Australian Competition and Consumer Commission

CONSUMER DATA RIGHT REGIME

Update 2 to Privacy Impact Assessment

Analysis as at 29 September 2020
Report finalised on 8 February 2021

© Maddocks 2021
The material contained in this document is of the nature of general comment only. No reader should rely on it without seeking legal advice.
## Contents

### Part A  Introduction  3
1. Overview ................................................................. 3
2. Structure of this PIA Update report ....................... 4

### Part B  Executive Summary  6
3. Introduction ....................................................... 6
4. Summary of findings ......................................... 6
5. Recommendations ............................................. 8

### Part C  Methodology  17
6. Our methodology ............................................. 17
7. Scope of this PIA Update report ........................ 18

### Part D  Project Description  19
8. Changes to consents ......................................... 19
9. AP Disclosure Consent (and Accredited Data Recipient Requests) ................... 29
10. TA Disclosure Consent ....................................... 34
11. Insight Disclosure Consent ............................... 35
12. New levels and kinds of accreditation ............... 36
13. Joint Account Holders ........................................ 50
14. Secondary Users ............................................... 56

### Part E  Analysis of Risks  58
15. Overview ............................................................ 58
16. General risks .................................................... 59
17. Risks associated with changes to consents .......... 65
18. Risks associated with the disclosure of CDR Data to Accredited Persons (through AP Disclosure Consents and Accredited Data Recipient Requests) ............ 82
19. Risks associated with the disclosure of information relating to CDR Consumers to non-accredited persons (through TA Disclosure Consents and Insight Disclosure Consents) ........................................... 92
20. Risks associated with the introduction of new levels and kinds of accreditation ................................. 107
21. Risks associated with the changes to joint accounts ................................................................. 126
22. Risks associated with the introduction of Secondary Users being able to authorise the sharing of CDR Data .......................................................... 139

### Attachment 1  Glossary  145

### Attachment 2  List of Stakeholder submissions  147
Part A Introduction

1. Overview

1.1 Maddocks is very pleased to provide this second privacy impact assessment update report (PIA Update 2 report) for the Australian Competition and Consumer Commission (ACCC).

1.2 On 11 December 2019, the Department of the Treasury published the Privacy Impact Assessment into the Consumer Data Right Regime (Original CDR PIA report), together with the responses to the recommendations made in that report.

1.3 As the Original CDR PIA report was undertaken as a “point in time” analysis of the development of the legislative framework (that is, the Competition and Consumer Act 2010 (Cth) (CC Act), Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) (CDR Rules), Data Standards and the Open Banking Designation), the Original CDR PIA report recommended that it be treated as a “living document”, which should be further updated and/or supplemented as the various components of the legislative framework are amended and/or developed.

1.4 Since the CDR Rules commenced on 6 February 2020, the ACCC has been reviewing, considering and revising the CDR Rules and a number of amendments to the CDR Rules have been made. Further stakeholder consultation processes have also been undertaken during that time.

1.5 Maddocks has been engaged to consider the privacy impacts of a further round of proposed amendments to the CDR Rules, including a number of changes that have been developed in parallel with our engagement. We have based our discussion and analysis in this PIA Update report on a consolidated version of the CDR Rules provided to us on 29 September 2020, which includes:

1.5.1 proposed changes to consents;

1.5.2 the introduction of changes that will allow a CDR Consumer to consent to disclosure of their CDR Data, which has been collected and is held by an Accredited Data Recipient, to another Accredited Person (AP Disclosure Consents);

1.5.3 the introduction of changes that will allow a CDR Consumer to consent to disclosure of their CDR Data, which has been collected and is held by an Accredited Data Recipient, to a Trusted Adviser who is not an Accredited Person (TA Disclosure Consents);

1.5.4 the introduction of changes that will allow a CDR Consumer to consent to disclosure of a “CDR insight”, derived from their CDR Data by an Accredited Data Recipient, to any person (Insight Disclosure Consent);

1.5.5 the introduction of new levels and kinds of accreditation, so that a person may apply for unrestricted accreditation, data enclave accreditation, limited data accreditation, or affiliate accreditation;

1.5.6 changes to the application of the CDR regime to joint account holders; and

1 Recommendation 1 in the Original CDR PIA report.
1.5.7 the introduction of ‘secondary users’ being able to authorise sharing of CDR Data.

1.6 Our work occurred in parallel with the drafting of the proposed amendments to the CDR Rules, which we understand is on-going. The version of the CDR Rules which was published by the ACCC for stakeholder consultation included additional proposed amendments which, at the time of publication we had not had the opportunity to review and consider whether they pose any additional privacy risks. These further amendments included:

1.6.1 changes to the way that partnerships are managed for the purposes of the CDR regime, including the introduction of the concept of nominated representatives;
1.6.2 changes in relation to management of CDR complaint data;
1.6.3 requirements in relation to use of the CDR logo;
1.6.4 changes in relation to product data requests;
1.6.5 the introduction of a new ability for the Accreditation Registrar to temporarily prevent the making of consumer data requests or responding to such requests, in order to ensure the security, integrity and stability of the Accreditation Register;
1.6.6 new civil penalty provisions; and
1.6.7 for the banking sector, changes to eligible CDR Consumers, required consumer data, and the introduction of the concept of pre-application CDR Data.

1.7 The ACCC subsequently received submissions from stakeholders which provided feedback on the version of the CDR Rules which was published by the ACCC. At the date of the analysis contained in this PIA Update report, the ACCC was considering that feedback and continuing to develop and refine the policies underpinning the changes to the CDR Rules that were proposed. It was decided that this PIA Update would be finalised on the basis of the version of the CDR Rules as at 29 September 2020, taking into account stakeholder submissions received on the published version of the proposed changes, so that our analysis and recommendations can be considered by the ACCC and used to further inform its work in relation to the CDR Rules.²

2. Structure of this PIA Update report

2.1 This PIA Update report is comprised of the following sections:

2.1.1 Part B - Executive Summary: This section contains a summary of the privacy risks we have identified, together with a list of all recommendations we have made as a result of our analysis.

2.1.2 Part C - Methodology: This section details how we are undertaking the PIA Update report, and includes information about the scope of the PIA Update report.

² Note at the time of finalising this PIA Update report: We appreciate that some of the proposed changes to the CDR Rules (which are discussed in this PIA Update report) were not introduced, or were introduced in a different form, or will be further considered and developed at a later time.
2.1.3 **Part D - Project Description:** This section contains a summary of the further proposed changes to the CDR Rules discussed in paragraph 1.5 of this Part A, and discusses the various concepts and information flows relevant to those proposed changes.

2.1.4 **Part E - Analysis of Risks:** We have analysed the potential privacy risks that we have identified as being associated with the relevant proposed changes to the CDR Rules. We have identified the current mitigation strategies and conducted a gap analysis to identify any areas of concern, as well as specify our recommendations.

2.1.5 **Attachment 1 - Glossary:** This section sets out a list of some capitalised terms that we have used in this PIA Update report, and their definitions.

2.1.6 **Attachment 2 - List of Stakeholder submissions:** This contains a list of stakeholders who provided written submissions as part of the ACCC’s stakeholder consultation process.
Part B Executive Summary

3. Introduction

3.1 In this Part B [Executive Summary], we have provided a summary of the privacy risks we have identified in the proposed changes to the CDR Rules, as well as a consolidated list of all of the recommendations we have made as a result of our analysis and the associated privacy risks we have identified during that analysis.

3.2 We understand that the ACCC, in consultation with other Commonwealth agency stakeholders as required, will separately develop a response to our recommendations.

4. Summary of findings

4.1 We have identified various privacy risks related to the proposed amendments to the CDR Rules. These are set out in detail in Part E [Analysis of Risks], but include privacy risks associated with:

4.1.1 in general:

(a) the overall complexity of the proposed amendments, which will significantly add to the already complicated legislative framework underpinning the CDR regime;

(b) the lack of clarity around collection, use, holding and disclosure of CDR Data (including any relevant obligations on an entity);

4.1.2 in relation to the proposed changes to consents:

(a) the risk that CDR Consumers will not understand the consents they are providing and, given the additional complexities being proposed to the consent process, that they may experience “information overload”;

(b) the lack of clarity around new concepts for consent, including using CDR Data for general research purposes; and

(c) CDR Consumers being unaware that their CDR Data can be sold, and what happens if they withdraw a Collection Consent (but not a Use Consent);

4.1.3 for the proposed changes to allow disclosure of CDR Data to another Accredited Person:

(a) a lack of clarity around the obligations of the participating entities, including the role or status of each entity (an ‘accredited person’ or ‘accredited data recipient’) during the information flows;

(b) the potential for CDR Data to be disclosed to another person without a check that that person is still an Accredited Person; and

(c) the lack of transparency around Use Consents and Disclosure Consents for direct marketing purposes;
4.1.4 for risks associated with the proposed changes to allow disclosure of CDR Data and Insights to non-accredited persons:

(a) CDR Consumers not understanding the implications of consenting to the disclosure of CDR Data or CDR Insights to non-accredited recipients;

(b) the sharing of CDR Insights being invasive for CDR Consumers, particularly vulnerable CDR Consumers who may not understand the consequences from providing their consent; and

(c) the transfer of CDR Data and CDR Insights not needing to be compliant with the CDR Rules or the Data Standards;

4.1.5 in relation to the proposed introduction of new levels and kinds of accreditation:

(a) the risk of insufficient incentive to ensure compliance with legislative requirements;

(b) transparency about arrangements for CDR Consumers; and

(c) the lack of legislative requirements for CAP arrangements (including in relation to the treatment of redundant data);

4.1.6 in relation to the changes to joint accounts:

(a) the fact that JAMS only applies to the disclosure of CDR Data by a Data Holder to an Accredited Data Recipient; and

(b) JAMS in the context of vulnerable CDR Consumers; and

4.1.7 in relation to the introduction of ‘secondary users’:

(a) a potential lack of clarity in relation to the rights of Secondary Users to request further disclosures by an Accredited Data Recipient to an additional Accredited Person, Trusted Advisor or an Insight Recipient, including after the applicable Secondary User Instruction has been withdrawn by the Account Holder;

(b) the potential for disclosure of CDR Data relating to another person with account privileges who is not the Account Holder or a Secondary User;

(c) transparency for the Secondary User if the relevant Secondary User Instruction has been withdrawn;

(d) the limitation on the ability to share CDR Data for joint accounts with a co-approval option; and

(e) transparency for other individuals, who are not themselves Secondary Users or the Account Holder, but who have account privileges for the relevant account.

4.2 Some of these risks are significant, and we understand that the ACCC is currently considering and further developing the relevant policy and associated issues. Our recommendations may assist in mitigating some of these risks, and are set out in paragraph 5 of this Part B [Executive Summary].
5. Recommendations

5.1 We have made the following recommendations in this PIA Update report. These are summarised below, but should be read in connection with the relevant Parts of this PIA Update report.

General

**Recommendation 1** Continue refine drafting of the CDR Rules, and issue clear guidance

We 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. We suggest that different forms of guidance could be developed and specifically tailored to assist:
  - CDR Consumers;
  - applicants for accreditation;
  - Data Holders;
  - Accredited Persons for each level of accreditation; and
  - enclave providers and sponsors; and
- on how the process in Rule 4.11 is intended to operate, so as to ensure that CDR Consumers are provided with the right type of information and choices before providing their consent
- on the CDR Rules relevant to the new levels and kinds of accreditation (including clarification and expansion of Rule 1.7(v), which only relates to outsourced service arrangements).

**Recommendation 2** Continue conducting consumer research

We recommend that the ACCC consider whether it would be appropriate to continue, in consultation with the Data Standards Body, conducting consumer research on:

- what is the best way to present a CDR Consumer with all of the different types of consents, to ensure that CDR Consumers are provided with an adequate amount of information before providing their consent, but balancing this against the risk of “information overload” for the CDR Consumer;
- the appropriateness of presenting pre-selected options to a CDR Consumer with details of their current consent (and ensure the requirements around permitting pre-selected options are limited to only details of the CDR Consumer’s current consent), as this information may assist in informing a CDR Consumer which aspects of their consent they would like to amend (as they will be able to view what they previously selected, such as their election to delete redundant data); and
- a suitable way for information in relation to Secondary Users to be presented to Account Holders without involving “information overload”.
Consents

Recommendation 3  Considerations in relation to amendment of consent

We recommend that the ACCC:

- consider whether it would be appropriate to give the CDR Consumer the opportunity, when they are amending their consent, to withdraw their Use Consent if they do not want the Accredited Person to continue using any already-collected CDR Data;

- in relation to information provided to CDR Consumers by Accredited Persons when they are amending their consent:
  
  - clarifying whether information specified in Rule 4.11(3) is required to be provided each time a CDR Consumer amends their consent, or only when the CDR Consumer provides their original consent; and
  
  - consider whether the CDR Consumer should only be provided the information in Rule 4.11(3) if the information has changed since the last time the CDR Consumer gave/amended their consent. This will assist in ensuring a CDR Consumer is provided with adequate information before amending their consent, but does not experience “information overload;

- consider including similar limitations on how often, and when, the Accredited Person can invite a CDR Consumer to amend their consent in general (because if a CDR Consumer is constantly inundated with invitations to amend their consent, they may feel pressured to do so, meaning the amendments to their consents may not be given voluntarily); and

- consider including, as part of the information required to be provided as part of Rule 4.11, a requirement for Accredited Persons to notify CDR Consumers when asking for their consent that they can, at a later stage, amend that consent through the Accredited Person’s Consumer Dashboard (e.g. to vary the validity period of the consent, or to change the type of CDR Data the Accredited Person collects from a Data Holder).

Recommendation 4  Include timing requirements on obligations

We recommend that the ACCC consider including requirements for the Accredited Person to provide the relevant information within a certain timeframe (to ensure that for example, an Accredited Person provides a CDR Consumer with the relevant information before they amend their consent), noting the importance of notifying CDR Consumers about information relating to their consents (such as in relation to the withdrawal or amendment of a consent).
**Recommendation 5**  
Further consider the drafting of new concepts in relation to consent contained in the CDR Rules

We recommend that the ACCC consider:

- the need for the new concept of ‘categories’ as it adds further complexities to an already-complex consent process;

- in relation to the selling of CDR Data:
  - including requirements around the selling of CDR Data (e.g. requirements for the Accredited Person to seek a CDR Consumer’s express consent for the selling of their CDR Data); and
  - including a requirement for the Accredited Person to provide the CDR Consumer with a clear option to not consent to the selling of their CDR Data;

- whether it should expressly specify that if an Accredited Data Recipient becomes a Data Holder of CDR Data, any Disclosure Consents that relate to that CDR Data expire (or otherwise explain it is appropriate why those Disclosure Consents continue) (this would be a similar approach to the expiry of Collection Consents and Use Consents);

- whether it should include, similar to the proposed amendments to the requirements of an Accredited Person’s Consumer Dashboard, requirements for the Data Holder’s Dashboard to contain details of each amendment that has been made to each authorisation;

**Recommendation 6**  
Consider the use of CDR Data for the purposes of general research

We recommend that the ACCC consider:

- requiring an Accredited Person to clearly notify the CDR Consumer, when seeking a Use Consent for the purposes of general research:
  - which specific research projects the Accredited Person will use the CDR Consumer’s CDR Data for;
  - the specific purposes for which the Accredited Person uses the relevant research (for example, to conduct market research on its customers to inform the development of new products);
  - the types of the CDR Consumer’s CDR Data used in the relevant research; and/or
  - any potential consequences on this use for research for the CDR Consumer (for example, that their de-identified data from the research may be disclosed and sold); or

- alternatively, whether the information an Accredited Person will use for research should be de-identified, so that no identifiable information of a CDR Consumer will be used by the Accredited Person.
Disclosure of CDR Data to Accredited Persons

**Recommendation 7** Clarify information flow between Accredited Data Recipients and Accredited Persons

We recommend that the ACCC consider clearly setting out the new information flow of disclosure of CDR Data from an Accredited Data Recipient to an Accredited Person (including clarifying the fact that an Accredited Person (A2) becomes an Accredited Data Recipient after receipt of CDR Data and therefore must comply with any obligations relevant to Accredited Data Recipients), given the importance of each party understanding their obligations (especially as the CDR Rules contain certain obligations on Accredited Persons, and certain obligations on Accredited Data Recipients).

**Recommendation 8** Clearly specify when, if one consent expires, the other consent expires

We recommend that the ACCC consider whether it would be appropriate to clearly specify when, if one consent expires, the other consent expires. For example, this could include clarifying whether the expiry of a consent is contingent on one party notifying the other of the expiry of the associated consent, or whether the associated consent automatically expires.

**Recommendation 9** Obligations in relation to accreditation for AP Disclosures

We recommend that the ACCC consider including obligations on:

- the Accredited Data Recipient (A1) to check the credentials of the Accredited Person (A2) before any CDR Data is disclosed (similar to the obligations on Data Holders); and
- each party to notify the other if their accreditation gets suspended, revoked, or surrendered.

**Recommendation 10** Inform CDR Consumers about the status of any Accredited Data Recipient Requests

We recommend that the ACCC consider whether the CDR Consumer should be informed about:

- the refusal to progress their Accredited Data Recipient Request (including by refusing to provide the CDR Data to the Accredited Person (A2)); and
- the reasons for the refusal.

This will assist in ensuring that CDR Consumers retain control over their CDR Data (and oversight over any Accredited Data Recipient Requests).
**Recommendation 11 Inviting CDR Consumer to amend their Disclosure Consent**

We **recommend** that the ACCC consider whether it would be appropriate to include requirements for the Accredited Data Recipient (A1) to invite the CDR Consumer to amend their Disclosure Consent if the Accredited Data Recipient (A1) is notified by the Accredited Person (A2) that the CDR Consumer has amended their Collection Consent. This requirement could be drafted in a similar way to the proposed amendments in relation to a Data Holder inviting a CDR Consumer to amend their authorisation if the Data Holder is notified that they have amended their associated Collection Consent with the Accredited Data Recipient (see Rule 4.22A).

**Recommendation 12 Notification requirements if a Collection Consent for the purposes of an Accredited Data Recipient Request is withdrawn**

We **recommend** that the ACCC consider clarifying the obligations on an Accredited Person (A2) to notify an Accredited Data Recipient (A1) if a Collection Consent for the purposes of an Accredited Data Recipient Request is withdrawn, similar to the requirements specified in Rule 4.13(2)(b). This will assist in ensuring that an Accredited Data Recipient (A1) does not continue to disclose CDR Data if the associated Collection Consent given to an Accredited Person (A2) has been withdrawn.

**Recommendation 13 Greater transparency for CDR Consumer in relation to direct marketing**

We **recommend** that the ACCC consider whether CDR Consumers should receive greater transparency, before providing Use Consents and Disclosure Consents for direct marketing, about what is “in it” for an Accredited Data Recipient if they recommend/provide information about another Accredited Person (e.g. information about any arrangements/monetary benefits the Accredited Data Recipient receives if they recommend that Accredited Person).
Joint Accounts

**Recommendation 14  Control and oversight over joint account data**

We **recommend** that the ACCC consider ensuring that the CDR Rules prescribe how JAHs can have control and visibility over their joint account data once it is held by an Accredited Data Recipient.

**Recommendation 15  Reflection of options made in offline version of JAMS into the online version**

We **recommend** that the ACCC consider:

- requiring Data Holders to promptly input any disclosure option selected in an offline version of JAMS into the online version of JAMS; and

- implementing measures to ensure that the disclosure option selected in the offline version of JAMS is correctly reflected in the online version of JAMS.

**Recommendation 16  Measures in relation to vulnerable CDR Consumers**

We **recommend** that the ACCC:

- consider ensuring that the CDR Rules prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure option process in JAMS is to apply (or that a notification need not be given); and

- continue to monitor the appropriateness of the measures in place in the CDR Rules to protect vulnerable CDR Consumers, including to investigate any additional measures that could be implemented to afford further protections.
Disclosure of CDR Data and Insights to Non-Accredited Persons

**Recommendation 17** Disclose CDR Data and/or CDR Insights only to entities who comply with the APPs

We recommend that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.

**Recommendation 18** Consider measures to protect the transfer of CDR Data and CDR Insights

We recommend that the ACCC consider implementing measures to ensure that CDR Data and CDR Insights are appropriately protected during the transfer between an Accredited Person and a Trusted Adviser or Insight Recipient.

**Recommendation 19** Consider appropriateness of CDR Insights in the CDR regime

We recommend that the ACCC:

- consider:
  - whether it is appropriate for CDR Insights to be part of the CDR Regime in circumstances where there is a significant risk that vulnerable CDR Consumers may be pressured into providing an Insight Disclosure Consent, or may otherwise not fully understand the potential negative consequences that their consent may have; or
  - if the ACCC determines that it is appropriate for CDR Insights to remain within the scope of the CDR Regime, implementing mechanisms to ensure that vulnerable CDR Consumers are giving free and fully-informed Insight Disclosure Consents; and
- consider whether it is generally appropriate for CDR Insights to be generated and disclosed as part of the CDR Regime. This is because of the inherent risks associated with the disclosure of the results of the analysis of raw CDR Data.
Tiers of accreditation

Recommendation 20 Liability for affiliates

We recommend that the ACCC consider whether the CDR Rules should specify that a sponsor should be liable for the actions of their affiliates and their compliance with the legislative framework (similar to the position for an Accredited Person’s outsourced service providers).

Recommendation 21 Notification if CAP arrangement is suspended or terminated, or expires

We recommend that the ACCC consider whether there should be a requirement in the CDR Rules (or perhaps a condition of accreditation) to notify the Data Recipient Accradiator if the relevant CAP arrangement is suspended or terminated or expires, and for the Data Recipient Accradiator to have the ability to suspend or revoke the restricted accreditation in such a situation.

