA's recommendation[36] for the ACCC to consider whether the proposed amendments should include requirements for the Data Holder's dashboard to contain details of each amendment that has been made to each authorisation. This would align with current 'no wrong doors' principles that the consumer must be able to use either their Data Holder or Accredited Data Recipient dashboard to view or amend their consents.[37]

To ensure greater consumer control and transparency of their data sharing arrangements, it is our view that Data Holders should be able to maintain full traceability over any on-disclosure to entities involved in a data sharing request. This is particularly relevant where there are intermediaries involved, such as restricted and unrestricted Accredited Persons working within CAP arrangements. We note there is technical complexity, given that the current data standards call for each consent amendment to be enacted via a consent cancellation in conjunction with a consent creation. The consent creation will contain the details of the amended consent. This approach to consent will make it difficult for Data Holders to reliably determine what has changed between consents. We recommend supporting this proposal with changes to the data standards to enact consent modification – thereby enabling Data Holders to track what has changed in the amended consent.

We hold concerns that the proposed ability for Accredited Data Recipients to include 'free text', which could have adverse impacts on consumers if the Accredited Data Recipients use this in an inappropriate or misleading way. For example, (a) an aggregator collecting data on behalf of an organisation includes free text that leads the consumers to believe they are sharing data directly with the organisation and not with the aggregator; or (b) marketing messages are included in free text, which encourage consumers to ignore important messages from Data Holders.

7.6 Use of the CDR logo

Given the importance of the CDR Logo as a signifier of trust for consumers, we recommend provision for ACCC to monitor the internet to ensure that non-accredited entities are not using the logo on their websites. For example, Commonwealth Bank has a monitoring system to ensure fraudulent websites masquerading as CommBank are taken down.

[36] Maddocks, PIA, page 57
[37] Maddocks, PIA, page 57

7.7 Permitting use of CDR Data for research

The Commonwealth Bank recommends further consultation on the proposed draft rules relating to the permitted use of CDR Data for research and selling of CDR Data.

Section 8: Clarifying rule amendments

8.1 Application of product reference data rules to 'white labelled' products

We note that the proposed draft rules only cover white labelled products with respect to product reference data and only if both parties are Data Holders. We propose that the Rules be amended to make it clear and consistent that the Data Holder in this case refers to the entity that enters into the contract with consumers to provide the relevant product for both product reference data and consumer data sharing. If a product is white labelled and the consumer has not entered into a contract with the product manufacturing entity, then that entity is not deemed a Data Holder for the purposes of the CDR. This is because the consumer will most likely be unaware of the relationship with that product manufacturer and their online channel may not be conducive for data sharing in relation to either the white labelled product or end consumer.

We note the current design of the Register does not have an established way to represent one legal entity sharing product reference data on behalf of another. Changes to the entity model of the Register may have flow on impacts for consumer data request services.

8.2 Closed accounts

We are supportive of the proposed rules to align the data sharing requirements for closed accounts across transaction data, account data and product specific data, as this will ensure a consistent consumer experience for closed accounts across all data scopes (noting that only available data on closed accounts will be able to be shared).

8.3 Reporting and record keeping requirements

The Commonwealth Bank recommends the revised compliance obligations for the proposed reporting and record keeping requirements commence no earlier than July 2021. This will allow for further clarification of the proposed changes envisaged by the proposed draft rules and provide sufficient time for CDR participants to design appropriate changes to their current implementation to ensure compliance with the proposed requirements. For example, the introduction of non-individual consumers, additional consent types, more granular reporting of refusals to disclose (sub rule 9.4(1)(d)) and additional requirements regarding consumer record requests (sub rule 9.5).

It is our view that the requirement in sub rule 9.5(4) to provide requested copies no later than 10 business days after receiving the request is unduly restrictive, particularly given the additional record response requirements imposed by proposed draft sub rules 9.5(1) and 9.5(2), as well as the proposed inclusion of complex consumers (non-individuals) and multiple consent types. The Commonwealth Bank calls for greater alignment with the Australian Privacy Principles which provide an 'SLA (Service Level Agreement)' of 30 calendar days.

We note the proposed draft sub rule 9.5(2) imposes additional scope to consumer requests for copies of records. The additional scope relating to sub rule 9.3(2)(c) *"notification of withdrawals of authorisations*

received from Data Holders" provides limited value to consumers as the resulting consent changes will be reflected in other records provided to the customer under sub rule 9.3(2)(b) *"amendments to or withdrawals of consents by CDR consumers".* Additionally, sub rule 9.3(2)(c) is a CDR technical concept that will have limited meaning to consumers or cause confusion. On these grounds, we do not support the inclusion of proposed draft sub rule 9.3(2) (c).

We note it may be difficult for Accredited Persons to meet the requirements of sub rule 9.3(2)(b), given the current Consumer Data Standards call for each consent amendment to be enacted via a consent cancellation in conjunction with a consent creation. As the consent creation will contain the details of the amended consent, it will be difficult for Data Holders to reliably determine what changed between consents. To resolve this issue, we recommend this proposal be supported by Data Standards changes to enact consent management – thereby enabling Data Holders to understand what has changed in the amended consent.

8.5 Registrar amendments

We are broadly supportive of the proposed amendments to provide the Registrar with powers to protect the security, integrity and stability of the Register and associated database. We recommend that sub rule 5.34(1)(a) be amended to include a direction for an Accredited Person to refrain from responding to consumer data requests.