Recommendation 22 Mechanisms for restricted level Accredited Person to ‘switch’ enclave provider or sponsor

We recommend that the ACCC consider clarifying the mechanisms available to a restricted level Accredited Person who wishes to ‘switch’ enclave provider or sponsor after accreditation.

Recommendation 23 Requirements in relation to CAP arrangements

We recommend that the ACCC consider:

- the intended application of Rule 7.12(2)(b) to CAP arrangements for data enclave accreditation arrangements and for affiliate accreditation arrangements; and

- including matters that must be included in a CAP arrangement, including:
  - that the provider must comply with a direction by the principal in respect of redundant data;

- whether there would be benefits in broadening Rule 9.3(2)(i) to apply to providers in a CAP arrangement.
Recommendation 24 Measures in relation to Limited Data Accredited Persons

We recommend that the ACCC:

- ensure that it is satisfied that the types of CDR Data that may be handled by Limited Data Accredited Persons is appropriate, including through considering feedback received from stakeholders. This is particularly important once other sectors are introduced, and the CDR Data may (if appropriate consent is obtained) be analysed together with other information about the CDR Consumer; and

- consider whether it should clarify how a Data Holder or an Accredited Data Recipient who receives a request for CDR Data will know that the request is from, and/or made on behalf of, a Limited Data Accredited Person, and that the request is for the permitted types of CDR Data, before disclosure. This will assist in providing assurance that the Data Holder/Accredited Data Recipient will not mistakenly disclose more types of CDR Data than the Limited Data Accredited Person is permitted to handle.

Secondary Users

Recommendation 25 Clarification of rights of Secondary Users

We recommend that the ACCC consider whether further clarification in the CDR Rules is required, and/or further guidance material should be issued in relation to:

- the ability for Secondary Users to request the Accredited Data Recipient of CDR Data to further disclose that data to an additional Accredited Person, Trusted Advisor or an Insight Recipient;

- if a Secondary User Instruction is withdrawn by the Account Holder, whether an Accredited Data Recipient who has already received the CDR Data can still disclose it to another Accredited Person, a Trusted Advisor or an Insight Recipient; and

- the consequences of withdrawal or revocation of a Secondary User Instruction on authorisations that have already been given by the Secondary User.

We also recommend that the ACCC consider whether it would be appropriate to include in the legislative framework:

- a mechanism so that, where there are several individuals with account privileges for an account, all individuals are notified that a Secondary User Instruction has been given by an Account Holder;

- a requirement for Data Holders to notify the Secondary User if a relevant Secondary User Instruction has been revoked or withdrawn through its Consumer Dashboard for the Secondary User; and

- an ability for Secondary Users to authorise the disclosure of their CDR Data to Accredited Persons in situations where the account is a joint account with a co-approval option selected.
# Part C  Methodology

## 6. Our methodology

### 6.1 We conducted our PIA Update broadly in accordance with the Office of the Australian Information Commissioner’s *Guide to undertaking privacy impact assessments*. This involved the following steps:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description of steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Plan for the PIA Update:</strong> We were provided with initial instructions about the proposed amendments to the CDR Rules, including in an initial workshop with the ACCC. We were provided with a draft of the proposed amendments to the CDR Rules, to assist us to gain an understanding of the ACCC’s intentions for the proposed amendments to the CDR Rules. We also agreed on the scope of this PIA Update report (discussed further in this Part C [Methodology] below), the approach to undertaking a broader stakeholder consultation process, and the timeframes for the necessary activities involved in conducting this PIA Update report.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Project description and information flows:</strong> We prepared an initial draft Project Description for the proposed amendments to the CDR Rules, which was provided to the ACCC for review to ensure that it was complete and correct. The initial draft was refined following feedback from the ACCC.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Privacy impact analysis and compliance check:</strong> In this stage, we worked to identify and critically analyse how the proposed amendments to the CDR Rules will impact upon privacy, both positively and negatively. For the reasons elaborated in the Original CDR PIA report, we took the same approach to risk assessment which was adopted in the original CDR regime analysis, and did not endeavour to quantify or label the level of risk associated with each of the identified privacy risks.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Privacy management and addressing risks:</strong> We worked to consider potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Stakeholder consultation:</strong> A draft of a stakeholder consultation document that we prepared as a result of the above steps was published by the ACCC, together with a draft of the proposed legislative instrument to amend the CDR Rules, with an invitation to members of the public to provide written submissions in respect of either or both documents. The ACCC provided us with relevant submissions, from which we identified and considered further valuable insights.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Recommendations:</strong> From the steps referred to above, we prepared recommendations to remove or reduce identified avoidable privacy risks.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Further revision of draft PIA Update report:</strong> Following instructions from the ACCC, we undertook Steps 2-6 outlined above in relation to the introduction of the concept of secondary users into the CDR Rules.</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Report:</strong> We finalised this PIA Update report.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Respond and review:</strong> We understand that the ACCC will review this PIA Update report, in consultation with other stakeholders as required, to respond to our recommendations.</td>
</tr>
</tbody>
</table>
7. Scope of this PIA Update report

7.1 The scope of this PIA Update report is limited to the proposed changes to the CDR Rules as described in Part D [Project Description]. As was the case with the Original CDR PIA report, this document does not include consideration of:

7.1.1 the application of the CDR regime other than its initial implementation in the banking Sector; or

7.1.2 any possible future versions of the CC Act, the Open Banking Designation, the CDR Rules or the Data Standards.

7.2 Our analysis in this document has been undertaken on the basis of our understanding of the proposed amendments to the CDR Rules, and the current “point in time” status of the CC Act, CDR Rules, Data Standards and the Open Banking Designation, as at 29 September 2020.
Part D  Project Description

8. Changes to consents

8.1 As discussed in the Original CDR PIA report\(^3\), the CDR Rules (as currently drafted) provide that the CDR Consumer must provide the Accredited Data Recipient with their consent to:

8.1.1 collect their CDR Data from the Data Holder; and

8.1.2 use their CDR Data for specific purposes once it is received.

8.2 The provision of this consent constitutes a ‘valid request’ by the CDR Consumer that the Accredited Data Recipient collect their CDR Data from the relevant Data Holder (so that the Accredited Data Recipient can use the CDR Consumer’s CDR Data for the provision of goods and services).

8.3 There are several changes being proposed to the concept of “consent” in the proposed amendments to the CDR Rules. Changes to the operation of consent in the CDR regime are discussed below.

8.4 In the Original CDR PIA report, for convenience, we used “Accredited Data Recipient” to refer to an accredited person who either has, or may, receive CDR Data under the CDR Regime. As discussed in the Original CDR PIA report:

8.4.1 a person is an **Accredited Person** if they hold an accreditation under section 56CA(1) of the CC Act; and

8.4.2 a person is an **Accredited Data Recipient** of CDR Data (under section 56AK of the CC Act) if:

(a) they are an Accredited Person;

(b) the CDR Data is held by (or on behalf of) the person;

(c) the CDR Data was disclosed to the person under the CDR Rules; and

(d) the person is not a Data Holder for the CDR Data.\(^4\)

8.5 The distinction between an Accredited Person and an Accredited Data Recipient is important in relation to the proposed amendments. Accordingly, in this PIA Update report, we have used the terms Accredited Person and Accredited Data Recipient, as defined in the legislative framework.

---

\(^3\) Paragraph 15 of **Part D [Project Description]** of the Original CDR PIA report.

\(^4\) For further discussion on when an Accredited Person is an Accredited Data Recipient, please see concept (f) in **Part E [Fundamental Concepts]** of the Original CDR PIA report.
Types of consent in the CDR regime

8.6 The proposed amendments to the CDR Rules include dividing the concept of “consent” into three different categories. These three types of consent include the following:

8.6.1 **Collection Consent**, which is a consent given by a CDR Consumer for an Accredited Person to collect particular CDR Data from a CDR Participant for that CDR Data;

8.6.2 **Use Consent**, which is a consent given by a CDR Consumer for an Accredited Data Recipient of particular CDR Data to use that CDR Data in a particular way; and

8.6.3 **Disclosure Consent**, which is a consent given by a CDR Consumer for an Accredited Data Recipient of particular CDR Data to disclose that CDR Data:
   (a) to an Accredited Person in response to a Consumer Data Request (**AP Disclosure Consent**);
   (b) to a Trusted Advisor of the CDR Consumer (**TA Disclosure Consent**);
   (c) where the CDR Data is an insight (**CDR Insight**) (**Insight Disclosure Consent**); or
   (d) to an Accredited Person for the purposes of direct marketing.

8.7 In addition, the proposed amendments to the CDR Rules categorise the above types of consents, as follows:

8.7.1 Collection Consents;

8.7.2 Use Consents relating to the goods or services requested by the CDR Consumer;

8.7.3 Use Consents and Disclosure Consents relating to CDR Insights;

8.7.4 Use Consents and Disclosure Consents relating to direct marketing;

8.7.5 Use Consents to de-identify some or all of the collected CDR Data for the purpose of disclosing (including by selling) the de-identified data;

8.7.6 Use Consents relating to general research;

8.7.7 AP Disclosure Consents; and

8.7.8 TA Disclosure Consents.

8.8 We understand that an Accredited Person must, when asking a CDR Consumer for their consent, allow a CDR Consumer to provide their express consent to each of the following choices for each category of consent:

8.8.1 the types of CDR Data to which the consent will apply (for Collection Consents and Disclosure Consents);

8.8.2 the specific uses of collected CDR Data to which they are consenting (for Use Consents);

---

5 A CDR Participant for CDR Data is a Data Holder, or an Accredited Data Recipient, of the CDR Data (section 56 AL of the CC Act).

6 See paragraph 7.3 of this of this **Part B [Project Description]** for further information on CDR Insights.
8.8.3 the period of the Collection Consent, Use Consent, or Disclosure Consent; and

8.8.4 the person to whom CDR Data may be disclosed (for Disclosure Consents).

8.9 The CDR Rules currently refer to ‘consent’, which collectively refers to collection and uses of CDR Data (as captured by the new definitions of Collection Consent, and Use Consent). The concept of Disclosure Consent is new for the CDR Regime, as it will facilitate an Accredited Data Recipient being able to disclose CDR Data to new categories of persons.

**Requirements when asking for CDR Consumer’s Disclosure Consent**

8.10 The proposed amendments contain new requirements that an Accredited Person must comply with when asking for a CDR Consumer’s Disclosure Consent.

8.11 The proposed amendments specify that an Accredited Person must not ask a CDR Consumer to give a Disclosure Consent in relation to CDR Data unless the CDR Consumer has already given the Collection Consent and Use Consent required to collect, and where relevant, derive the CDR Data to be disclosed.\(^7\)

8.12 When a CDR Consumer provides a Disclosure Consent, the Accredited Person must allow the CDR Consumer to:

8.12.1 actively select the particular types of CDR Data to which the Disclosure Consent applies; and

8.12.2 choose the period of this Disclosure Consent; and

8.12.3 select the person to whom the CDR Data may be disclosed.

8.13 The proposed amendments to the CDR Rules also specify that if the Accredited Person charges the CDR Consumer a fee for disclosure of CDR Data, the Accredited Person must, when asking for the CDR Consumer’s consent:

8.13.1 clearly distinguish between the CDR Data (if any) for which a fee will be charged and the CDR Data (if any) for which a fee will not be charged; and

8.13.2 allow the CDR Consumer to actively select or otherwise clearly indicate whether they consent to the disclosure of the CDR Data (if any) for which a fee will be charged.

8.14 In addition, if the Accredited Person intends to charge a fee for the disclosure of the CDR Consumer’s CDR Data, the Accredited Person must specify the fee amount and the consequences if the CDR Consumer does not consent to the disclosure of that data.

8.15 The proposed amendments to the CDR Rules provide that an Accredited Person’s processes for asking a CDR Consumer to give or amend a Disclosure Consent is not required to accord with the Data Standards.

---

\(^7\) This does not prevent the Accredited Person from asking for a Disclosure Consent in relation to CDR Data that has yet to be collected or derived.
Amendment of a CDR Consumer’s Collection Consent, Use Consent or Disclosure Consent

8.16 The current CDR Rules do not permit a CDR Consumer to amend their consent.

8.17 The proposed amendments to the CDR Rules will permit a CDR Consumer to, at any time, amend any consents they have provided to an Accredited Person through the Accredited Person’s Consumer Dashboard. An amendment to a CDR Consumer’s consent takes effect when the CDR Consumer amends their consent (and a CDR Consumer cannot specify a different day or time for this date of effect).

Accredited Person invites CDR Consumer to amend consent

8.18 The Accredited Person may also invite a CDR Consumer to amend their consent via the Accredited Person’s Consumer Dashboard, or in writing directly to the CDR Consumer, if:

8.18.1 the amendment would better enable the Accredited Person to provide the goods or services requested by the CDR Consumer; or

8.18.2 the amendment would:

(a) be consequential to an agreement between the Accredited Person and the CDR Consumer to modify those requested goods or services; and

(b) enable the Accredited Person to provide the modified goods or services.

8.19 If an Accredited Person invites a CDR Consumer to amend the validity period of their current consent, they must not:

8.19.1 give the invitation more than a reasonable period before the current consent is expected to expire; or

8.19.2 give more than a reasonable number of such invitations within this period.

Process for amending consent

8.20 For the purposes of amending a consent, the Accredited Person may present the CDR Consumer with pre-selected options. These pre-selection options will reflect the following details of the CDR Consumer’s current consent:

8.20.1 the types of CDR Data to which the consent applies;

8.20.2 the specific uses of the CDR Data;

8.20.3 the validity period of the consent;

8.20.4 any persons to whom CDR Data may be disclosed; and

8.20.5 if the CDR Consumer has elected to the deletion of their redundant data.

---

We note that the proposed amendments, as currently drafted, also require an Accredited Person to allow a CDR Consumer to amend a consent in the same manner that it asks for a CDR Consumer to give a consent, which overlap with the requirements for this amendment to occur through the Accredited Person’s Consumer Dashboard.
8.21 When a CDR Consumer amends their consent, the Accredited Person must give the CDR Consumer:

8.21.1 a statement that indicates the consequences of amending the consent; and

8.21.2 a statement that the Accredited Person will be able to continue to use any CDR Data that has already been disclosed to it to the extent allowed by the amended consent.

8.22 The proposed amendments to the CDR Rules broaden the definitions of authorisation and consent to include any amended authorisation or consent.

expiry of consumer data request, consent and authorisation

withdrawal of authorisation

8.23 If an Accredited Person is notified by the Data Holder that the CDR Consumer’s authorisation has been withdrawn, and the Collection Consent has not expired, the Collection Consent expires when the Accredited Person receives this notification from the Data Holder.

8.24 This notification from the Data Holder would not cause the expiry of any Use Consents in relation to CDR Data already collected. However, the Accredited Person would need to notify the CDR Consumer of this fact (as specified in paragraphs 8.28 to 8.29 of this Part D [Project Description]).

revocation or surrender of accreditation

8.25 If an Accredited Person’s accreditation is revoked or surrendered, all of their Collection Consents, Use Consents and Disclosure Consents expire when the revocation or surrender takes effect.

amendment of consent validity period

8.26 As discussed in the Original CDR PIA report, a CDR Consumer’s consent expires if a particular event occurs. The proposed amendments to the CDR Rules expands on one of those situations to provide that, if the CDR Consumer has amended the validity period of their consent, that consent expires 12 months after the consent was amended (unless a listed event occurs earlier).

amendment of authorisation validity period

8.27 Similarly, the proposed amendments to the CDR Rules will mean that if a CDR Consumer has amended the validity period of their authorisation, that authorisation expires at the end of the amended validity period (unless a listed event occurs earlier).

notification to CDR Consumer if Collection Consent expires, but Use Consent does not

8.28 If a CDR Consumer’s Collection Consent expires, but their Use Consent does not, the Accredited Person must notify the CDR Consumer that they may, at any time:

8.28.1 withdraw the Use Consent; and

8.28.2 make the election to delete redundant data in respect of that CDR Data.

9 See paragraphs 15.30-15.31 of Part D [Project Description] in the Original CDR PIA report for further information.
8.29 This Accredited Person may provide this notification:

8.29.1 via its Consumer Dashboard; or

8.29.2 in writing directly to the CDR Consumer.

**Notification if Collection Consent for CDR Data is amended**

8.30 If a CDR Consumer amends their Collection Consent provided to an Accredited Person, the Accredited Person must then notify:

8.30.1 if the Collection Consent is in relation to a Data Holder Request, the Data Holder; and

8.30.2 if the Collection Consent is in relation to an Accredited Data Recipient Request, the other Accredited Data Recipient.

8.31 If a Data Holder receives a notification that the CDR Consumer’s Collection Consent has been amended (as specified in 8.30.1), the Data Holder must invite the CDR Consumer to amend their authorisation to disclose CDR Data. The Data Holder must, when inviting the CDR Consumer to amend their authorisation, comply with the CDR Rules that apply to asking a CDR Consumer to give authorisation to disclose CDR Data.

8.32 The proposed amendments also require the Data Holder to, when asking a CDR Consumer to authorise the disclosure of CDR Data or amend a current authorisation, give a CDR Consumer any information the Accreditation Register holds in relation to the Accredited Person (we understand the intention is that this may require provision of information about specific goods and services).

**Ongoing notification requirement for Collection Consents and Use Consents**

8.33 Requirements in relation to notification of current Collection Consents and Use Consents will be amended, to reflect that if 90 days have elapsed since the latest of several situations (including, as introduced by the proposed amendments, since the CDR Consumer gave their consent, or the CDR Consumer last amended their consent), the Accredited Person must notify the CDR Consumer that their Collection Consent and/or Use Consent (as relevant) is current.

**Information provided to CDR Consumers in relation to their consents**

8.34 CDR Consumers are provided with information on their consents in many forms in the CDR regime. Due to many of the changes mentioned above, the proposed amendments also include changes to the information with which a CDR Consumer must be provided. These sources of information have been grouped, as follows:

8.34.1 information provided to CDR Consumers when they provide any consent;

8.34.2 information on an Accredited Person’s Consumer Dashboard;

8.34.3 information included in a CDR receipt; and

8.34.4 information contained in an Accredited Data Recipient’s CDR Policy.

8.35 We have discussed these stages separately below.
Information provided to CDR Consumers when they give any consent

8.36 As discussed above, the proposed amendments to the CDR Rules require additional information to be provided to CDR Consumers when they are asked to provide their consent (including to reflect other changes made in the proposed amendments, such as the introduction of Disclosure Consents).

8.37 In addition, when an Accredited Person asks a CDR Consumer to provide a Collection Consent or a Use Consent, the Accredited Person must specify how the collection, or use, complies with the data minimisation principle, including how:

8.37.1 for Collection Consents, that collection is reasonably needed, and relates to no longer a time period than is reasonably needed; and

8.37.2 for Use Consents, that use would not go beyond what is reasonably needed,

in order to provide the goods or services to the CDR Consumer, or make the other uses the CDR Consumer has consented to (such as for the purposes of general research).

Information on an Accredited Person’s Consumer Dashboard

8.38 The CDR Rules, as currently drafted, contain requirements for an Accredited Person to provide CDR Consumer’s with a Consumer Dashboard that meets the requirements specified in the CDR Rules. As noted in the Original CDR PIA report, the CDR Rules provide that the Consumer Dashboard must have several functionalities, and contain certain pieces of information prescribed in the CDR Rules. Given the changes being proposed to the CDR Rules (as noted above), the proposed amendments also amend the requirements for an Accredited Person’s Consumer Dashboard.

8.39 The proposed amendments include requiring the Accredited Person’s Consumer Dashboard to have a functionality that allows a CDR Consumer, at any time, to amend or withdraw any current Collection Consents, Use Consents or Disclosure Consents.

8.40 Further, the proposed amendments will require an Accredited Person’s Consumer Dashboard to also contain the following details in relation to particular consents given by the CDR Consumer:

8.40.1 for Collection Consent or Disclosure Consent, if the consent applies over a period of time:

(a) what that period is; and

(b) how often the data has been, and is expected to be, collected or disclosed over that period;

8.40.2 for an Insight Disclosure Consent, a description of each CDR Insight disclosed, to whom it was disclosed, and when it was disclosed; and

8.40.3 details of each amendment that has been made to the consent.

---

10 For further information, please see paragraph 15.17-15.18 of Part D [Project Description] in the Original CDR PIA report.
The proposed amendments will require an Accredited Data Recipient (i.e. an Accredited Person who becomes an Accredited Data Recipient upon collection of CDR Data) to update their Consumer Dashboard to:

8.41.1 in relation to collection of CDR Data, indicate the CDR Participant\textsuperscript{12} from which the Accredited Person collected the CDR Data; and

8.41.2 in relation to disclosure of CDR Data, indicate:

(a) what CDR Data was disclosed;

(b) when the CDR Data was disclosed; and

(c) the Accredited Person to whom the CDR Data was disclosed, identified in accordance with any entry on the Accredited Register specified as being for that purpose.

Information included in a CDR receipt

8.42 As detailed in the Original CDR PIA report\textsuperscript{13}, the CDR Rules, as currently drafted, contain requirements for an Accredited Person to give a CDR Consumer a CDR receipt. The proposed amendments specify that this CDR receipt must be provided as soon as practicable after the CDR Consumer gives, amends, or withdraws, a Collection Consent, a Use Consent or a Disclosure Consent.

8.43 The proposed amendments clarify that a CDR receipt must set out, in the case of:

8.43.1 a Collection Consent, the name of each CDR Participant the CDR Consumer has consented to the collection of CDR Data from; and

8.43.2 a Disclosure Consent, the name of the person the CDR Consumer has consented to the disclosure of CDR Data to.

8.44 A CDR receipt given for an amendment of a consent must set out details of each amendment that has been made to the consent.

Information contained in an Accredited Data Recipient’s CDR Policy

8.45 Under the current CDR Rules an Accredited Data Recipient must have a CDR Policy, which must contain several pieces of information.\textsuperscript{14} The proposed amendments will also require an Accredited Data Recipient’s CDR Policy to contain, if the Accredited Data Recipient wishes to undertake general research using the CDR Data:

8.45.1 a description of the research; and

8.45.2 a description of any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.

\textsuperscript{11} The proposed amendments for lower levels of accreditation contain additional Rules about updating Consumer Dashboards. See paragraphs 8.14 to 8.16, and 8.39.2 to 8.39.3, of this Part B [Project Description].

\textsuperscript{12} The Data Holder for a Data Holder Request, or Accredited Data Recipient for an Accredited Data Recipient Request (as relevant).

\textsuperscript{13} For further information, please see paragraph 15.15-15.16 of Part D [Project Description] in the Original CDR PIA report.

\textsuperscript{14} Please see the table in Part F [Analysis of APP Application and Compliance] in the Original CDR PIA report for further information on the requirements for a CDR Policy, and the information required to be contained in that CDR Policy.
Other relevant matters

8.46 Under the current CDR Rules, an Accredited Person may not ask a CDR Consumer for consent to:

8.46.1 sell the CDR Data that it receives under the CDR regime; and

8.46.2 aggregate CDR Data for the purposes of identifying, compiling insights in relation to, or building a profile in relation to, any person who is not the CDR Consumer who made the Consumer Data Request.\(^\text{15}\)

8.47 The proposed amendments to the CDR Rules amend these restrictions, by:

8.47.1 removing the restriction on an Accredited Person asking for consent to sell CDR Data; and

8.47.2 including a restriction that an Accredited Person must not ask a CDR Consumer for consent that is not in a category of consents (i.e. the consent must fall into one of the categories specified in paragraph 8.7 of this Part B [Project Description]).

Use and Disclosure of CDR Data for the purposes of general research

8.48 The proposed amendments to the CDR Rules introduce a concept of permitting an Accredited Data Recipient to:

8.48.1 use CDR Data for the purposes of general research, in accordance with a current Use Consent for that purpose from the CDR Consumer; and

8.48.2 for the purposes of general research, disclose to the CDR Consumer any of their CDR Data.

8.49 General research is defined as research by the Accredited Data Recipient that does not relate to the provision of goods or services to any particular CDR Consumer.

8.50 In addition to the matters a CDR Consumer is asked to provide their consent to, the proposed amendments require an Accredited Person to ask for the CDR Consumer’s express Use Consent for the purposes of any general research the Accredited Person intends to undertake, and must provide a link to a description in the Accredited Person’s CDR Policy of:

8.50.1 the research to be conducted; and

8.50.2 any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.

Use of CDR Data for the purposes of de-identifying the data

8.51 As described above, a category of consent includes where an Accredited Person may ask a CDR Consumer to provide a Use Consent to de-identify some or all of the collected CDR Data for the purpose of disclosing (including by selling) the de-identified data. Accordingly, the proposed amendments permit the Accredited Data Recipient to use the CDR Consumer’s CDR Data for the purposes of de-identifying collected CDR Data for the purposes of disclosing (including by selling) the de-identified data.

\(^{15}\) As noted in the Original CDR PIA report, the CDR Rules specify some situations in which this restriction does not apply (see paragraph 15.12 of Part D [Project Description] in the Original CDR PIA report for further information).
Uses and Disclosures relating to direct marketing

8.52 In accordance with a CDR Consumer’s direct marketing Use Consent and/or Disclosure Consent, an Accredited Data Recipient may:

8.52.1 send to the CDR Consumer information about other goods or services provided by another Accredited Person, if the Accredited Data Recipient:

(a) reasonably believes that the CDR Consumer might benefit from those other goods or services; and

(b) sends such information to the CDR Consumer on no more than a reasonable number of occasions; and

8.52.2 disclose CDR Data to an Accredited Person to enable the Accredited Person to provide the goods and services specified in paragraph 8.52.1 of this Part B [Project Description], if the CDR Consumer has:

(a) given the Accredited Person:

(i) a Collection Consent to collect the CDR Data from the Accredited Data Recipient; and

(ii) a Use Consent; and

(b) given the Accredited Data Recipient a Disclosure Consent to disclose the CDR Data to the Accredited Person.

Records to be kept and maintained

Data Holder

8.53 In addition to the requirements of the CDR Rules as currently drafted, the proposed amendments to the CDR Rules require a Data Holder to keep and maintain records that record and explain:

8.53.1 amendments to authorisations to disclose CDR Data;

8.53.2 instances where the Data Holder has refused to disclose requested CDR Data and the Rule or Data Standard relied upon in refusing to disclose the CDR Data; and

8.53.3 the processes (including a video of each process) by which the Data Holder asks CDR Consumers:

(a) for their authorisation to disclose CDR Data; and

(b) for an amendment to their authorisation.

Accredited Data Recipient

8.54 In addition to the requirements of the CDR Rules as currently drafted, the proposed amendments to the CDR Rules require an Accredited Data Recipient to keep and maintain records that record and explain:

8.54.1 all consents, including, if applicable, the uses of the CDR Data that the CDR Consumer has consented to under any Use Consents;

8.54.2 amendments to consents by CDR Consumers;
8.54.3 the fact that CDR Data has been disclosed to Accredited Persons, and the identity of Accredited Persons to whom any CDR Data was disclosed;

8.54.4 the fact that CDR Data has been disclosed to Trusted Advisors, and the identity of Trusted Advisors to whom CDR Data was disclosed;

8.54.5 disclosures of CDR Insights, including a description of each CDR Insight disclosed, to whom it was disclosed and when;

8.54.6 the processes (including a video of each process) by which the Accredited Data Recipient asks CDR Consumers:

(a) for their consent; and

(b) for an amendment to their consent; and

8.54.7 any terms and conditions on which the Accredited Data Recipient offers goods or services, where the Accredited Data Recipient discloses to an Accredited Person, CDR Data in order to provide the good or service.

9. AP Disclosure Consent (and Accredited Data Recipient Requests)

9.1 Currently, the CDR Rules provide for a Consumer Data Request to be made by an Accredited Person to a Data Holder. The proposed amendments to the CDR Rules will permit an Accredited Person to make a Consumer Data Request to an Accredited Data Recipient. In summary, this means that a CDR Consumer can:

9.1.1 request an Accredited Person to collect their CDR Data from a Data Holder (who, after receiving CDR Data, will become an Accredited Data Recipient) (Data Holder Request); and

9.1.2 request an Accredited Person (A2) to collect their CDR Data from an Accredited Data Recipient (A1) (who, after receiving CDR Data, will also become an Accredited Data Recipient) (Accredited Data Recipient Request).

9.2 The concept of an Accredited Data Recipient request, as described in paragraph 9.1.2, is a new concept included in the proposed amendments to the CDR Rules, and is linked to the new concept of Disclosure Consent, as specified above in paragraph 8.7.

9.3 To accommodate the new concept of Accredited Data Recipient Requests, the proposed amendments to the CDR Rules have broadened the language used in relation to Consumer Data Requests to include collection of CDR Data from Accredited Data Recipients (as well as Data Holders). Accordingly, a number of the proposed amendments to the CDR Rules relate to expanding the language from collecting CDR Data from a Data Holder, to collecting CDR Data from CDR Participants (which, as noted above, includes Data Holders and Accredited Data Recipients of the CDR Data).
Valid Consumer Data Request

9.4 The CDR Rules in relation to valid Consumer Data Requests have been amended to reflect that division of the concept of ‘consent’ into Collection Consent, Use Consent, and Disclosure Consent. This includes specifying that an Accredited Person may ask a CDR Consumer to give the following consents, in order to provide goods and services to the CDR Consumer:

9.4.1 a Collection Consent for the Accredited Person to collect their CDR Data from the CDR Participant; and

9.4.2 a Use Consent for the Accredited Person to use that CDR Data.

Data Holder Request

9.5 The proposed amendments to the CDR Rules do contain some changes to the Rules in relation to Data Holder Requests, however a majority of these amendments are clarification of language (i.e. to reflect that ‘consent to collect and use CDR Data’ is now, under the proposed amendments, Collection Consent and Use Consent). Given these changes are not substantive, but more clarification of language, we have not discussed them in this PIA Update report.

9.6 The only substantive change to Data Holder Requests is the fact that an Accredited Person may send a Data Holder Request if, among other things, the request is valid (noting the language previously used was ‘the consent is current’).

Accredited Data Recipient Request and AP Disclosure Consent

9.7 The proposed amendments to the CDR Rules introduce a concept of Accredited Data Recipient Requests, which are requests made by an Accredited Person (A2) to an Accredited Data Recipient (A1). For clarity, the Accredited Person is not an Accredited Data Recipient until they collect the CDR Consumer’s CDR Data from either:

9.7.1 a Data Holder under a Data Holder Request; or

9.7.2 an Accredited Data Recipient under an Accredited Data Recipient Request.

9.8 Given the complexities of the AP Disclosure Consent process (and the Accredited Data Recipient Request process), we have set out below a diagram illustrating this new information flow, together with a description of each stage in the process.

---

16 The Data Holder for a Data Holder Request, or Accredited Data Recipient for an Accredited Data Recipient Request (as relevant).
AP Disclosure Consent (and Accredited Data Recipient Request) process

- **Collection Consent and Use Consent (for Data Holder Request)**
  - CDR Consumer

- **Data Holder Request**
  - Accredited Data Recipient (A1)
  - Data Holder

- **Disclosure of CDR Data**
  - Accredited Person (A2)
  - Accredited Data Recipient Request

- **Disclosure of CDR Data**

The diagram illustrates the flow of consent and data requests between the CDR Consumer, the Accredited Data Recipient (A1), the Data Holder, and the Accredited Person (A2).
In addition to a CDR Consumer providing their Collection Consent and Use Consent to an Accredited Person (A1) for a Data Holder Request, the CDR Consumer may also provide an AP Disclosure Consent to the Accredited Person (A1).

As discussed in paragraph 8.12 of this Part B [Project Description], the CDR Consumer will be able to make several choices when providing their AP Disclosure Consent.

If a CDR Consumer provides an AP Disclosure Consent at this stage, the CDR Consumer will be able to select the Accredited Person (A2) to whom the Accredited Data Recipient (A1) may disclose their CDR Data.

If the Accredited Data Recipient (A1) intends to charge the CDR Consumer a fee for the disclosure, the Accredited Data Recipient (A1) must provide the information specified in paragraphs 8.13 to 8.14 of this Part B [Project Description] to the CDR Consumer.

The CDR Consumer has the opportunity to, similar to a Data Holder Request, provide a Collection Consent and Use Consent to the Accredited Person (A2) for the Accredited Person (A2) to collect CDR Data from an Accredited Data Recipient (A1), and for the Accredited Person (A2) to use that CDR Data. As is the case when seeking consent for the purposes of a Data Holder Request, the Accredited Person (A2) has to provide the CDR Consumer with a range of information in relation to their Collection Consent and Use Consent.

The proposed amendments to the CDR Rules also broaden the concept of charging for the collection of CDR Data to apply to Accredited Data Recipient Requests, specifying that if the Accredited Data Recipient (A1) charges a fee for disclosure of CDR Data to the Accredited Person (A2), and the Accredited Person (A2) intends to pass that fee onto the CDR Consumer, the Accredited Person (A2) must, when asking for the CDR Consumer’s consent:

- clearly distinguish between the CDR Data (if any) for which a fee will be passed on and the CDR Data (if any) for which a fee will not be passed on; and
- allow the CDR Consumer to actively select or otherwise clearly indicate whether they consent to the disclosure of the CDR Data (if any) for which a fee will be passed on.

In addition, if the Accredited Person (A2) intends to pass on a fee to the CDR Consumer, the Accredited Person (A2) must specify the amount of the fee, and the consequences if the CDR Consumer does not consent to the collection of that data.

The proposed amendments to the CDR Rules provide that an Accredited Person’s processes for asking a CDR Consumer to give and amend their Collection Consent for the purposes of an Accredited Data Recipient Request is not required to accord with the Data Standards.
Accredited Person (A2) makes Accredited Data Recipient Request to Accredited Data Recipient (A1)

9.17 The Accredited Person (A2) may make an Accredited Data Recipient Request to an Accredited Data Recipient (A1) for the Accredited Data Recipient (A1) to disclose some or all of the CDR Data that:

9.17.1 is the subject to the relevant Collection Consent and Use Consent provided to the Accredited Person (A1); and

9.17.2 it is able to collect and use in accordance with the data minimisation principle.

Accredited Data Recipient (A1) asks CDR Consumer for AP Disclosure Consent (if the Disclosure Consent is not already provided) (optional)

9.18 An Accredited Data Recipient (A1) may ask a CDR Consumer for an AP Disclosure Consent in relation to an Accredited Person (A2) (in accordance with the relevant CDR Rules), if:

9.18.1 the Accredited Data Recipient (A1) receives an Accredited Data Recipient Request from an Accredited Person (A2);

9.18.2 the Accredited Data Recipient (A1) does not have a current AP Disclosure Consent from the CDR Consumer to disclose the CDR Consumer’s CDR Data to that Accredited Person (A2) (i.e. the CDR Consumer did not provide an AP Disclosure Consent at the stage specified in paragraphs 9.9 to 9.12 of this Part B [Project Description]); and

9.18.3 the Accredited Data Recipient (A1) reasonably believes that the Accredited Data Recipient Request was made by an Accredited Person on behalf an eligible CDR Consumer.

Accredited Data Recipient (A1) discloses CDR Data to Accredited Person (A2) (optional)

9.19 If the CDR Consumer provides their AP Disclosure Consent, the Accredited Data Recipient (A1) is authorised, but is not required to, disclose the CDR Consumer’s CDR Data to the Accredited Person (A2).

9.20 In summary, the Accredited Data Recipient (A1) can disclose the CDR Data to the Accredited Person (A2) if the CDR Consumer has given:

9.20.1 the Accredited Person (A2):

(a) a Collection Consent to collect the CDR Data from the Accredited Data Recipient (A1); and

(b) a Use Consent; and

9.20.2 the Accredited Data Recipient (A1) an AP Disclosure Consent to disclose the CDR Data to the Accredited Person (A2).

9.21 At this stage, Accredited Person (A2) will become an Accredited Data Recipient under the legislative framework, as the Accredited Person (A2) will meet the definition of an Accredited Data Recipient.
Withdrawal of AP Disclosure Consent

9.22 As is the case in relation to Data Holder Requests, a CDR Consumer can also withdraw the Collection Consent and Use Consent (given to the Accredited Person (A2)) and the AP Disclosure Consent (given to the Accredited Data Recipient (A1)) at any time. In addition to the requirements of the current CDR Rules, if the CDR Consumer withdraws their AP Disclosure Consent, the Accredited Data Recipient (A1) must notify the Accredited Person (A2) of the withdrawal.

Expire of Collection Consent and AP Disclosure Consent

9.23 If:

9.23.1 an Accredited Person (A2) has a Collection Consent to collect particular CDR Data from a particular Accredited Data Recipient (A1); and

9.23.2 the Accredited Data Recipient (A1) has an AP Disclosure Consent to disclose that CDR Data to that Accredited Person (A2),

and one of those consents expires, the other consent expires at the same time.

Notification if Collection Consent or AP Disclosure Consent expires for Accredited Data Recipient Request

9.24 If the Collection Consent an Accredited Person (A2) holds in relation to an Accredited Data Recipient Request expires, they must notify the Accredited Data Recipient (A1) of this expiry.

9.25 If the AP Disclosure Consent an Accredited Data Recipient (A1) holds in relation to an Accredited Data Recipient Request expires, they must notify the Accredited Person (A2) of this expiry.

10. TA Disclosure Consent

10.1 As discussed above, CDR Consumers will be able to provide a TA Disclosure Consent to the disclosure of their CDR Data from an Accredited Person to a Trusted Adviser.

10.2 The following classes of person will be eligible to become Trusted Advisers:

10.2.1 accountants;

10.2.2 lawyers;

10.2.3 tax agents;

10.2.4 BAS agents;

10.2.5 financial advisors;

10.2.6 financial counsellors;

10.2.7 mortgage brokers; and

---

17 See paragraphs 15.26 to 15.29 of Part D [Project Description] in the Original CDR PIA report for further information.

18 We note that in the proposed amendments, this Rule is titled “Notification of collection consent or use consent expires”, however we understand the intention is for the Rule to refer to situations where AP Disclosure Consents expire, rather than Use Consents.
10.2.8 any other class as approved by the ACCC.

10.3 Trusted Advisers will not be Accredited Persons.

10.4 Relevantly, the Accredited Person must not make the following a condition for the supply of the goods or services requested by the CDR Consumer:

10.4.1 the nomination of a Trusted Adviser;

10.4.2 the nomination of a particular person as a Trusted Adviser; or

10.4.3 the giving of a TA Disclosure Consent in respect of a Trusted Adviser.

10.5 However, Accredited Persons may charge CDR Consumers a fee for disclosing their CDR Data to a Trusted Adviser.

10.6 For completeness, we note that the CDR Rules will not regulate:

10.6.1 how CDR Data must be transferred to a Trusted Adviser; or

10.6.2 how a Trusted Adviser must handle that CDR Data.

11. Insight Disclosure Consent

11.1 The proposed amendments to the CDR Rules will allow CDR Consumers to provide an Insight Disclosure Consent to the disclosure of a CDR Insight by an Accredited Data Recipient to a person (Insight Recipient).

11.2 The CDR Rules will not seek to limit who can be an Insight Recipient (i.e. anyone can be an Insight Recipient).

11.3 The proposed amendments provide that a CDR Insight, in relation to the CDR Data of a CDR Consumer, means a set of data that:

11.3.1 is derived from the CDR Data;

11.3.2 has an identifier that associates it with the CDR Consumer; and

11.3.3 without that identifier, would be considered to be de-identified for the purposes of the CDR Rules.

11.4 It is intended that CDR Consumers will be able to request, from the Accredited Person, a copy of the CDR Insight about them. It is also possible that CDR Consumers may be able to see the CDR Insight before it is disclosed by the Accredited Person to the Insight Recipient.
12. New levels and kinds of accreditation

General

12.1 Under the current CDR Rules, there is only one level of accreditation (the 'unrestricted level'). However, section 56BH of the CCA Act allows the CDR Rules to provide that accreditations may be granted at different levels corresponding to different risks, including risks associated with specified classes of CDR Data, classes of activities or classes of applicants for accreditation.

12.2 The proposed amendments to the CDR Rules will introduce two new levels of accreditation, being the:

12.2.1 unrestricted level; and

12.2.2 the restricted level.

12.3 There will also be three different kinds of restricted accreditation, being:

12.3.1 data enclave accreditation;

12.3.2 limited data accreditation; and

12.3.3 affiliate accreditation.

12.4 For all applications for accreditation, an applicant will still be required to apply to the Data Recipient Accreditor, and to provide all of the information that is required by the CDR Rules. The Data Recipient Accreditor will still consider the application in accordance with the accreditation criteria specified in the CDR Rules (although different criteria will apply, depending on the relevant level and kind of accreditation).

Data enclave accreditation

12.5 We understand that:

12.5.1 the ACCC's stakeholder consultations have revealed that the cost of demonstrating compliance with the ICT and other systems requirements for handling CDR Data is one of the most significant barriers to a person seeking to be an Accredited Person; and

12.5.2 the proposed amendments are intended to address this barrier by allowing the Data Recipient Accreditor to accredit a person (the Data Enclave Accredited Person) to access and use CDR Data by leveraging the ICT and data environment of another person already accredited at the unrestricted level (the Unrestricted Accredited Person) whose environment will comply with the requirements of the CDR regime.

Applying for data enclave accreditation

12.6 The accreditation criteria for the data enclave accreditation will remain the same as for an unrestricted level applicant – that is, that the person would, if accredited, be able to comply with the obligations in Rule 5.12. Rule 5.12 will remain substantially the same as is currently the case for unrestricted level applicants, but amended so that the accredited person must:

12.6.1 take all reasonable steps to ensure that it is licensed or otherwise authorised to use any CDR logo as required by the Data Standards;
12.6.2 having regard to the fit and proper person criteria, be a fit and proper person to be accredited “at the relevant level and kind”; and

12.6.3 have adequate insurance, or a comparable guarantee, “appropriate to the level and kind”. 19

12.7 A person applying for data enclave accreditation will need to specify a proposed ‘enclave provider’ in their application and continue to have an enclave provider after being accredited (Rule 5.1B(1)).

12.8 An enclave provider must:

12.8.1 have unrestricted accreditation (i.e., they must be an Unrestricted Accredited Person);  
12.8.2 be the provider in a ‘CAP arrangement’ with the Data Enclave Accredited Person. A CAP arrangement (short for combined accredited person arrangement) is between two accredited persons, a ‘principal’ and a ‘provider’, under which the provider will perform functions on behalf of the principal. In a data enclave CAP arrangement, the Unrestricted Accredited Person will be the provider, who will make consumer data requests for CDR Data and hold the collected CDR Data on behalf of the Data Enclave Accredited Person. The CAP arrangement may also provide for the Unrestricted Accredited Person (the provider) to use or disclose CDR Data on behalf of the Data Enclave Accredited Person (the principal); and

12.8.3 be recorded on the Accreditation Register as the enclave provider of the principal.

12.9 The Data Recipient Accréditator must, if they decide to grant data enclave accreditation, notify the applicant of the name and accreditation number of the enclave provider. The enclave provider must also be entered on the Accreditation Register.

After accreditation

12.10 After accreditation, the Data Enclave Accredited Person, when asking for consent, will be required to tell the CDR Consumer that:

12.10.1 their CDR Data may be, or will be, collected by the provider under a CAP arrangement, and:

12.10.2 the provider’s name;  
12.10.3 the provider’s accreditation number; and

12.10.4 a link to the provider’s CDR Policy, with a statement that the CDR Consumer can obtain further information about such collections or disclosures from the CDR policy if desired.

12.11 It appears from the proposed amendments that the Data Enclave Accredited Person will be able to ask the CDR Consumer for consent directly, or by another person acting on behalf of the Data Enclave Accredited Person under a CAP agreement. We understand that the new Rule 4.11(4) is intended to clarify that in both cases the consent is taken to have been requested by, and given to, the Data Enclave Accredited Person.

12.12 A Data Enclave Accredited Person will only be able to make a request for CDR Data, or hold any collected CDR Data (or any data derived from that CDR Data), “through the enclave provider acting on its behalf under the CAP arrangement”.

19 We understand that guidance will be issued about these requirements.
12.13 A Data Enclave Accredited Person’s CDR Policy will need to include a list of other Accredited Persons with whom they have a CAP arrangement, the name of the Unrestricted Accredited Person who is the enclave provider, and the nature of the services provided by that provider.

12.14 Disclosing a CDR Consumer’s CDR Data to another party to a CAP arrangement (i.e., between the provider and the principal) will be a ‘permitted use or disclosure’ of the CDR Data, if this is reasonably needed for other permitted uses or disclosures.

12.15 If CDR Data may be collected by a provider under a CAP arrangement, the proposed amendments will require an Accredited Person to ensure that their consumer dashboard includes the provider’s name and accreditation number. This means that the consumer dashboard provided by a Data Enclave Accredited Person must contain the name and accreditation number of the Unrestricted Accredited Person (who is the enclave provider).

12.16 Under Privacy Safeguard 5, for the banking sector, an Accredited Person who has collected CDR Data must update their consumer dashboard. The proposed amendments will mean that this Rule will only apply to the provider under the CAP arrangement (i.e., the Unrestricted Accredited Person). The proposed amendments mean that the Unrestricted Accredited Person must indicate on the CDR Consumer’s consumer dashboard that their CDR Data was collected “by an accredited person [i.e., the Unrestricted Accredited Person] on behalf of the accredited person [i.e., the Data Enclave Accredited Person] under a CAP arrangement”.

12.17 Similarly, in relation to Privacy Safeguard 10, the current CDR Rules contain requirements for a Data Holder to update a CDR Consumer’s consumer dashboard if they disclose CDR Data to an Accredited Data Recipient. The proposed amendments clarify that if the Data Holder discloses CDR Data to an Accredited Data Recipient (i.e., the Data Enclave Accredited Person) “through another accredited person action on its behalf under a CAP arrangement” (i.e. Unrestricted Accredited Person as the enclave provider), only the enclave provider should be listed on the consumer dashboard.

12.18 Under Privacy Safeguard 11, a Data Holder is required to identify to the CDR Consumer the Accredited Person to whom the CDR Data was disclosed. The effect of the proposed amendments is that this requirement only relates to the provider (i.e., the Unrestricted Accredited Person).

12.19 For Privacy Safeguard 12 in relation to redundant data, the current CDR Rules set out steps that must be taken if (among other things) the Accredited Person thinks it appropriate in the circumstances to de-identify rather than delete CDR Data. The proposed amendments will clarify that such a decision must be taken by the principal of a CAP arrangement (i.e., the Data Enclave Accredited Person), who must give certain directions to any provider under the CAP arrangement that “has been provided with a copy of the redundant data”.

12.20 An Accredited Data Recipient is required to keep and maintain certain records. The proposed amendments will extend these requirements to include “any CAP arrangement … in which the accredited data recipient is the principal, including how the provider will use or manage any CDR data shared with it”.
12.21 There are also some changes to the application of Schedule 2, including a new provision in relation to Part 2.2(7) about implementation and maintenance of a third-party management framework (discussed below in paragraph 12.45 below). The enclave provider (Unrestricted Accredited Person) and the Data Enclave Accredited Person will be required to comply with different requirements of Schedule 2, as indicated in the table below:

<table>
<thead>
<tr>
<th>Schedule 2 requirement</th>
<th>Unrestricted Accredited Person (also an enclave provider)</th>
<th>Data Enclave Accredited Person must comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 (Purpose of Part) and 1.2 (interpretation)</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>1.3 (Step 1—Define and implement security governance in relation to CDR data)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>1.4 (Step 2—Define the boundaries of the CDR data environment)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>1.5 (Step 3—Have and maintain an information security capability)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>1.6 (Step 4—Implement a formal controls assessment program)</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>1.7 (Step 5—Manage and report security incidents)</td>
<td>✅</td>
<td>Paragraphs 1.7(b) and (c) only</td>
</tr>
<tr>
<td>In respect of itself</td>
<td>In respect of the enclave</td>
<td></td>
</tr>
<tr>
<td>2.1 (Purpose of Part)</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>2.2 (1) (a) to (i) (An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>2.2 (2) (a) to (e) (An accredited data recipient of CDR data must take steps to secure their network and</td>
<td>✅</td>
<td>Paragraph (d) only (re hardening of end-user devices)</td>
</tr>
<tr>
<td>Schedule 2 requirement</td>
<td>Unrestricted Accredited Person (also an enclave provider)</td>
<td>Data Enclave Accredited Person must comply</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>systems within the CDR data environment).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 (3) (a) to (c) (An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2.2 (4) (a) to (c) (An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In relation to the devices the person uses to access the data enclave, or host the network from which it accesses the data enclave</td>
</tr>
<tr>
<td>2.2 (5) (a) to (c) (An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In relation to the devices the person uses to access the data enclave</td>
</tr>
<tr>
<td>2.6 (a) to (c) (An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>2.7 (a) (Third party management)</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

12.22 We understand that the changes to Schedule 2 have been developed in accordance with cybersecurity advice obtained by the ACCC.
12.23 A Data Enclave Accredited Person is required to provide annual assurance assessments and attestation reports to the Data Recipient Accradiator, which are less onerous than the similar reports required to be provided by an Unrestricted Accredited Person. The enclave provider (i.e., the Unrestricted Accredited Person) must also provide regular enclave attestation reports to the Data Recipient Accradiator about the Data Enclave Accredited Person’s compliance with Schedule 2.

Revocation and suspension of accreditation

12.24 In addition to existing situations for revocation, suspension or surrender of accreditation, an Accredited Person’s data enclave accreditation may be suspended or revoked by the Data Recipient Accradiator if the accreditation of the provider in the CAP arrangement (i.e., the Unrestricted Accredited Person) is suspended or revoked.

12.25 Before any revocation, the Data Recipient Accradiator must also notify the enclave provider if the principal’s accreditation is being revoked, or the principal if the enclave provider’s accreditation is being revoked.

Summary of enclave accreditation process

12.26 To assist with understanding this new process, we have set out below an information flow diagram.
Data enclave accreditation - CAP arrangement

- "Unrestricted" Accredited Data Recipient (Provider)
- Enclave
- Data Holder Request (on behalf of the principal)
- Disclosure of CDR Data
- Access to CDR Data
- Data Holder Request
- Collection Consent and Use Consent (for Data Holder Request)
- "Restricted" Accredited Person (Principal)
Limited data accreditation

12.27 As for data enclave accreditation, the criterion for limited data accreditation will be the same as that currently applicable for an unrestricted level applicant. That is, that the person would, if accredited, be able to comply with the obligations in Rule 5.12 (as discussed in paragraph 12.6 above).

12.28 A person with limited data accreditation (Limited Data Accredited Person) will only be permitted to collect CDR data of a kind specified in a Schedule to the CDR Rules.

12.29 For the banking sector, the CDR Rules will specify the following kinds of CDR Data as data may be collected by a Limited Data Accredited Person:

   12.29.1 “Basic Bank Account Data”;
   12.29.2 “Basic Customer Data”;
   12.29.3 “Detailed Bank Account Data”;
   12.29.4 “Bank Payee Data”; and
   12.29.5 “Bank Regular Payments”,

with these terms having the same meaning as in the Data Standards. We understand that these categories of CDR Data have been identified as representing ‘low’ to ‘medium’ risk categories by the ACCC’s ICT security advisers.

12.30 A Limited Data Accredited Person will have substantially the same obligations in relation to the CDR Data environment protections in Schedule 2 of the CDR Rules as an Unrestricted Accredited Person. A Limited Data Accredited Person will only be required to comply with:

   12.30.1 all requirements in Part 1 of Schedule 2 (i.e., except for the interpretation clauses in 1.1 and 1.2); and
   12.30.2 all requirements in Part 2 of Schedule 2 (except the new Part 2.2(7) in relation to third party management, which is discussed further below in paragraph 12.45).

12.31 After accreditation, the types of CDR Data that a Limited Data Accredited Person will be permitted to handle will be restricted, but a Limited Data Accredited Person will have the same obligations as an Unrestricted Accredited Person in relation to the collection, use and disclosure that CDR Data.

Affiliate accreditation

12.32 The third new kind of restricted accreditation is affiliate accreditation.

Applying for affiliate accreditation

12.33 The proposed amendments introduce new criterion for affiliate accreditation, being that:

   12.33.1 the applicant has a ‘sponsor’ (as described in paragraph 12.37 below); and
   12.33.2 the sponsor certifies that the applicant meets the accreditation criteria (which are the same as for an unrestricted level applicant – as discussed in paragraph 12.6 above).
12.34 This means that there is no requirement for the applicant to demonstrate to the Data Recipient Accreditor that they meet the requirements in Rule 5.12 (including that they are a ‘fit and proper person’ and have appropriate internal and external dispute resolution processes).

12.35 A person applying for affiliate accreditation must specify a proposed sponsor in their application and, once accredited, must continue to be an affiliate of a sponsor.

12.36 A person applying for affiliate accreditation must specify a proposed sponsor in their application.

12.37 To be a sponsor of an affiliate, a person must:

12.37.1 have unrestricted accreditation (i.e. they must be an Unrestricted Accredited Person);

12.37.2 be recorded on the Accreditation Register as the sponsor of the affiliate; and

12.37.3 agree to take reasonable steps to ensure that the affiliate complies with its obligations as an Accredited Person,

and the affiliate must undertake to provide the sponsor with information and access to its operations as is needed for the sponsor to fulfil its obligations as sponsor.

12.38 Under the proposed amendments to the CDR Rules, sponsors (i.e. the Unrestricted Accredited Person) and affiliates (i.e. the Restricted Accredited Person), will be able to make Consumer Data Requests, and handle CDR Data, in accordance with two different arrangements:

12.38.1 through the process described in paragraph 9 of this Part B [Project Description], in which:

(a) the affiliate receives a Collection Consent and Use Consent from a CDR Consumer for an Accredited Data Recipient Request;

(b) the sponsor receives an AP Disclosure Consent from the CDR Consumer; and

(c) the sponsor then discloses the CDR Data that it holds to the affiliate;

12.38.2 under a CAP arrangement (as described in paragraph 12.8.2 of this Part B [Project Description]), in which:

(a) the affiliate is the principal and the sponsor is the provider;

(b) the sponsor (provider) will do either or both of:

(i) making consumer data requests on behalf of the affiliate; or

(ii) disclosing CDR Data that it holds as an Accredited Data Recipient to the affiliate in response to a consumer data request; and

(c) the sponsor (provider) may also use or disclose CDR Data on behalf of the principal.

12.39 If accreditation is granted to the affiliate, the Data Recipient Accreditor must notify the applicant of the name and accreditation number of the sponsor. It must also ensure the sponsor is included on the Accreditation Register.
12.40 After accreditation, a person with affiliate accreditation (affiliate) may only make a consumer data request:

12.40.1 “through the sponsor acting on its behalf under a CAP arrangement”; or

12.40.2 to the sponsor (where the sponsor is an Accredited Data Recipient of the CDR Data).

12.41 A sponsor will be required take reasonable steps to ensure that the affiliate complies with its obligations as an Accredited Person.

12.42 As for data enclave arrangements, for affiliate arrangements involving a CAP arrangement:

12.42.1 the affiliate must ensure that their CDR policy contains information in relation to their CAP arrangement with the sponsor, and the sponsor will also be required to include similar information in relation to their CAP arrangement with the affiliate (as described in paragraph 12.13 above);

12.42.2 the Rules in relation to Privacy Safeguard 5 (about updating the consumer dashboard) only apply to the sponsor, who must update their consumer dashboard to show that the CDR Data was collected by the sponsor on behalf of the affiliate under a CAP arrangement (as described in paragraph 12.16 above);

12.42.3 the Rules in relation Privacy Safeguard 10 only apply to the sponsor, and the sponsor should not be listed on the Data Holder’s consumer dashboard as the entity to whom the CDR Data has been disclosed (as described in paragraph 12.17 above);

12.42.4 under Privacy Safeguard 11, a Data Holder will only be required to identify to the CDR Consumer the sponsor to whom the CDR Data was disclosed; and

12.42.5 for the purposes of Privacy Safeguard 12 in relation to redundant data, it is the affiliate (i.e., the principal under the CAP arrangement) who must think it appropriate in the circumstances to de-identify rather than delete CDR Data. The affiliate must give certain directions to any sponsor that has been provided with a copy of the redundant data.

12.43 Disclosing a CDR Consumer’s CDR Data to another party to a CAP arrangement (i.e., between the sponsor and the affiliate) is a ‘permitted use or disclosure’ of the CDR Data, if this is reasonably needed for other permitted uses or disclosures.

12.44 Some changes to the requirements in Schedule 2 are also proposed for affiliate accreditation.

12.45 An Unrestricted Accredited Person, who is also a sponsor, must comply with all requirements of Schedule 2. This includes new requirements in Part 2.2(7) about implementation and maintenance of a third–party management framework. This requires management of third parties, including affiliates, in line with a defined third-party management framework (which should include due diligence before establishing new relationships or contracts, contractual arrangements which are reflective of responsibilities for the CDR data and data environment, annual review and assurance activities, reporting requirements and post-contract requirements).
12.46 The requirements to comply with Schedule 2 are summarised in the table below:

<table>
<thead>
<tr>
<th>Schedule 2 requirement</th>
<th>Unrestricted Accredited Person (also a sponsor)</th>
<th>Affiliate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 (Purpose of Part) and 1.2 (interpretation)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>1.3 (Step 1—Define and implement security governance in relation to CDR data)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>1.4 (Step 2—Define the boundaries of the CDR data environment)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>1.5 (Step 3—Have and maintain an information security capability)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>1.6 (Step 4—Implement a formal controls assessment program)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>1.7 (Step 5—Manage and report security incidents)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>2.1 (Purpose of Part)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>2.2 (1) (a) to (i) (An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment)</td>
<td>✔️ Par (i) only (encryption in transit)</td>
<td>✔️</td>
</tr>
<tr>
<td>2.2 (2) (a) to (e) (An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment).</td>
<td>✔️ Par (d) only (re hardening of end-user devices)</td>
<td>✔️</td>
</tr>
</tbody>
</table>
### Schedule 2 requirement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Unrestricted Accredited Person (also a sponsor)</th>
<th>Affiliate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2 (3) (a) to (c)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 (4) (a) to (c)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 (5) (a) to (c)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(An accredited data recipient must take steps to limit prevent, detect and remove malware in regard to their CDR data environment)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6 (a) to (c)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.7 (a)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Third party management)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Revocation and suspension of accreditation**

12.47 In addition to existing situations for revocation, suspension or surrender of accreditation, affiliate accreditation may be suspended or revoked by the Data Recipient Accréditeur if the accreditation of the Accredited Person’s sponsor is suspended or revoked.

12.48 Before any revocation of the sponsor’s accreditation, the Data Recipient Accréditeur must also notify the affiliate. Similarly, before any revocation of the affiliate’s accreditation, the Data Recipient Accréditeur must notify the sponsor.

**Summary of affiliate accreditation process**

12.49 To assist with understanding this new process, we have set out below information flow diagrams (one for where there is a CAP arrangement, and one involving AP Disclosure Consents).
Affiliate accreditation - AP Disclosure Consent process

CDR Consumer → "Unrestricted" Accredited Data Recipient (Sponsor)

"Unrestricted" Accredited Data Recipient (Sponsor) → "Restricted" Accredited Person (Affiliate)

Collection Consent and Use Consent (for Accredited Data Recipient Request)

AP Disclosure Consent (for Accredited Data Recipient Request)

Disclosure of CDR Data
13. **Joint Account Holders**

13.1 The current CDR Rules include provisions relating to joint accounts. Importantly, the current CDR Rules provide that a Data Holder who could be required to disclose CDR Data that relates to a joint account must provide a Joint Account Management Service (JAMS), to be delivered in accordance with the Data Standards. JAMS must be provided online, and if there is a Data Holder Dashboard for the joint account, may be included in the dashboard. JAMS may also, but need not, be provided offline.

13.2 JAMS can be used by CDR Consumers who are Joint Account Holders (JAHs) to indicate the disclosure option they would like to apply to their joint account/s (i.e. a disclosure option must be selected to apply to an account, through JAMS, prior to that account appearing in the authorisation process). JAMS must give effect to a disclosure option applying, or no longer applying, as soon as practicable after a JAH has selected a disclosure option in JAMS.

13.3 No information is currently provided during the authorisation process to explain to CDR Consumers how to select a disclosure option in JAMS.

13.4 To ensure that CDR Consumers are provided with sufficient guidance regarding joint accounts and selecting a disclosure option in JAMS, such that they can make informed decisions about their joint accounts, a number of amendments to the CDR Rules have been proposed. These proposed amendments to the joint account mechanisms in the CDR regime are discussed below.

**Selecting a disclosure option in JAMS to occur during the authorisation process**

13.5 The proposed amendments to the CDR Rules will include the ability for CDR Consumers who are JAHs to select a disclosure option in JAMS during the authorisation process. CDR Consumers will be permitted to select a disclosure option in JAMS during the authorisation process, however it will not be mandatory. CDR Consumers will still be able to select a disclosure option in JAMS at other times, and through other processes, in accordance with the CDR Rules.

13.6 Whilst going through the authorisation process, the first JAH (JAH A) will be able to select a disclosure option in JAMS. When JAH A selects a disclosure option, it will trigger a notification to the second JAH (JAH B), inviting them to select a corresponding disclosure option in JAMS. Importantly, the proposed amendments to the CDR Rules will allow there to be multiple holders of a joint account (i.e. more than two people will be permitted to be joint account holders). As such, all references in this PIA Update report to JAH B refer to one or more JAH Bs, unless expressly noted otherwise.

13.7 Irrespective of whether JAH A selects a disclosure option in JAMS, the relevant Data Holder will be able to share CDR Data with the Accredited Data Recipient on JAH A’s non-joint accounts, and JAH A will receive the relevant goods or services for those accounts. However, the Data Holder will require both JAH A and JAH B to select the same disclosure option in JAMS before JAH A can receive goods or services in relation to the joint account/s from the Accredited Data Recipient (i.e. no CDR Data on the joint account/s can be shared until the same disclosure option in JAMS is selected by JAH B).

13.8 The only instance in which CDR Data on a joint account can be shared without the approval of JAH B, is if the Data Holder considers it is necessary to avoid seeking the approval of JAH B in order to prevent physical or financial harm or abuse to JAH A.
Notifications to JAH B and instructions for how to select a disclosure option in JAMS

13.9 As discussed above, the proposed amendments to the CDR Rules mean that once JAH A has selected a disclosure option in JAMS, the Data Holder must notify JAH B that JAH A has selected a disclosure option and invite JAH B to select a corresponding disclosure option in JAMS. The notification to JAH B must be made through the Data Holder’s ordinary methods for contacting JAH B (e.g. in person or via an email). This notification must:

13.9.1 provide an outline of what the consumer data right is;

13.9.2 inform JAH B of the disclosure option that JAH A has selected, or otherwise inform JAH B that JAH A has indicated that they would not like any disclosure option to apply to the relevant joint account;

13.9.3 inform JAH B that, at present, no disclosure option applies to the account;

13.9.4 explain to JAH B that no disclosure option will apply to the account unless both JAH A and JAH B have selected the same disclosure option to apply;

13.9.5 invite JAH B to make the same disclosure option as JAH A in respect of the relevant joint account; and

13.9.6 if JAH A did select a disclosure option, identify the relevant accredited person to whom JAH A would like to disclose CDR Data in respect of the relevant joint account.

Additional requirements on JAMS to ensure informed decisions are made

13.10 The proposed amendments to the CDR Rules will require Data Holders to include further information on JAMS to assist CDR Consumers who are JAHs to make informed decisions about disclosure options. Data Holders will be required to ensure that JAMS includes information about:

13.10.1 the difference between the ‘pre-approval’ option and ‘co-approval’ option (including the impact of each decision), if the Data Holder offers both ‘pre-approval’ and ‘co-approval’ disclosure options. We understand that:

   (a) the ‘pre-approval’ option means, if both JAH A and JAH B select the ‘pre-approval’ option, a Data Holder will be able to disclose CDR Data to an Accredited Data Recipient in relation to the relevant joint account if only one JAH has authorised that disclosure (i.e. the other JAH will not need to also authorise that disclosure); and

   (b) the ‘co-approval’ option means that, if both JAH A and JAH B select the ‘co-approval’ option, both JAH A and JAH B will be required to authorise the Data Holder to disclose CDR Data in respect of a relevant joint account to an Accredited Data Recipient;

13.10.2 the impact of a disclosure option if the Data Holder offers, and both JAH A and JAH B select in JAMS, the ‘pre-approval’ or the ‘co-approval’ option;

13.10.3 that if JAH A and JAH B do not select the same disclosure option to apply to the joint account, disclosure of joint account data relating to the account will ordinarily not be allowed under the CDR Rules;

13.10.4 the fact that both JAH A and JAH B can remove their disclosure option selection in JAMS at any time (independently of each other), the process for removing the selection, and the impact of this withdrawal; and
13.10.5 the fact that when the CDR Data on the joint account is disclosed by a Data Holder to an Accredited Data Recipient, both JAH A and JAH B will ordinarily be able to see information about the authorisation on their Data Holder Consumer Dashboard (as is required by the CDR Rules), for both disclosure options (subject to the discussion below).

13.11 We understand that the CDR Rules will require Data Holders to offer the pre-approval option on joint accounts, but Data Holders may also choose to offer the co-approval option.

Selecting a disclosure option for Consumer Data Requests to Data Holders

13.12 If a Data Holder asks JAH A to authorise disclosure following receipt of a Consumer Data Request, and JAH A has not previously selected a disclosure option to apply to the account, the Data Holder must ask JAH A to select a disclosure option in JAMS, in accordance with the Data Standards.

13.13 If JAH A selects a disclosure option in JAMS, the Data Holder must, through its ordinary methods for contacting JAH B:

13.13.1 notify JAH B that an Accredited Person has made a Consumer Data Request, on behalf of JAH A, that relates to the relevant joint account;

13.13.2 explain to JAH B that JAH A has authorised the disclosure of the joint account data, and that a co-approval option applies to the joint account;

13.13.3 notify JAH B of:

(a) the name of the Accredited Person that made the request;

(b) the period of time to which the CDR Data that is the subject of the request relates;

(c) the types of CDR Data for which the Data Holder is seeking an authorisation to disclose;

(d) whether the authorisation is being sought for the disclosure of CDR Data on a single occasion, or over a period of time of not more than 12 months; and

(e) if the disclosure is over a period of time, what that period of time is, insofar as these matters relate to the relevant Consumer Data Request;

13.13.4 ask JAH B whether they approve of the joint account data being disclosed;

13.13.5 advise JAH B the time by which the Data Holder needs JAH B to provide this approval;

13.13.6 inform JAH B that they may, at any time, remove the approval;

13.13.7 provide JAH B with instructions for how to remove their approval; and

13.13.8 explain to JAH B the consequence of removing the approval.

13.14 Relevantly, JAH B may remove their approval at any time, regardless of whether that approval was expressly given under a co-approval option, or whether a pre-approval option applies.
13.15 The Data Holder may only disclose joint account data if JAH A has authorised the Data Holder to disclose the relevant CDR Data and:

13.15.1 a pre-approval option applies to the joint account, and JAH B has not removed this approval via their Consumer Dashboard; or

13.15.2 a co-approval option applies to the joint account, and:

(a) JAH B has approved the disclosure of the CDR Data within the relevant timeframe, and JAH B has not removed this approval via their Consumer Dashboard; or

(b) the Data Holder considers it necessary to avoid seeking the approval of JAH B in order to prevent physical or financial harm or abuse to JAH A; or

13.15.3 no disclosure option applies to the joint account and the Data Holder considers it necessary to avoid inviting JAH B to choose a disclosure option in order to prevent physical or financial harm or abuse to JAH A.

13.16 For completeness, the proposed amendments to the CDR Rules will also require Data Holders to notify JAHs in a number of circumstances relating to Consumer Data Requests. The Data Holder must:

13.16.1 notify JAH A, and any other JAH B, through its ordinary means of contacting JAH A, if:

(a) JAH B gives, amends or removes a particular approval through their Consumer Dashboard; or

(b) JAH B does not provide an approval within the relevant timeframe;

13.16.2 notify JAH B, through its ordinary means of contacting JAH B, if JAH A gives, amends or removes a particular authorisation through their Consumer Dashboard; and

13.16.3 if JAH A amends an authorisation relating to a particular approval notify JAH B (through its ordinary methods for contacting JAH B) of:

(a) the nature of the amendments; and

(b) how JAH B may remove an approval to prevent further CDR data relating to the joint account being disclosed.

13.17 However, these notifications are not required if the Data Holder considers it necessary to avoid making the notification to a JAH to prevent physical or financial harm or abuse to another JAH.

Data Holder Consumer Dashboard

13.18 Currently, the CDR Rules require Data Holders to provide Consumer Dashboards for CDR Consumers. The current CDR Rules prescribe that a Data Holder’s Consumer Dashboard must contain particular functionalities and information. Importantly, a Data Holder’s Consumer Dashboard is currently required to include the details of each authorisation to disclose CDR Data (i.e., details of the Accredited Data Recipient receiving the CDR Data from the Data Holder) and of the types of CDR Data that have been authorised to be disclosed to that Accredited Data Recipient.
13.19 In the proposed amendments to the CDR Rules, if JAH A is authorising a Data Holder to disclose CDR Data that is customer data in relation to a joint account, details of that CDR Data are not required to be included in the equivalent Data Holder Consumer Dashboard for JAH B. For example, JAHs will not be able to see the personal information (i.e. name and address) of another JAH.

13.20 If the JAHs have selected the ‘pre-approval’ option in relation to a joint account, JAH A can withdraw their authorisation through normal processes provided for in the CDR regime. This includes through the Data Holder Consumer Dashboard (noting that this must allow JAH A to withdraw their authorisation at any time, and notify them of the impact of such a withdrawal). If JAH A withdraws their authorisation, the Data Holder will no longer be able to disclose the CDR Data in relation to the joint account, and the corresponding consent provided to the Accredited Data Recipient will expire at the same time as when JAH A withdraws their authorisation.

13.21 The effect of a ‘pre-approval’ selection is that JAH B will not be able to withdraw their authorisation (as it will have been provided by JAH A), but JAH B will be able to withdraw their disclosure option selection, effectively withdrawing their permission to the sharing of information in relation to their joint account with JAH A. This will result in the Data Holder no longer being able to disclose the CDR Data in relation to the joint account. The proposed amendments to the CDR Rules will accordingly require the equivalent Data Holder Consumer Dashboard for JAH B to outline the process for JAH B to withdraw their JAMS election, and the impact of such a withdrawal.

**Remove restrictions on showing joint accounts during the authorisation process**

13.22 The proposed amendments to the CDR Rules will remove the current restriction on Data Holders which requires them not to show any joint account during the authorisation process unless a prior disclosure option has been selected. As such, Data Holders will be able to show joint accounts during the authorisation process, even if a disclosure option has not yet been selected by both JAHs.

**Restriction on amendments to JAMS**

13.23 The proposed amendments to the CDR Rules, in respect of JAMS, will prohibit Data Holders from:

13.23.1 adding anything to the JAMS process beyond those requirements specified in the CDR Rules and the Data Standards;

13.23.2 offering additional or alternative services as part of the process;

13.23.3 including or referring to other documents, or providing any other information, so as to reduce comprehensibility; or

13.23.4 offering any pre-selected disclosure options.

**Summary of JAMs**

13.24 To assist with understanding this new process, we have set out below an information flow diagram.

---

20 We understand that the Data Standards will also prohibit the personal information of another individual being shown on a CDR Consumer’s Data Holder Consumer Dashboard.
CDR Consumer (JAH A) and CDR Consumer (JAH B) select a disclosure option in JAMS (and authorise Data Holder)

CDR Consumer (JAH A) → Disclosure option in JAMS → Data Holder

Gives authorisation for Data Holder to disclose CDR Data

Data Holder → Disclosure option in JAMS → CDR Consumer (JAH B)

Gives authorisation for Data Holder to disclose CDR Data (if a co-approval option applies)

CDR Consumer (JAH B)
14. **Secondary Users**

14.1 The CDR Rules only permit an ‘eligible’ account holder (Account Holder) to authorise the Data Holder to disclose their CDR Data to Accredited Persons. The proposed changes to the CDR Rules will allow authorisations to be given by an individual (a Secondary User) who:

14.1.1 is not themselves the Account Holder for the relevant account;

14.1.2 but:

(a) has ‘account privileges’ in relation to the Account Holder’s account (account privileges will be defined separately for each designated sector in which the CDR regime will be implemented, and for the banking sector this is discussed in paragraph 14.2 below); and

(b) is approved by the Account Holder to share CDR Data relating to the account with Accredited Persons, through the Account Holder providing the Data Holder with an instruction to treat the person as a secondary user for the purposes of the CDR Rules (Secondary User Instruction).

14.2 For the initial implementation of the CDR regime in the banking sector, an individual will have account privileges if they are:

14.2.1 18 years or older;

14.2.2 able to make transactions on an account; and

14.2.3 ‘eligible’, meaning that the individual must have access to an account with the Data Holder that is open and accessible online²¹, and if the account is a joint account, a pre-approval option applies to that account (as discussed in paragraph 13.10.1(a) of this Part D [Project Description]).

14.3 Secondary Users will be eligible CDR Consumers in their own right under the legislative framework, as Secondary Users will fall within the definition of CDR Consumers for CDR Data under section 56AI of the CCA Act, and the proposed amendments expand the definition of ‘eligible’ to include a CDR Consumer who is a ‘secondary user for an account with the Data Holder’.

14.4 Accordingly, Secondary Users will be afforded the rights and protections found in the legislative framework as they apply to CDR Consumers (for example, they will be required to be provided with Consumer Dashboards by both Data Holders and Accredited Persons, and will be protected by the Privacy Safeguards).

**Requirements for Data Holder Consumer Dashboards and online services**

14.5 If the Account Holder has an account which has a Secondary User, the proposed amendments to the CDR Rules require the Data Holder to provide the Account Holder with:

14.5.1 an online service that provides the Account Holder with the ability to:

(a) make Secondary User Instructions; and

---

²¹ For completeness, we note that in the banking sector, a Secondary User will not become eligible unless they have been given online access to the account, however the Account Holder’s Secondary User Instruction may be provided prior to the Secondary User actually having this online access.
(b) revoke Secondary User Instructions; and

14.5.2 an online service or a Consumer Dashboard that:

(a) specifies details of each authorisation to disclose CDR Data given by the Secondary User; and

(b) allows the Account Holder to withdraw any Secondary User Instruction at any time.

**Joint Accounts and Secondary Users**

14.6 As discussed above in paragraph 14.2.3, for a Secondary User to be eligible (therefore meaning they have account privileges) in relation to an account that is a joint account, a pre-approval option must apply to that account. Accordingly, a Secondary User for a joint account will not be eligible to ask an Accredited Person to make a consumer data request on their behalf unless this pre-approval option applies to the joint account.
Part E  Analysis of Risks

15. Overview

15.1 This Part E contains our analysis of the risks that we have identified as a result of the proposed amendments to the CDR Rules.

15.2 For convenience, we have grouped the following information flows and concepts, which may involve new or changed privacy considerations in addition to those identified in the Original CDR PIA report:

15.2.1 general risks that are relevant to all of the information flows and concepts;

15.2.2 changes to consents;

15.2.3 the disclosure of CDR Data to Accredited Persons (through AP Disclosure Consents and Accredited Data Recipient Requests);

15.2.4 the disclosure of information relating to CDR Consumers to non-accredited persons (through TA Disclosure Consents and Insight Disclosure Consents);

15.2.5 the introduction of new levels and kinds of accreditation;

15.2.6 changes to joint accounts; and

15.2.7 the introduction of Secondary Users being able to authorise the sharing of CDR Data.

15.3 We have described and considered the privacy risks associated with these information flows and concepts in the tables below, including stakeholder views in relation to those identified risks. We have also identified some of the key existing mitigation strategies that have been included in the legislative framework underpinning the CDR regime, or are intended to be included in the proposed amendments to the CDR Rules, together with our analysis of, and recommendations to mitigate, any identified gaps.

Please see Part D [Project Description] for further information on each of the information flows/concepts.
## General risks

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Complexity of the proposed amendments</td>
<td></td>
<td>The complexities of the proposed amendments raise privacy risks associated with:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• entities participating in the CDR regime (such as Data Holders, Accredited Persons and Accredited Data Recipients) not understanding, or taking steps to implement, their obligations under the legislative framework;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• the protections for CDR Consumers (built into the legislative framework) not being appropriately applied to CDR data, the result being that any risk of mishandling of CDR Data is not proactively managed. Instead breaches of the framework will need to be reactively managed by the regulator(s) after the CDR Consumer has been exposed to harm (which is likely to involve additional time and resources for the regulators); and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• CDR Consumers not understanding the operation of the legislative framework, meaning that they may:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o not be properly informed before giving relevant consents; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o be unlikely to know whether a particular action by an entity breaches their privacy rights.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The complexities 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.</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We recommend that the ACCC:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• continue to refine the drafting of the CDR Rules;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• issue detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules, as amended by the proposed changes. We suggest that different forms of guidance could be developed and specifically tailored to assist:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o CDR Consumers;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o applicants for accreditation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o Data Holders;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o Accredited Persons for each level of accreditation; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o enclave providers and sponsors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Recommendation 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The majority of stakeholders who provided submissions supported this Recommendation, with stakeholders making the following statements:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NAB stated that: <em>The CDR regime is already extremely complex to navigate and the proposed changes are significant – including additional categories of consent, complex information flows, new frameworks for participation and new definitions. CDR participants have previously raised concerns regarding ascertaining and understanding compliance obligations. NAB is concerned that the additional complexity will lead to consumer confusions, compliance challenges for small ADIs and uncertainty for ADRs</em>.</td>
</tr>
</tbody>
</table>
## GENERAL RISKS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
| 1.  | Lack of clarity around collection, use, holding and disclosure of CDR Data |                                | • The **Customer Owned Banking Association** stated that: “…there are still some aspects of the current Rules that haven’t been adequately addressed in terms of guidance and detail and it would be more beneficial for the focus to be on filling these gaps before moving to expansion of the Rules, which would instead create even more gaps and questions”.

• The **Financial Rights Legal Centre** stated that: “The complexity of the consent regime will make it extremely difficult for industry participants to understand the regime and their obligations at each and every step of the new information flows. This is likely to lead to consumer data being mishandled, not being protected appropriately, or actively managed that serves the consumer’s interest. The more breaches and mistakes, the more the regulatory bodies will need to supervise and retrospectively regulate, and the more likely consumers will lose trust in the regime and either avoid taking part or withdraw from the regime altogether.”

• The **OAIC** stated that: “… the draft Rules also proposed to introduce four kinds of ‘disclosure consents’. The draft Rules further divide these (and collection and use consents) into ‘categories’ of consents. Rule 4.11(1)(c) requires an ADR to ask for the consumer’s express consent for particular matters in relation to each category of consent. As a result, we note that navigating the consent flow will become more complex for consumers and regulated entities.”

| 2.  | Lack of clarity around collection, use, holding and disclosure of CDR Data |                                | As we previously raised in relation to PIA Update 1, we have found it difficult to determine from the proposed amendments which entity or entities will be considered to have ‘collected’ CDR data in the context of a CAP arrangement, and when that entity or those entities will be considered to be ‘holding’ CDR data. In particular, we have found references to collection by a provider ‘on behalf of the principal’ to be somewhat ambiguous. |

There is a risk that an entity will not understand their obligations under the
### GENERAL RISKS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>LEGISLATIVE FRAMEWORK UNDERPINNING THE CDR REGIME AS IT IS UNCLEAR WHETHER THEY HAVE COLLECTED, ARE HOLDING, OR HAVE DISCLOSED, CDR DATA AT VARIOUS STAGES IN THE PROPOSED NEW INFORMATION FLOWS.</td>
</tr>
</tbody>
</table>
| 3.  | **CDR CONSUMERS WILL NOT UNDERSTAND THE CONSENTS THEY ARE PROVIDING, AND WILL EXPERIENCE “INFORMATION OVERLOAD”** | Rule 4.10(1) (including the proposed amendments) provides that an Accredited Person’s processes for asking a CDR Consumer to give and amend consent must:  
- accord with any consumer experience Data Standards;  
- be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids (having regard to any consumer experience guidelines); and  
- if the consent is not a Collection Consent for | This clarity is important because it affects whether the provider is considered to be an ‘accredited person’ or an ‘accredited data recipient’ at various stages, which then affects other legislative obligations (including the application of the privacy safeguards).  

If the ACCC implements **Recommendation 1**, we consider this will assist in mitigating the identified risk. |
|     | **we recommend** that the ACCC consider whether it would be appropriate to continue, in consultation with the Data Standards Body, conducting consumer research on what is the best way to present a CDR Consumer with all of the different types of consents, to ensure that CDR Consumers are provided with an adequate amount of information before providing their consent, but balancing this against the risk of “information overload” for the CDR Consumer (**Recommendation 2**). |
|     | **Stakeholders who provided submissions strongly supported this as a significant risk (and indicated strong support for the above Recommendation), indicating that CDR Consumers will not understand the new consent processes, which could cause significant confusion and information overload (resulting in not obtaining fully informed and meaningful consent from CDR Consumers).** |
|     | **For example:**  
- The **OAIC** stated that: “The OAIC generally supports a requirement that amendments to consent be sought broadly in the same manner as original consent. This would mean requiring the consumer to undergo the ‘full’ consent and authorisation ‘flow’ to amend any aspect of their consent. At the same time… there may be a need to simplify certain aspects of the consent and authorisation flow to avoid the risk of information overload and enhance the consumer experience. In doing so… it is important to ensure any |
## GENERAL RISKS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
|     | not give an Accredited Person properly informed consent.             | the purposes of an Accredited Data Recipient Request, or a Disclosure Consent, accord with any other Data Standards. | • The **Office of Victorian Information Commissioner** stated that: “The introduction of new information flows, concepts, and types of entities able to collect CDR data (or ‘insights’) increases the risk that consumers will not be able to fully understand how the CDR system works; for example, who is collecting their CDR data, who is holding it, or to whom it is being disclosed…it is unlikely – if not impossible – that consumers will be able to provide truly informed, and therefore meaningful consent. This is problematic given that consent forms the basis of the CDR framework…While OVIC supports the intention of the new categories of consent to provide greater and more granular control to consumers, this must be balanced against the potential for consent fatigue and information overload, factors that are of increasing consent to privacy regulators globally”

• The **Commonwealth Bank of Australia** stated that: “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”

• **AGL Energy Limited** stated that: “We believe the ACCC’s proposed guardrails for preventing consumer overload is so broad that they are almost redundant in their application. If the ACCC wish to pursue this option, then it should be subject to further consumer testing before finalising rule changes… Information overload is a key driver for consumer disengagement and therefore must be appropriately managed within the Rules”

• The Office of Victorian Information Commissioner stated that: “The introduction of new information flows, concepts, and types of entities able to collect CDR data (or ‘insights’) increases the risk that consumers will not be able to fully understand how the CDR system works; for example, who is collecting their CDR data, who is holding it, or to whom it is being disclosed…it is unlikely – if not impossible – that consumers will be able to provide truly informed, and therefore meaningful consent. This is problematic given that consent forms the basis of the CDR framework…While OVIC supports the intention of the new categories of consent to provide greater and more granular control to consumers, this must be balanced against the potential for consent fatigue and information overload, factors that are of increasing consent to privacy regulators globally”

• The Commonwealth Bank of Australia stated that: “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”

• AGL Energy Limited stated that: “We believe the ACCC’s proposed guardrails for preventing consumer overload is so broad that they are almost redundant in their application. If the ACCC wish to pursue this option, then it should be subject to further consumer testing before finalising rule changes… Information overload is a key driver for consumer disengagement and therefore must be appropriately managed within the Rules”
## General Risks

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>NAB</strong> stated that: “Different categories of consent add more complexity to the regime and it is not clear how this will assist consumers and whether this change has been informed by consumer testing…While the descriptions have specific meanings under CDR, they are generic terms and the intent could be lost on consumers. There is a risk that the approach will simply add to ‘information overload’ during the early stages as consumers learn how the CDR works which could in turn make consumers less likely to participate in the CDR”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Regional Australia Bank</strong> stated that: “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…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.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>The Financial Rights Legal Centre</strong> stated that: “[the consent process] requires the consumer to take additional steps to seek clarity and information …[and] places the entire responsibility on the consumer to read the CDR policy, understand the policy and its potential consequences and make a decision based on that full understanding of the consequences of that policy”</td>
</tr>
</tbody>
</table>

© Maddocks 2021
17. Risks associated with changes to consents

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
| 4.  | CDR Participants, and Accredited Persons, will not understand the amendments to the CDR Rules (including the impact on their obligations when collecting, using, and disclosing, CDR Data) | As discussed in Item 1, the complexities of the drafting of the proposed amendments may mean that an Accredited Person does not fully understand their obligations in relation to the type of consent they are seeking (noting there are several obligations relating to the various types, including the introduction of ‘categories’, of Collection Consents, Use Consents, and Disclosure Consents). | The proposed amendments increase the amount of information an Accredited Person must provide a CDR Consumer, and introduces a new concept of ‘categories’ of consents. We recommend that the ACCC consider:  
- the need for the new concept of ‘categories’ as it adds further complexities to an already-complex to understand consent process (Recommendation 5); and  
- providing Accredited Persons with very clear guidance on how the process in Rule 4.11 is intended to operate, so as to ensure that CDR Consumers are provided with the right type of information and choices before providing their consent (Recommendation 1).  
Stakeholders broadly agreed with the identified risk and the above Recommendations. Stakeholders also raised additional associated matters (such as the need to tag CDR Data from the point of collection, and the risk of alternative methods being used, such as screen scraping, due to the complexities involved with obtaining consent).  
For example:  
- The Commonwealth Bank of Australia stated that: “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…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...” |
## Changes to Consents

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>followed, which would assist regulators with compliance and enforcement activities”.</td>
</tr>
</tbody>
</table>

- The **Australian Retail Credit Association** stated that: “The requirement to itemise and obtain separate consents in respect of each data set, account, use and disclosure (including to intermediaries) will mean that a business may not have all the necessary consent to collect use and disclose data in order to provide the good or service to the customer (i.e. the customer may choose to provide some consents and not others – even where those choices may be inconsistent given the product or service they are considering)… it is likely that many credit providers may offer alternative means of filling any ‘gaps’ in the consent (e.g. relying on other data collection methods such as screen scraping or provision of PDF account statements). However, given the lack of a clear and certain ability to access and use the CDR data (and the need to also use alternative sources), there is also a real possibility that the credit provider will simply solely rely on those other methods of collecting data instead of the CDR (noting the credit provider’s subsequent use of that data will be subject to the much less restrictive Australian Privacy Principles).”

One stakeholder (**FinTech Australia**) submitted that: “…there needs to be a common set of standards that apply to consumer consents, to ensure a level of consistency and consumer understanding on the various consent and authorisation methods being proposed… a form of ‘open source’ consent model is required to ensure a level of traction in the system, such that similar technical standards, consent management protocols and customer experience applies throughout the entire CDR process… an overarching consent management model [should] be developed, using open source standards, in parallel with and alongside any changes to consents under the Rules. Without such a consent model in place, the risk of inconsistent methods of communications of consent, and consumer mistrust, is high.”
## CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td><strong>When a CDR Consumer provides a Use Consent for an Accredited Data Recipient to use CDR Data for general research purposes, the CDR Consumer will not understand what they are consenting to</strong></td>
<td>The proposed amendments provide that when a CDR Consumer is asked to provide a Use Consent for the purposes of general research, they must be provided a link to the description in the Accredited Data Recipient's CDR Policy, which specifies the research to be conducted, and any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.</td>
<td><strong>We recommend</strong> that the ACCC consider:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• requiring an Accredited Person to clearly notify the CDR Consumer, when seeking a Use Consent for the purposes of general research:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• which specific research projects the Accredited Person will use the CDR Consumer’s CDR Data for;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• the specific purposes for which the Accredited Person uses the relevant research (for example, to conduct market research on its customers to inform the development of new products);</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• the types of the CDR Consumer’s CDR Data used in the relevant research; and/or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• any potential consequences on this use for research for the CDR Consumer (for example, that their de-identified data from the research may be disclosed and sold); or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• alternatively, whether the information an Accredited Person will use for research should be de-identified, so that no identifiable information of a CDR Consumer will be used by the Accredited Person.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>(Recommendation 6)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We have further refined our Recommendation based on stakeholder feedback (please see below). Generally stakeholders were supportive of CDR Data being used for research purposes. However, many stakeholders noted difficulties around obtaining fully informed consent to use CDR Data for research purposes, and around the uncertainty of the breadth of the definition of research.</td>
</tr>
</tbody>
</table>
For example:

- The **Office of the Victorian Information Commissioner** stated that: “If the use of CDR data for research purposes is based on consent, consumers should accordingly be able to withdraw such consent in the future (or, in the context of the CDR, amend their consent to remove the use of their CDR data for research purposes).”

- The **OAIC** stated that: “While consumers have the option to consent to the use of their CDR data for research, the data analytics activities that may be used in such research project can be difficult to explain and understand, which may mean a consumer’s consent to research is not genuinely informed… To ensure consumers are genuinely informed of the consequences of providing consent to research, the OAIC recommends that the ACCC consider whether the Rules should provide greater particularity in terms of ADR transparency about their research, either when seeking consent or in the CDR policy. This could include information about:
  
  - the specific purposes for which the ADR uses such research (for example, to conduct market research on its customers to inform the development of new products)
  - the types of CDR data used in research, and
  - any potential consequences for the consumer (for example, that their de-identified data from the research may be disclosed and sold).”

- The **Financial Rights Legal Centre** stated that: “The concept of research is not confined to non-commercial, academic research or any other socially beneficial form of research in the public good but is broad enough to include product development, business development, market research and anything up to and including the building of data profiles unrelated to their provision of a specific service to the consumer. This is concerning and runs counter to the original principles of CDR to confine the use of data to the specific use cases for good or services provided... The proposed rules around research consent undermines the voluntary nature of consent. The proposal ensures that the consumer needs to be informed of any additional benefit to be
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>provided to the CDR consumer for consent to the use and the consultation paper foresees that.</em></td>
</tr>
</tbody>
</table>

- **EnergyAustralia** stated that: “...the current wording could capture research that is unrelated to the ADR’s core business or research that a customer would not reasonably expect their CDR data to be used for... There are risks around businesses using this “General Research” consent in a way that was not intended, particularly in ways that support sales of other services. i.e. an ADR could conduct research on essentially any customer attribute/propensity and disclose this data to another business for a fee.”

Alternatively, one stakeholder commented on the limitations of this consent for the purposes of research:

The **Australian Retail Credit Association** stated that:

“The ‘data minimisation principal’ potentially does not permit the business to use the data sets compiled by the accredited data recipient to undertake the analysis to develop models and algorithms to improve the provision of their products and services. While the proposed ‘research’ rules are a partial solution, they apply significant obstacles in the way of the businesses' ability to use the data for those purposes and still fall well short of the needs of the business.”

Accordingly, they stated that it is not appropriate to:

- “Require the consent to be separate from the overall collection and use consents”
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Require the accredited data recipient to describe “any additional benefit to be provided to the CDR consumer for consenting to the use. It is not appropriate to expect a credit provider to provide an additional benefit to a customer to use their data to develop or refine credit scoring algorithms. Requiring a credit provider to address this issue in the consent would simply create an expectation in the customer’s mind that they ‘deserve’ compensation and lead to more customers refusing to provide consent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Apply the ‘research’ purpose to the use of data only, rather than collection and use, as it would be important for a credit provider to collect data in order to test whether it was predictive within their credit models…”</td>
</tr>
</tbody>
</table>

Another stakeholder also discussed the benefits of streamlining consents related to use of de-identified data for the purposes of research and development.

**Experian** stated that: “To expand the use of CDR for insights and research in the development of new products and services, the rules should consider ways to streamline consent and authorised use of the de-identified data that is collected. This is especially important for data driven models that produce insights that can be leveraged across multiple distinct products and services in the marketplace. There is more value to the consumer than risk in using de-identified data such as the use of de-identified data will allow for improved products, services and processes that may benefit the consumer at any point in time.”
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>CDR Consumer unaware their CDR Data can be sold</td>
<td>If the Accredited Person sells a CDR Consumer’s CDR Data when disclosing the CDR Data to another Accredited Person, the recipient of that CDR Data will be required to comply with the relevant requirements and obligations in the CDR Rules, and will also be “accredited”.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>There is no clear prohibition on an Accredited Person asking a CDR Consumer for consent to sell their CDR Data, but note that this is also not expressly permitted (unless it falls into the category of consent that refers to “selling” CDR Data). Further, there are no requirements in the proposed amendments for the CDR Consumer to be informed of, or be able to choose whether they consent to, the selling of their CDR Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>We <strong>recommend</strong> that the ACCC consider:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• including requirements around the selling of CDR Data (e.g. requirements for the Accredited Person to seek a CDR Consumer’s express consent for the selling of their CDR Data); and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• including a requirement for the Accredited Person to provide the CDR Consumer with a clear option to not consent to the selling of their CDR Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(<strong>Recommendation 5</strong>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stakeholders who provided submissions strongly agreed with the identified risk and supported this Recommendation, noting that CDR Consumers may not be aware that the Accredited Data Recipient can sell their CDR Data, nor are comfortable with the selling of their CDR Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example:</td>
<td></td>
</tr>
</tbody>
</table>
|     |                                                                      | • The **Office of the Victorian Information Commissioner** stated that: “While the CDR Rules require additional information relating to de-identification to be presented to consumers when seeking their content (including that the de-identified data will be disclosed, by sale or otherwise…), it should be clear to the consumer whether their data (albeit de-identified) will in fact be sold…there may be value to consumers if they were able to expressly
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>consent – or not – to the sale of their de-identified CDR data, given some may be uncomfortable with the sale of such data, but would otherwise agree to its disclosure.</td>
</tr>
</tbody>
</table>

- The **Financial Rights Legal Centre** stated that: “What is even more disturbing is that there are no requirements in the proposal for the consumer to be informed or choose whether they can consent to the sale of their CDR data. An accredited person only has to seek consent that falls within a category of consents: proposed Rule 4.12(3). In other words consent to sell data can be bundled – a concept that was meant to be eradicated by another important element of consent o that consent be “specific as to purpose.”

- The **Commonwealth Bank of Australia** stated that: “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 **Consumer Policy Research Centre** stated that: “We do not support any amendments to the CDR Rules that increase the capacity for CDR data to be on-sold by Accredited Persons, particularly when meaningful benefit of this proposal to consumers has not been articulated. According to results of our 2020 consumer survey, 90% of Australians object to companies on-selling their personal data.36 We understand that government guidance relating to both CDR and the Privacy Act maintains that deidentified data is no longer considered to be personal data, however we suggest that consumer attitudes may not draw the same distinction.”
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Timing of notifications</td>
<td></td>
<td>As examples of the identified risk, the proposed amendments provide the following notification obligations without any timing requirements on those obligations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• in the case of amending a consent, an Accredited Person must give the CDR Consumer statements in relation to the amendment of the consent, however there is no timing for when the CDR Consumer needs to receive this information (Rule 4.12(3)); and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• if the CDR Consumer’s Collection Consent expires, but the Use Consent is current, the Accredited Person must notify the CDR Consumer that they can withdraw the Use Consent and make an election to delete redundant data (Rule 4.18A).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Given the importance of notifying CDR Consumers about information relating to their consents (such as in relation to the withdrawal or amendment of a consent), we recommend that the ACCC consider including requirements for the Accredited Person to provide the relevant information within a certain timeframe (to ensure that for example, an Accredited Person provides a CDR Consumer with the relevant information <strong>before</strong> they amend their consent) (<strong>Recommendation 5</strong>).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>One stakeholder who provided a submission agreed with the identified risk and supported this Recommendation. This stakeholder (the <strong>OAIC</strong>) also stated that additional requirements to Rule 4.18A should be made, such as to include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• “A requirement for ADRs to provide the notification in Rule 4.18A as soon as practicable after the collection consent expires. This will ensure that a consumer is able to fully stop an ADR from handling their CDR data, as soon as possible, and</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A requirement for ADRs to include the following statements in the Rule 4.18A notification:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o A statement that the consumer’s collection consent has expired, but their use continues, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o A statement outlining what the implications of withdrawing the use consent will be for the consumer.&quot;</td>
</tr>
<tr>
<td>8.</td>
<td>Information provided to CDR Consumer when they amend their consent</td>
<td>Rule 4.12C(3) provides that when a CDR Consumer amends their consent, the Accredited Person must give the CDR Consumer:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• a statement that indicates the consequences of amending the consent; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• a statement that the Accredited Person will be able to continue to use any CDR Data that has already been disclosed to it to the extent allowed by the amended consent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We consider that providing this information to CDR Consumers is privacy enhancing, especially notifying them that the Accredited Person will be able to continue to use any CDR Data already to disclosed to it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We recommend that the ACCC consider whether it would be appropriate to give the CDR Consumer the opportunity, to at this stage, withdraw their Use Consent if they do not want the Accredited Person to continue using any already-collected CDR Data (Recommendation 5).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The drafting in Rule 4.12C(3) is unclear as to whether the ACCC intends for all of the information required in Rule 4.11(3) to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• be provided to a CDR Consumer every time the CDR Consumer amends their consent (noting Rule 4.11(3) specifies what information an Accredited Person must give a CDR Consumer when asking a CDR Consumer to give consent); or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• only be provided once when the CDR Consumer gives their original consent (and therefore the only information a CDR Consumer will receive when amending their consent is that specified in new Rule 4.12C(3)).</td>
</tr>
</tbody>
</table>
## CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>If an Accredited Data Recipient becomes a Data Holder, a CDR Consumer’s Disclosure Consent does not expire</td>
<td>There is a risk that when an Accredited Data Recipient becomes a Data Holder, the CDR Consumer’s Disclosure Consents do not expire, meaning that the CDR Consumer’s CDR Data can continue to be disclosed (and potentially sold).</td>
<td>We recommend that the ACCC consider whether it should expressly specify that if an Accredited Data Recipient becomes a Data Holder of CDR Data, any Disclosure Consents that relate to that CDR Data expire (or otherwise explain it is appropriate why those Disclosure Consents continue) (Recommendation 5).</td>
</tr>
<tr>
<td>10.</td>
<td>CDR Consumer wishes to amend one aspect of their consent</td>
<td>The current CDR regime does not facilitate a CDR Consumer amending their consent, however this concept will be introduced in</td>
<td>We support the proposed amendments to the CDR Rules as a privacy enhancing step, as they will provide CDR Consumers with greater control of their consents, and increase their engagement with the CDR regime as it will be more “user-friendly”.</td>
</tr>
</tbody>
</table>
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>the proposed amendments to the CDR Rules. The proposed amendments will also mean that CDR Consumers will have control over their Collection Consents, Use Consents and Disclosure Consents (rather than simply over their “consent”). This additional level of granularity will mean that it will be easier for the CDR Consumer to amend certain things like extending the validity period of a consent, without amending this period for each consent.</td>
<td>One stakeholder submitted that CDR Consumers should also be able to amend each category of consent. This stakeholder (the <strong>OAIC</strong>) specifically stated: “...the OAIC recommends that consumers be given the option to amend each category of consent given to an ADR (i.e. not just collection consents and use consents, but disclosure consents as well, including direct marketing consents and research consents). This will ensure consumers can exercise choice and control in relation to all aspects of the handling of their CDR data.” We consider the ACCC, when considering this suggestion, should weigh up the benefit of giving this additional control over categories of consents with the potential for “information overload”, and should conduct consumer research when deciding how much information should be presented to CDR Consumers when amending their consent.</td>
</tr>
</tbody>
</table>

| 11. | Consequence of withdrawing a Collection Consent | The proposed amendments to the CDR Rules will mean that if a CDR Consumer’s Collection Consent expires (including because the CDR Consumer withdraws that consent), an Accredited Person must notify the CDR Consumer that they may: | We consider that notifying CDR Consumers is a privacy enhancing feature, as it will assist in ensuring that they are aware that the expiry of a Collection Consent does not mean that an Accredited Person is prevented from continuing to use that CDR Data (and will give the CDR Consumer to withdraw their Use Consent and make an election to delete any redundant data). One stakeholder (the **OAIC**) agreed with our analysis, stating that: “[the OAIC] strongly supports the notification requirements proposed by Rule 4.18A”. This stakeholder also raised the issue about timing of redundancy of data. This stakeholder stated that: “Where a disclosure consent is needed to provide the relevant good or service requested, the OAIC understands that the consumer would need to withdraw all three types of consents (collection, use and |

**Consequence of withdrawing a Collection Consent**

There is a risk that a CDR Consumer will not understand what happens with their CDR Data and any Use Consents if they withdraw a Collection Consent.
## CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• withdraw the Use Consent; and</td>
<td><em>disclosure</em> in order to fully stop the ADR from handling their CDR data. CDR data would therefor only becomes ‘redundant’ and be required to be deleted or de-identified under Privacy Safeguard 12, once all three consents have been withdrawn (or otherwise expired).*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• make the election to delete redundant data in respect of that CDR Data.</td>
<td>Another stakeholder suggested that further consumer research and stakeholder consultation be conducted in relation to the issue, stating that: “We encourage further consumer research and consultation with stakeholders on the mechanics of point-in-time redundancies to ensure that consumers will understand that a revocation of their consent for one part of their data will not provide for the data collected to-date to be deleted. Any education and awareness campaign should be informed by this consumer research” (AGL Energy Limited).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Rule 4.18A)</td>
<td>In addition to the requirements of Rule 4.18A, one stakeholder submitted that further steps should be taken to assist CDR Consumers with withdrawing their consent in its entirety. This stakeholder (the Financial Rights Legal Centre) stated that: “The complexity and range of consents will lead to many not understanding that they may have only withdrawn or amended one form of consent without withdrawing all their consent, being alerted to their other consent remaining live or not be alerted to the right to have their data deleted … CDR participants must be required to give consumers the opportunity to withdraw all their consents in one step. CDR participants must then be required to give consumers the opportunity to delete their data to the full extent that they can in the next step. Otherwise withdrawing of consent will never be easy and the complexity will be used and misused to maintain a consumer’s custom without their full knowledge or awareness.”</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.</td>
<td>Accredited Person pressures CDR Consumer to amend their consent</td>
<td>The proposed amendments to the CDR Rules permit an Accredited Person to invite a CDR Consumer to amend their consent if:</td>
<td>We consider that the ACCC may wish to consider the feasibility of an option to ‘withdraw all consents’, so as to ensure that CDR Consumers are given a simple mechanism to withdraw all of their consents, as a further privacy-enhancing measure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the amendment would better enable the Accredited Person to provide the goods or services requested by the CDR Consumer; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the amendment would:</td>
<td>We consider that the requirements for limiting how often, and when, an Accredited Person can invite a CDR Consumer to amend their consent are privacy enhancing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o be consequential to an agreement between the Accredited Person and the CDR Consumer to modify those requested goods or services; and</td>
<td>We recommend that the ACCC consider including similar limitations on how often, and when, the Accredited Person can invite a CDR Consumer to amend their consent in general (because if a CDR Consumer is constantly inundated with invitations to amend their consent, they may feel pressured to do so, meaning the amendments to their consents may not be given voluntarily) (Recommendation 5).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and</td>
<td>We also recommend that the ACCC continue to conduct consumer research to investigate the appropriateness of presenting pre-selected options to a CDR Consumer with details of their current consent (and ensure the requirements around permitting pre-selected options are limited to only details of the CDR Consumer’s current consent), as this information may assist in informing a CDR Consumer which aspects of their consent they would like to amend (as they will be able to view what they previously selected, such as their election to delete redundant data) (Recommendation 2).</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o enable the Accredited Person to provide the modified goods or services.</td>
<td>Further, if the Accredited Person invites a CDR Consumer to amend the validity period of their current consent, they must not give:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Further, if the Accredited Person invites a CDR Consumer to amend the validity period of their current consent, they must not give:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the invitation more than a reasonable period before the current consent is expected to expire; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• more than a reasonable number of such invitations within this period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In addition, the Accredited Person may present the CDR Consumer with pre-selected options in relation to their current consent.</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13.</td>
<td>CDR Consumer will not understand they can amend their consent</td>
<td></td>
<td>We <strong>recommend</strong>, to enhance the privacy protections in the CDR Rules, that the ACCC consider including, as part of the information required to be provided as part of Rule 4.11, a requirement for Accredited Persons to notify CDR Consumers when asking for their consent that they can, at a later stage, amend that consent through the Accredited Person’s Consumer Dashboard (e.g. to vary the validity period of the consent, or to change the type of CDR Data the Accredited Person collects from a Data Holder) (<strong>Recommendation 5</strong>). One stakeholder agreed with the identified risk and strongly supported this Recommendation. This stakeholder (the <strong>OAIC</strong>) stated that: “To ensure that a consumer is informed about the full range of rights they have in relation to their consent, the OAIC recommends Rule 4.11(3) be amended to required ADRs to present consumers with information about their ability to amend consent (during the consent flow) and instructions for doing so.”</td>
</tr>
</tbody>
</table>
### CHANGES TO CONSENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>CDR Consumer will not remember amendments made to the authorisations provided to the Data Holder</td>
<td></td>
<td>We <strong>recommend</strong> that the ACCC consider whether it should include, similar to the proposed amendments to the requirements of an Accredited Person’s Consumer Dashboard, requirements for the Data Holder’s Dashboard to contain details of each amendment that has been made to each authorisation (Recommendation 5).</td>
</tr>
</tbody>
</table>

Unlike the requirements for when a CDR Consumer amends their consent, the CDR Consumer may amend, or be prompted by the Data Holder to amend, their authorisation, however, will not be able to see these amendments on their Data Holder Consumer Dashboard.
18. Risks associated with the disclosure of CDR Data to Accredited Persons (through AP Disclosure Consents and Accredited Data Recipient Requests)

### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>CDR Participants, and Accredited Persons, will not understand the amendments to the CDR Rules</td>
<td></td>
<td>Given the importance of each party understanding their obligations (especially as the CDR Rules contain certain obligations on Accredited Persons, and certain obligations on Accredited Data Recipients), we recommend that the ACCC consider clearly setting out this new information flow (including clarifying the fact that an Accredited Person (A2) becomes an Accredited Data Recipient after receipt of CDR Data and therefore must comply with any obligations relevant to Accredited Data Recipients) (Recommendation 7).</td>
</tr>
<tr>
<td></td>
<td>This new information flow (i.e. disclosure of CDR Data from an Accredited Data Recipient to an Accredited Person) is difficult to track through in the proposed amendments. There is a risk that, given the complexity of the drafting, the obligations of the various parties at each stage will not be understood (especially considering that an ‘Accredited Person’ who receives the CDR Data from an ‘Accredited Data Recipient’ will then themselves become an ‘Accredited Data Recipient’ of that CDR Data).</td>
<td></td>
<td>Some stakeholders agreed with the identified risk and this Recommendation, with one stakeholder (the <strong>Financial Rights Legal Centre</strong>) stating that: “The AP [Accredited Person] / ADR [Accredited Data Recipient] distinction is unclear and complex, which will lead to industry misunderstanding and likely breaches.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Another stakeholder submitted that it was not necessary to introduce rules in relation to the disclosure of CDR Data by Accredited Data Recipients. This stakeholder (<strong>Deloitte</strong>) stated that: “</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“The ACCC has proposed that rules allow an ADR to transfer data to other third parties, including both other accredited data recipients and non-accredited data recipients…However… the CDR regulatory framework already has a category of CDR participant that holds data – that of a data holder… It is not clear why the ACCC would seek to have one set of rules for transferring a consumer’s data from one class of CDR participant (a data holder) and introduce a different set of rules for transferring a consumer’s data from another class of CDR participant (an ADR). This seems to add unnecessary complexity to the CDR framework”</td>
</tr>
</tbody>
</table>
## AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
| 16. | Unclear when Collection Consent, or AP Disclosure Consent, expires | The proposed amendments to the CDR Rules provide that if:  
- an Accredited Person (A2) has a Collection Consent to collect particular CDR Data from a particular Accredited Data Recipient (A1); and  
- the Accredited Data Recipient (A1) has an AP Disclosure Consent to disclose that CDR Data to that Accredited Person (A2), and one of those consents expires, the other consent expires at the same time (Rule 4.14(1B)). | It is not clear to what is intended by “the other consent expires at the same time”, and if this is intended to mean that an associated consent expires:  
- automatically when the other consent expires; or  
- when that party is notified by the other party of the expiry of the other consent.  
We **recommend** that the ACCC consider whether it would be appropriate to clearly specify when, if one consent expires, the other consent expires. For example, this could include clarifying whether the expiry one a consent is contingent on one party notifying the other of the expiry of the associated consent, or whether the associated consent automatically expires.  
The identified risk and this Recommendation were supported by some stakeholders, with one (the **Financial Rights Legal Centre**) stating that: “It is not clear under the proposal when one consent expires (such as a collection consent held by Accredited Person) what happens to the other consents in the process (such as ADR’s disclosure consent... This adds complexity and a lack of clarity to a process…” |
### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
| 17. | Accredited Data Recipient (A1) discloses CDR Data to Accredited Person (A2) without checking their accreditation | There is a risk, as the CDR Rules do not require the Accredited Data Recipient (A1) to check the Accredited Person’s (A2) accreditation before disclosing CDR Data, that the Accredited Data Recipient (A1) discloses CDR Data to a person who is not indeed “accredited”.  
We understand that the identified risk may be mitigated by the technical implementation of the ACCC’s CDR ICT system, rather than relying on legislative protections in the proposed amendments to the CDR Rules. how the technical implementation will address the privacy risks.  
CDR Data is required to be encrypted in transit in accordance with Schedule 2.                                                                                             | It is unclear from the proposed amendments to the CDR Rules whether the Accredited Data Recipient (A1) will be required to check the credentials of the Accredited Person (A2) (such as through the ACCC CDR ICT system and Accreditation Register) before disclosing CDR Data to that Accredited Person (A2). This is especially important as the Accredited Person (A2) may have for example, been previously accredited when the Accredited Data Recipient (A1) disclosed CDR Data for another CDR Consumer to that Accredited Person (A2), but since that disclosure, the Accredited Person’s (A2) has been suspended, revoked, or surrendered.  
Further, the proposed amendments do not specify the process for disclosing CDR Data in response to an Accredited Data Recipient Request (noting that currently the CDR Rules (Rule 4.6) impose requirements on the disclosure of CDR Data from a Data Holder to an Accredited Data Recipient). This means there are no requirements for the disclosure to be, for example, in accordance with the Data Standards.  
We query whether it would be more appropriate for (some of) these issues to be addressed in the CDR Rules, or at least further explanation given to entities participating in the CDR regime.  
Given the importance of ensuring that CDR Data is only disclosed to an “accredited” person, we recommend that the ACCC consider including obligations on:  
- the Accredited Data Recipient (A1) to check the credentials of the Accredited Person (A2) before any CDR Data is disclosed (similar to the obligations on Data Holders); and |
### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• each party to notify the other if their accreditation gets suspended, revoked, or surrendered. (Recommendation 9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Several stakeholders who provided submissions agreed with the identified risk and strongly supported this Recommendation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Commonwealth Bank of Australia</strong> stated that: “… 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.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Financial Rights Legal Centre</strong> stated that: “… it is unclear from the proposal whether ADRs will be required to check credentials of an Accredited Person. This could lead to disclosures of CDR data to unaccredited persons, since accreditations may have lapsed, revoked or suspended.”</td>
</tr>
<tr>
<td>18.</td>
<td>CDR Consumer unaware of status of Accredited Data Recipient Request</td>
<td>Under the proposed amendments to the CDR Rules, an Accredited Data Recipient (A1) is not obliged to disclose CDR Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We understand that these proposed amendments reflect that, unlike Data Holders, an Accredited Data Recipient cannot be required to disclose CDR Data. However, we consider that CDR Consumers should be provided with transparency around the progress of their Accredited Data Recipient Request.</td>
</tr>
</tbody>
</table>
## AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
|     | seek an AP Disclosure Consent from a CDR Consumer, even if the CDR Consumer has provided a Collection Consent to the relevant Accredited Person (A2). | To ensure the CDR Consumer retains control over their CDR Data (and oversight over any Accredited Data Recipient Requests), we recommend that the ACCC consider whether the CDR Consumer should be informed about:  
- the refusal to progress their Accredited Data Recipient Request (including by refusing to provide the CDR Data to the Accredited Person (A2)); and  
- the reasons for the refusal. (Recommendation 10) |  
One stakeholder agreed with the identified risk, stating that: “consumers will be kept in the dark about certain consents” (Financial Rights Legal Centre). |

In addition, even if the CDR Consumer has provided an AP Disclosure Consent to the Accredited Data Recipient (A1), that Accredited Data Recipient (A1) is not obliged to provide the CDR Data to the nominated Accredited Person (A2). Accordingly, there is a risk that a CDR Consumer will not receive an appropriate level of control or oversight over the status of their Accredited Data Recipient Request, or their CDR Data.
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>CDR Consumer amends the Collection Consent with the Accredited Person (A2) and not the associated Disclosure Consent with the Accredited Data Recipient (A1)</td>
<td>There is a risk that the CDR Consumer amends the Collection Consent with the Accredited Person (A2) but not the associated Disclosure Consent with the Accredited Data Recipient (A1).</td>
<td>We recommend that the ACCC consider whether it would be appropriate to include requirements for the Accredited Data Recipient (A1) to invite the CDR Consumer to amend their Disclosure Consent if the Accredited Data Recipient (A1) is notified by the Accredited Person (A2) that the CDR Consumer has amended their Collection Consent. This requirement could be drafted in a similar way to the proposed amendments in relation to a Data Holder inviting a CDR Consumer to amend their authorisation if the Data Holder is notified that they have amended their associated Collection Consent with the Accredited Data Recipient (see Rule 4.22A) (Recommendation 11).</td>
</tr>
<tr>
<td>20.</td>
<td>Accredited Data Recipient (A1) unaware that CDR Consumer has withdrawn their Collection Consent provided to Accredited Person (A2)</td>
<td>There is a risk that an Accredited Data Recipient (A1) continues to disclose CDR Data to an Accredited Person (A2) after the CDR Recipient has withdrawn their Collection Consent.</td>
<td>The proposed amendments require the Accredited Person (A2) to notify the Accredited Data Recipient (A1) if a Collection Consent expires (Rule 4.18B). Withdrawal of a consent is one way that a consent can expire (see Rule 4.14).</td>
</tr>
</tbody>
</table>

To ensure that an Accredited Data Recipient (A1) does not continue to disclose CDR Data if the associated Collection Consent given to an Accredited Person (A2) has been withdrawn, we recommend that the ACCC consider including clarifying the obligations on an Accredited Person (A2) to notify an Accredited Data Recipient (A1) if a Collection Consent for the purposes of an Accredited Data Recipient Request is withdrawn, similar to the requirements specified in Rule 4.13(2)(b) (Recommendation 12).
## AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Consent given to the Accredited Person (A2).</td>
<td></td>
</tr>
</tbody>
</table>

### 21. Transparency around Use Consents and Disclosure Consents for direct marketing purposes

There is a risk that before providing the relevant Use Consents and Disclosure Consents for the purposes of direct marketing, a CDR Consumer will not have transparency around what arrangements are in place between Accredited Persons when being recommended certain goods or services (which may mean that vulnerable consumers are taken advantage of).

The proposed amendments (Rule 7.5(3)(a)(iv)) specify that the Accredited Data Recipient may provide this information about another Accredited Person’s goods and services if the Accredited Data Recipient:

- reasonably believes that the CDR Consumer might benefit from those other goods or services; and
- sends such information to the CDR Consumer on no more than a reasonable number of occasions.

Given that this may be used to exploit vulnerable CDR Consumers, we recommend that the ACCC consider whether CDR Consumers should receive greater transparency, before providing Use Consents and Disclosure Consents for direct marketing, about what is “in it” for an Accredited Data Recipient if they recommend/provide information about another Accredited Person (e.g. information about any arrangements/monetary benefits the Accredited Data Recipient receives if they recommend that Accredited Person) (Recommendation 13).

The majority of stakeholders who made submissions agreed with the identified risk and supported this Recommendation. Although they remarked on the importance of customer experience and being able to provide best products and services (including marketing), stakeholders were generally concerned about the potential harm for CDR Consumers in relation to the proposed amendments to the CDR Rules in relation to direct marketing.

All stakeholders who submitted on the amendments in relation to direct marketing broadly agreed that consent is required and separate consents may be preferable.
### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
|     |      | Further, the proposed amendments also specify that the Accredited Data Recipient can disclose CDR Data to that Accredited Person if the CDR Consumer has given the relevant Collection Consent and Use Consent to the Accredited Person, and AP Disclosure Consent to the Accredited Data Recipient. | For example:  
- **Intuit** stated that: “It is important to the integrity of the CDR regime that consumers are aware of who they have granted access to their data and how that data will be used by ADRs to provide a good, service or benefit to the customer… Given the private sector application relies on the freedom to contract to terms, we do not believe that commercial arrangements between ADRs must be disclosed to consumers”.  
- **The OAIC** stated that: “There are likely to be many goods or services that an ADR ‘reasonably believes’ a CDR consumer may benefit from, notwithstanding that these goods or services may have no or a limited connection to the good or service currently being supplied by the ADR to the consumer. This raises the risk that a consumer may be ‘spammed’ with unwanted recommendations. Further, in the banking context, there is a risk that products could be recommended for a consumer that are inappropriate for their financial situation. Both of these practices could undermine consumer control and therefore trust in the CDR system. We also note that this represents a shift from the more cautious approach taken in the system to direct marketing to date.”  
- **The Financial Rights Legal Centre** stated that: “The proposal to permit accredited persons to collect and disclose CDR data between themselves in order to offer goods and services to consumers is a vast expansion of the current concept of “direct marketing” under the rules… Such an expansion provides the very real potential to increase predatory targeted marketing practices, particularly with respect to financially vulnerable people.” |
### Consumer Data Right Regime – Update 2 to Privacy Impact Assessment

#### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>… The reason for limiting on-selling and direct marketing is clear. The CDR regime provides the very real potential to increase predatory targeted marketing practices, particularly with respect to financially vulnerable people. Consumers struggling with debt are often the most profitable customers for banks and lenders and are constantly barraged with marketing offers for financial services products… The new proposal however now opens up the CDR to these very practices.”</td>
</tr>
</tbody>
</table>

- The **Consumer Policy Research Centre** stated that: “We consider there is significant potential for consumer harms (such as increased profiling, predatory pricing, and barriers to seeking redress) arising from proposed amendments that loosen protections against direct marketing and which expand permitted uses of CDR to include disclosure and sale of derived insights, commercial research by data recipients, and greater allowances for on-selling of CDR data. CPRC strongly recommends that the amendments to the Rules proposed at 7.5(1)(aa) and 7.5(3)(a)(iv) should be struck out, along with any relevant enabling clauses.”

- **SISS Data Services** stated that: “Disclosure that the ADRs have entered into a commercial [arrangement] should be disclosed to the Consumer”.

One stakeholder (**FinTech Australia**) provided a differing view, stating that: “In line with usual business practice, Fintech Australia would maintain that commercial arrangements between ADRs remain confidential where they have no bearing on or impact upon the rights or freedoms of the consumer.”
### AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>The Original CDR PIA report discusses the risks associated with the disclosure of CDR Data to an Accredited Data Recipient (See <em>Step 6 in the Original CDR PIA report</em>), which will also apply to situations where the Accredited Data Recipient discloses CDR Data to an Accredited Person.</td>
<td>See Original CDR PIA report.</td>
<td>See Original CDR PIA report.</td>
</tr>
</tbody>
</table>
19. Risks associated with the disclosure of information relating to CDR Consumers to non-accredited persons (through TA Disclosure Consents and Insight Disclosure Consents)

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>CDR Consumers do not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR</td>
<td></td>
<td>We note that the proposed amendments will allow the disclosure of CDR Data and CDR Insights to recipients who are not Data Holders or Accredited Persons (and do not have any obligations under the CDR legislative framework). These recipients may not even have any obligations under other privacy legislation (i.e. the recipient does not need to be an APP entity for the purposes of the Privacy Act, or have otherwise agreed to comply with the APPs). It is important that CDR Consumers understand that if their CDR Data, or a CDR Insight, is disclosed to a Trusted Adviser or an Insight Recipient, that information will be disclosed outside the CDR regime. This means that the information, once disclosed, will not be afforded the protections offered by the CDR Rules (and, in particular, the Privacy Safeguards). Additionally, it is important that CDR Consumers understand that CDR Data and CDR Insights may be disclosed to recipients that do not have obligations under any privacy legislation. <strong>We recommend</strong> that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity (<strong>Recommendation 17</strong>).</td>
</tr>
</tbody>
</table>
Some stakeholders agreed with the identified risk and supported this Recommendation.

For example:

- The **OAIC** stated that: “…CDR data provided to trusted advisors outside the CDR system should still be subject to a baseline level of protection, being the protections in the Privacy Act. This would ensure that consumers who wish to provide their CDR data to a trusted advisor would still have their data protected, in particular under the data breach notification scheme, and have access to redress mechanisms, monitoring and oversight by the OAIC.”

- **Origin Energy** stated that: “once the data is transferred from an ADR to a non-accredited person, the CDR consumer protections will not apply as the data has been transferred out of the CDR eco-system. This raises the potential for data to be misused or consumers having limited abilities to pursue the entity if the data has been misused.”

- The **Commonwealth Bank of Australia** stated that: “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).”

In addition, a stakeholder raised the need for requirements for consents to be included as part of the Data Standards. This stakeholder (**AGL Energy Limited**) stated that: “While we strongly disagree that disclosures should be allowed to ‘trusted advisors’ that are not accredited, should the ACCC pursue this then disclosure consent should only be allowed after an original consent is in place. The disclaimer information should be prescribed within the data standards to ensure a clear, consistent and consumer accessible packet of information on the risks of disclosing outside of the CDR system are in place”.

## DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Another stakeholder submitted that Trusted Advisers should be required to comply with the CDR Rules. This stakeholder <em>(Australian Energy Council)</em> stated that: “Allowing non-accredited parties, even if they hold other fiduciary duties, means the customer loses their CDR protections. A trusted advisor could not receive CDR accreditation by simply proving they hold other fiduciary duties, so it should not be treated as a valid substitute. The AEC would not oppose allowing disclosure to trusted advisors so long as the advisor is required to comply with the CDR rules. We would encourage the ACCC to consider arrangements to this effect, such as through the alternative affiliate accreditation model recommended earlier”.</td>
</tr>
<tr>
<td>24.</td>
<td>Consent from vulnerable CDR Consumers</td>
<td></td>
<td>We note that there is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully-informed, particularly in circumstances where the CDR Consumer:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• may not understand the negative consequences that may flow from giving their Insight Disclosure Consent (i.e. that the disclosure of the CDR Insight to another person may result in the CDR Consumer being refused access to goods or services); or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• may be pressured into providing their Insight Disclosure Consent by a potential provider of goods or services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We <strong>recommend</strong> that the ACCC consider:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• whether it is appropriate for CDR Insights to be part of the CDR Regime in circumstances where there is a significant risk that vulnerable CDR Consumers may be pressured into providing an Insight Disclosure Consent, or may otherwise not fully understand the potential negative consequences that their consent may have; or</td>
</tr>
</tbody>
</table>
### DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• if the ACCC determines that it is appropriate for CDR Insights to remain within the scope of the CDR Regime, implementing mechanisms to ensure that vulnerable CDR Consumers are giving free and fully-informed Insight Disclosure Consents.</td>
</tr>
</tbody>
</table>

(Recommendation 19)

Some stakeholders agreed with the identified risk and supported this Recommendation.

For example:

- **Origin** stated that: "We believe the scope of directly derived data is too general for application in the CDR Rules framework. While we appreciate the CDR Rules is deliberately broad to cater for future scenarios of data innovation, there are ‘grey’ areas of how this would: 1) be interpreted by ADRs; and 2) whether consumers will understand the terminology for the release of certain data… This is most likely to impact vulnerable customers who may not know or understand that the consent to transfer data insights may have a negative impact on them accessing a good or service… We recommend removing the reference to CDR insights in the proposed CDR Rules… Limiting CDR data to well-defined data sets would provide the best level of clarity.”

- **AGL Energy Limited** stated that: "We agree with Maddocks observations of potential risks relating to disclosures and encourage greater consideration by the ACCC to ensure that consent is free and fully informed on these matters.”
## DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>CDR Insights may be more invasive than sharing raw CDR Data</td>
<td>There is a risk that sharing a CDR Insight about a CDR Consumer may be as, or more, invasive than sharing a CDR Consumer’s raw CDR Data.</td>
<td>We note that CDR Insights contain the results of the analysis of raw CDR Data. Therefore, CDR Insights contain information that is more sensitive than raw CDR Data alone. We recommend that the ACCC consider whether it is appropriate for CDR Insights to be generated and disclosed as part of the CDR Regime. This is because of the inherent risks associated with the disclosure of the results of the analysis of raw CDR Data (<a href="#">Recommendation 19</a>). Although stakeholders who provided submissions commented on the usefulness of disclosures of CDR Insights, the majority of stakeholders commented that in their current form, the CDR Rules lack sufficient detail and need further defining to ensure raw CDR Data is not disclosed, and accordingly many stakeholders supported the above Recommendation. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>AGL Energy Limited</strong> stated that: “While we strongly encourage the ACCC should make rules to restrict CDR insight disclosures to exclude raw CDR data, we note that there is a risk that CDR insights may be even more invasive than the raw CDR data. This concern does not appear to be appropriately addressed in these proposed amendments. … At this stage, we do not consider there is sufficient detail in the ACCC Rules, or evidence that supports the proposed approach as being one that centres on more positive consumer outcomes – for all consumers and their individual circumstances”</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
|     |      |                               | • The **Australian Banking Association** stated that: “The ABA notes that ‘Insights’ of themselves can be as sensitive (if not more sensitive) than the data itself… There are moral issues associated with the disclosure of such data. These are exemplified in the following scenarios:

  o The deduced trait (i.e. the insight) may be accurate, but the customer may not be conscious of it. In this case, the passing of data about a customer trait of which the customer may/may not be conscious to a TA should not be permitted on the basis that the data is being disclosed to an unsecure environment and the consumer is unaware of the nature of the trait being disclosed.

  o The consumer may disagree with the deduced trait (i.e. the insight) and may challenge the assumptions and analysis by which it was derived. In this case the disclosure of the trait would have been made into an unaccredited environment before the customer had the opportunity to challenge the insight and ask for its deletion.

  The ABA suggests that an insight should be de-identified, aggregated data which does not relate to individual consumer records (for example average loan amounts derived from a number of consumer accounts).”

• The **OAIC** stated that: “In particular, the OAIC does not support the proposed model for the disclosure of CDR insights in its current form. The disclosure of an insight generated from CDR data would be as insightful, if not more, than ‘raw’ CDR data itself. In our view, the current model would pose significant privacy risks for consumers, and particularly vulnerable consumers, and is therefore in need of further safeguards to ensure these risks can be appropriately mitigated.” |
### DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Institute of Public Accountants</strong> stated that: “The definition of ‘insights’ as being derived CDR data and the question of what can be disclosed in terms of derived or raw data needs further consideration. However, we believe that the primary principle should be to enable consumers to share their CDR data, however defined, with their choice of trusted adviser, with a seamless experience to encourage confidence and take up. Making a distinction in the types of data may add an unnecessary level of complexity and confusion for consumers. In addition, the services provided by many accountants and tax agents through their accounting software (including bank data feeds) would include a mix of types of data. Again, making the distinction in types of data would add an unnecessary level of complexity which impacts not only the accountant but also the consumer/client.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Commonwealth Bank of Australia</strong> stated that: “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 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.”</td>
</tr>
</tbody>
</table>
## DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>… 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.”</td>
</tr>
</tbody>
</table>

- **Quantium** stated that: “Quantium supports the introduction of CDR data insights, and the ability to disclose them to any party once separated from identifying information… There is always a difficult question as to the acceptable magnitude of risk and possible harm associated with release of information that is pseudonymised by removal of direct identifiers, but not pervasively deidentified by removal or obfuscation of all direct or indirect identifiers such that reidentification risk can be reliably assessed as remote.”

- **NAB** stated that: “NAB is concerned about potential for consumer detriment if CDR insights are provided to non-accredited persons. Data insights can have the potential to be more sensitive information than the raw data. For example, detailed transaction history can be used to identify a person’s daily movement habits, health status and location.”

- **Equifax** stated that: “Equifax considers that raw CDR Data and insights should be disclosable to trusted advisors. This is what is done in practice today. If the CDR regime limits this freedom, it may well impact on the success of the CDR regime.”
### DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>One stakeholder (<strong>Xero</strong>) provided a differing view, stating that:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“The Rules framework should not attempt to specify groups of professions as non-accredited third parties. Rather, a consumer should be free to grant access to their data to their choice of third party. This will allow consumers to benefit fully from the regime, including new and emerging use cases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>… it must be up to the consumer what they choose to share. The Rules should not seek to prescribe what data a consumer can share with a non-accredited third party. Doing so is contradictory to the regime intent which seeks to give data owners control of their data.”</td>
</tr>
</tbody>
</table>

| 26. | Risk relating to the transfer of CDR Data and CDR Insights to Trusted Advisers and Insight Recipients | We note that in transferring CDR Data or CDR Insights to a Trusted Adviser or an Insight Recipient, an Accredited Person does not need to comply with the CDR Rules or Data Standards in relation to such transfers. In our view, this may increase the risks of loss or unauthorised access and disclosure during that transfer. | We note that it is important that CDR Data or CDR Insights that are disclosed to a Trusted Adviser or Insight Recipient are appropriately protected during the transfer of information. |
|     |                                                   | We recommend that the ACCC consider implementing measures to ensure that CDR Data and CDR Insights are appropriately protected during the transfer between an Accredited Person and a Trusted Adviser or Insight Recipient (**Recommendation 18**). |
|     |                                                   | Some stakeholders who provided submissions supported the concept of disclosing CDR Data to Trusted Advisers and remarked on the desirability of being able to share data with Trusted Advisers. |
|     |                                                   | For example: |
|     |                                                   | • **illian** stated that: “Trusted advisors play a crucial role in the financial sector... [and] have a need to access consumers banking data, both at the product and transactional level, in order to provide services to their clients. These types of services are typically provided by small businesses who would be...” |
## DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>unable to meet the current or proposed accreditation requirements, effectively locking them out of CDR. Consequently, Illion strongly support the ability for these Non-Accredited Person’s to access the Consumers CDR data, with the consumers consent, and under the control of an Accredited Data Recipient…[Trusted Advisors] are likely to require access to the raw transaction data (not just summarised content) so we strongly argue that the data provided to the Trusted not be restricted.”</td>
</tr>
</tbody>
</table>

- **Frollo** stated that: “Generally, Frollo agrees with the ADRs disclosing CDR Data to trusted advisors with consumer consent… Frollo strongly supports the disclosure of CDR Data to Mortgage Brokers for the following reasons:
  - consumers will benefit greatly by allowing their Mortgage Brokers to use their CDR Data to find and recommend the most appropriate mortgage in a fraction of the time;
  - Consumers already share the data (similar to CDR Data) with Brokers through unsecure methods (eg. screen scraping, statement downloads)…”

- **The OAIC** stated that: “The OAIC is broadly supportive of the draft Rules in relation to disclosures to non-accredited third party ‘trusted advisors’. In particular, we welcome the proposal to narrowly prescribe the types of trusted advisors in the draft Rules, as well as the underlying principles that trusted advisors will only be prescribed where the service they offer will provide a direct benefit to the relevant consumer, and where they are subject to existing professional or regulatory oversight.”
However, the majority of stakeholders held deep concerns regarding:

- the lack of governance (i.e. that Trusted Advisers were not subject to CDR Rules);
- the lack of informed consent (i.e. CDR Consumers are not aware that the security, accreditation and governance under CDR do not apply to ‘trusted advisors’);
- that fiduciary duties for Trusted Advisers are not the same as protection offered by the CDR regime; and
- a general concern for the transmission of data to Trusted Advisers outside of accredited networks/systems (and for this to be a “loophole” to get around the protections and obligations contained in the CDR regime).

For example:

- **NAB** stated that: "allowing CDR data to be transferred to non-accredited entities risks undermining the customer protection which the accreditation process is designed to provide. Accreditation for data recipients ensures the appropriate security standards and privacy protections (including the privacy safeguards) operate to protect consumers. Non-accredited persons are not subject to the stringent privacy safeguards and may not be subject to the privacy legislation. As a consequence, non-accredited entities may not have requirements to notify DHs of a data breach. This means that a DH may not be made aware of a data breach that compromises their customer’s data and presents a fraud risk.

  …NAB does not consider that the CDR needs to include the concept of sharing to ‘trusted advisors’ due to concerns for privacy and security. In NAB’s view, current arrangements work to share data with these types of individuals already.

  NAB is concerned that the effective supervision of ‘trusted advisors’ is dependent on the current regulatory oversight that exists outside of the CDR. As noted above, there may be gaps in oversight such as the possibility
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>that individuals are not subject to privacy law. In addition, it is unclear how a person or organisation would qualify for data to be shared with them.</td>
</tr>
</tbody>
</table>

- **The Financial Rights Legal Centre** stated that: “Disclosing CDR data to non-accredited parties is currently not allowed under the current rules for very good safety, security and privacy reasons. The consultation paper proposes to remove this restriction and allow the disclosure of highly sensitive CDR data to be disclosed to non-accredited persons with no safety and security protections in place.

The proposal undermines the entire raison d’etre of the Consumer Data Right and its safeguarded environment by facilitating the movement of highly sensitive financial data and other consumer data to unsafe and insecure environments with little to no protections or redress for the consumers when things will inevitably go wrong.

Any benefits that consumers may receive from the passing of their data to the professions proposed is offset by the lack of security standards applied to these entities and the fact that the strong consumer protections afforded by the CDR regime do not move with the data – leaving consumers vulnerable to lower privacy standards under the current woefully inadequate and out of date privacy regime.”

- **Origin Energy** stated that: “We have concerns that without clear boundaries on requirements and obligations, it is possible that an ADR could become an intermediary that enables CDR to be transferred to other entities without being appropriately accredited to receive the data. It may become a ‘loop hole’ in the CDR scheme for an entity to receive data to provide a service.”
### DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>AGL Energy Limited</strong> stated that: “We agree that disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer and strong measures put in place to ensure that ADRs do not act as mere data conduits to perversely the course of the CDR legislation and intention, including the strong privacy and consumer protections inbuilt to the regime.”</td>
</tr>
</tbody>
</table>
|     |      |                                | **The Commonwealth Bank of Australia** stated that: “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 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.” |
|     |      |                                | One stakeholder (**SISS Data Services**) submitted that Trusted Advisers should only access CDR Data via an Accredited Data Recipient, stating that: “…a trusted advisor should only be accessing data via an ADR which has a consumer-facing service. This ensures consumers have proper consent management and documented purposes for data collection. We would expect that the trusted advisor’s purpose for accessing data be somehow associated with the ADR’s purpose for data collection.” |
### DISCLOSURE TO NON-ACCREDITED PERSONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Should a trusted advisor wish to gain direct access to consumer data they have the right and opportunity to become an ADR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We seek clarification for any evidence an ADR should seek to confirm the validity of a trusted advisor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We believe rules should be added to ensure a Trusted Adviser must not share CDR data with another party, being another trusted Adviser, another ADR or a non-accredited party.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Another stakeholder voiced the need for a secure method to be used for this transfer of CDR Data to Trusted Advisers, stating that: “In terms of the format and method for disclosure of CDR data to a trusted advisor, it appears that the proposed rules do not intend to limit how the CDR data can be transferred (for example, through a standard). While OAIC appreciates that it may not be practical to limit the format and method, we consider it is important that CDR data be transferred to trusted advisors via an appropriately secure method. The OAIC recommends that the ACCC consider whether the Rules should provide guidance about secure options, for example minimum security requirements, for transfer of CDR data to trusted advisors.” (OAIC)</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In addition, stakeholders commented on the need for CDR Insights to only be disclosed with consent from the CDR Consumer. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>Finder.com.au</strong> stated that: “Finder is broadly supportive of the proposed rules to permit accredited parties to share insights derived from the CDR data to any person with a consumer’s consent. We agree that this may help with certain use cases like the ones outlined in the consultation paper. Similarly to the transfer of CDR data between accredited persons, we would recommend that a new consent request is sent to the consumer before CDR insights are shared.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>EnergyAustralia</strong> stated that: “We support that the ADR be required to pre-notify the customer before disclosure of Insights or TA disclosures can take place, via their dashboard and seek from the customer a reconfirmation that they agree to the disclosure. This will help to safeguard against the sharing of discriminatory insights or insights that are incorrect (due to poor analytics or being based on incomplete data), and disclosures of CDR data which appear excessive to the Trusted Advisor’s needs.”</td>
</tr>
</tbody>
</table>
20. Risks associated with the introduction of new levels and kinds of accreditation

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td>Complexity of the CDR Rules</td>
<td></td>
<td>As discussed above (Item 1), the proposed amendments to the CDR Rules are very complex to navigate, and this is particularly the case for the new kinds of accreditation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example, 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'; and an Unrestricted Accredited Person may be described as 'a person [having] unrestricted accreditation', or as an 'accredited person', or as 'the provider', or as 'the enclave provider', or an 'accredited data recipient'). This means that it is often somewhat difficult to work through which rules will apply to the different parties to a CAP arrangement, for the different information flows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In addition, it is unclear which party or parties to a CAP arrangement will be considered to have ‘collected’, and/or ‘disclosed’ CDR Data, or be ‘holding’ CDR Data. This risk is generally discussed above (see Item 2) but is particularly applicable for CAP arrangements in connection with data enclave accreditation and affiliate accreditation. For example, it is not immediately apparent from the proposed amendments whether an enclave provider or sponsor who ‘collects CDR data on behalf of the principal’ under a CAP arrangement, will be considered to have ‘collected’ the CDR Data and therefore be an Accredited Data Recipient, or whether only the principal is intended to be the Accredited Data Recipient in such a situation. It is also not clear who the CDR Data will have been ‘disclosed’ to the principal and/or the provider; or whether a data enclave provider will be considered to be ‘holding’ the CDR Data. This makes it somewhat difficult to apply the definition of ‘accredited data recipient’ in s56AK of the CC Act.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If it is intended that only the principal is considered to have collected the CDR Data (i.e., only it, and not the provider, is considered to be an Accredited Data Recipient), then it is also not clear when the principal will be considered to have become an Accredited Data Recipient. While we believe that it is likely to be intended that this will be the time that the CDR Data is transferred into the enclave or otherwise received by the sponsor, rather than when the CDR Data is accessed by the provider, this is not entirely clear from the drafting of the proposed amendments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>It is foreseeable that further complexity will arise where an entity undertakes transactions in multiple capacities. For example, an Unrestricted Accredited Person may have an appropriate consent from a CDR Consumer to collect CDR Data from a Data Holder; may then agree to be an enclave provider and collect the same CDR Data on behalf of a Data Enclave Accredited Person; and may also potentially collect the same CDR Data on behalf of another affiliate in its capacity as a sponsor. It may be difficult for that person (or the ACCC and/or OAIC at a later date) to determine the capacity in which they are collecting and/or holding CDR Data at any point in time, making it difficult to determine which obligation(s) in the CDR Rules apply.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example, Schedule 2 currently provides important protections for CDR Consumers in relation to the storage and handling of CDR Data. We suggest that it may be difficult for an Unrestricted Accredited Person who is also a sponsor and/or enclave provider for one or more other Accredited Persons (and perhaps also an outsourced service provider for these or other entities), and/or for the ACCC or OAIC, to establish compliance with the relevant requirements of Schedule 2 in respect of any transaction, because their obligations will differ depending on the capacity in which they are acting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Clarity is important to ensure that the obligations of both the Unrestricted Accredited Person and the Data Enclave Accredited Person can be ascertained and understood by these entities. In our view, the further complexity of the CDR Rules as a result of the proposed amendments increases risks of non-</td>
</tr>
</tbody>
</table>
NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>compliance, particularly by restricted Accredited Persons, with the important privacy protections contained in the legislative framework. This in turn may increase reliance on the regulators to take additional investigatory and/or legal action for noncompliance.</td>
</tr>
</tbody>
</table>

We recommend that the CDR Rules be further clarified (e.g. further expansion of Rule 1.7(v), which only relates to outsourced service arrangements), and/or clear and simple guidance provided by the ACCC, to assist entities understand their privacy obligations (Recommendation 1).

The majority of stakeholders who provided submissions strongly agreed with the identified risk and supported this Recommendation. Stakeholders were particularly concerned with the risk of confusion for both CDR Consumers and entities participating in the CDR regime (noting that stakeholders consulted represent a variety of corporate entities and community groups).

For example:

- The Commonwealth Bank of Australia stated that: “We agree with the PIA finding that further complexity will arise where a party undertakes transactions in multiple capacity es, increasing the difficulty for entities and the regulators to determine which CDR Rules apply.”

- Regional Australia Bank stated that: “While we recognise the intent to create more flexibility around accreditation, creation of additional sub-classifications may introduce undesired complexity and confusion.”

- The Office of Victorian Information Commissioner stated that: “The paper outlines extensive proposed amendments to the CDR Rules, from new tiers of accreditation and new types of consumer consents, to enabling consumers to disclose CDR data and ‘insights’ to non-accredited persons, amongst others. OVIC recognises that these changes are designed to
## NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Provides greater flexibility and control to consumers wishing to share CDR data. However, OVIC is concerned that the proposed changes will add further complexity to an already complicated system, not only for consumers, but also for the various entities participating in the CDR regime.</td>
<td></td>
</tr>
</tbody>
</table>

- **NAB** stated that: “These models introduce complexity which may lead to consumer confusion as well as potential for participants not to fully understand their regulatory obligations. The framework could be simplified, with the restricted levels split into two parts – limited data and sponsored (via data enclave or affiliate). The existing CAP arrangements could be extended to cover the ‘sponsored’ arrangements. NAB believes that further consultation is required to refine the tiering framework before the Rules are updated.”

- **Origin Energy** stated that: “We are concerned that a tiered accreditation will add unnecessary complexities with a requirement to segregate data sets to ensure that only the authorised data sets for the level of accreditation is provided to the accredited third party. The risks of data breaches increase with the system complexities to disaggregate data sets within data sets to provide only limited information to ADR 1, ADR 2, a non-accredited person or CAP Providers.”

- **Illion** stated that: “We would encourage a simpler tiering structure that leverages an intermediary model (where the intermediaries are required to have unrestricted accreditation) and requires that the intermediaries implement the consumer permissions model and provide access to CDR data. The intermediaries act as the gatekeeper of the CDR data, ensuring correct controlled access, whilst allowing the intermediary to provide the CDR data (without restriction) to third parties. The third parties could be required to hold a very low level of accreditation, or potentially no accreditation… The proposal appears overly complex, restrictive and potentially hugely complex to implement and police, whilst still imposing...
**NEW LEVELS AND KINDS OF ACCREDITATION**

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>

|  |  |  | significant costs on organisations wishing to achieve restricted accreditation. |

- The **Financial Rights Legal Centre** stated that: “The complexity of the tiered accreditation proposal means that there are a number of gaps and inconsistencies – some of which have been identified but many others are inevitably going to either arise in the future or not be identified and lead to harms.

  … To work, the proposed tiered accreditation system seems to be wholly dependent on commercial arrangements between the parties, which, again, will centre on dealing with the risks of the parties to the arrangement rather than focussing on the best interests of the consumer. It will also mean such rules and liabilities developed will be multiple, inconsistent and not guaranteed to deal with all the issues that will inevitably arise, leading to even further complexity, and a lack of transparency for consumers.

  In addition there will be overlapping and inconsistencies between these arrangements and their legislative liabilities and obligations.”

- The **Australian Energy Council** stated that: “… the proposed amendments will add a layer of complexity to the CDR regime that customers do not appear ready to navigate. With customers, as well as data holders and accredited data recipients (‘ADRs’), still developing familiarity with the rules framework and protections and obligations within it, introducing a sub-set of different requirements risks creating confusion. This may result in third parties unintentionally not complying with their legislative obligations as well as customers not understanding what protections they have and when they apply.”
NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Deloitte stated that: “It will be important that the additional complexity necessarily introduced with the adoption of tiered accreditation does not significantly compromise consumers understanding of and experience with data sharing or reduce consumer confidence in the data sharing framework.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The Australian Retail Credit Association stated that: “some of the constraints and conditions linked to those forms of restricted accreditation are too complex and restrictive – which will not support the adoption of the CDR by businesses and will cause additional customer confusion.”</td>
</tr>
</tbody>
</table>

Some stakeholders suggested that the proposed new levels and kinds of accreditation were welcomed, with one stakeholder (SISS Data Services) stated that: “We believe all suggested models are technically achievable and are risk appropriate. We have and continue to discuss accreditation levels with various FinTechs and have been able to match business cases with each level of accreditation. We do believe these levels will meet the required outcome of allowing new participants into the CDR regime while maintaining a balance between risk & cost of accreditation (and ongoing compliance).”
NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
| 28. | **Incentive on sponsor to ensure compliance by affiliate**<br>We query whether the obligations on a ‘sponsor’ in connection with their affiliate’s accreditation are sufficiently robust. | In order for an affiliate accreditation to be granted, the sponsor must certify that the affiliate complies with the relevant requirements of the CDR Rules. The sponsor must also take ‘reasonable steps’ to ensure ongoing compliance by the affiliate (Rule 5.5A).<br><br>An affiliate may only make consumer data requests through the sponsor acting on its behalf under a CAP arrangement (Rule 5.1D(2)).<br><br>The ACCC and/or OAIC may take action against an affiliate for non-compliance with the legislative framework, or a sponsor who does not take reasonable steps as described above (noting the amendments to the civil penalty provisions in the CDR Rules). | The accreditation requirements are important in ensuring CDR Consumers can have confidence that the recipients of their CDR Data have been appropriately ‘vetted’ as suitable entities to handle CDR Data. We query whether the current amendments provide a sponsor with enough incentive for it to actively monitor and otherwise ensure that the affiliate complies with their obligations as an Accredited Person. We also query whether there may be uncertainty about what will be required for a sponsor to have taken ‘reasonable steps’. For example, it is not clear whether a sponsor would satisfy the test by simply including an obligation in the CAP agreement which requires the affiliate to comply with the CC Act and the CDR Rules. If this would be sufficient, we suggest that it may provide little protection for a CDR Consumer if a restricted level Accredited Person does not meet its contractual requirements, noting that there is no obligation on a sponsor to enforce the CAP arrangement.<br><br>We **recommend** that the ACCC consider whether the CDR Rules should specify that a sponsor should be liable for the actions of their affiliates and their compliance with the legislative framework (similar to the position for an Accredited Person’s outsourced service providers) (**Recommendation 20**).<br><br>Although stakeholders who provided submissions acknowledged the benefits of achieving flexibility with the introduction of affiliates and sponsors, stakeholders broadly agreed with the identified risk, and supported this Recommendation so that liability for an affiliate is clearly stated in the CDR Rules.<br><br>For example:<br><br>- The **Australian Energy Council** stated that: “While the ACCC does intend to incentivise the sponsor to ensure the affiliate is compliant, it is not entirely clear what these incentives are and whether the sponsor even has the ability to appropriately monitor compliance. For the customer, the addition of affiliate restriction is likely to create further confusion and the ACCC should
NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>consider how customers should be expected to understand when they are engaging with an affiliate entity and what this means for their data. The AEC believes there are alternative mechanisms that have the ability to deliver the customer benefits of the proposed affiliate restriction, with fewer risks. Specifically, tiered accreditation could be implemented through changes to the combined accredited person (&quot;CAP&quot;) arrangements”</td>
</tr>
</tbody>
</table>

- The Commonwealth Bank of Australia stated that: “The Commonwealth Bank has concerns regarding the proposed self-attestation approach for restricted accredited parties, particularly given the PIA findings 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”

- The Office of Australian Information Commissioner stated that: “Rule 5.1D(6) requires a sponsor to take reasonable steps to ensure that the affiliate complies with its obligations as an ADR. The OAIC supports this requirement, and… also supports the principles-based approach to formulating the third party management framework in Schedule 2 of the Rules… In addition... the OAIC would recommend that the ACCC specify certain minimum steps which must be taken by affiliates in the Rules, in order to provide greater regulatory certainty. For example, in relation to reporting requirements, the Rules could require an affiliate to provide their sponsor with reports prepared under Rule 9.4, in addition to providing the report to the ACCC and OAIC.”

- NAB stated that: “… the liability framework may make the affiliate restriction commercially unviable. Under the regime, the sponsor is subject to additional liability and potential civil penalty provisions if the sponsor fails to take reasonable steps to ensure compliance of its affiliates. In practice, liability would be subject to commercial negotiation of indemnities between
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>the parties. However, for an affiliate, in addition to likely providing indemnities for its conduct to the sponsor, the affiliate is also an accredited person and therefore liable for misuse of data or failing to meet other obligations in its own right.</td>
</tr>
</tbody>
</table>

- **Frollo** stated that: *“In order for the sponsor of an affiliate to take reasonable steps to ensure that the affiliate complies with its obligations as an accredited person, some reporting obligations would need to exist between the affiliate and the sponsor. This may need to cover complaints and incidents (those that affect compliance).”*

- The **Financial Legal Rights Centre** stated that: *“There are few incentives on the sponsor to ensure compliance by affiliates since the sponsor will only need to take “reasonable steps to ensure its affiliates comply with the accreditation requirements and ongoing obligations of an accredited party.” There is no strict liability for any breaches. “Reasonable steps” is so uncertain, loose and subjective as to be worthless in practice.”*

- **RSM Australia** stated that: *“We support the expansion to include sponsor/affiliate relationships. However, self-assessments are renowned for being a poor indicator of adherence to a control framework due to inconsistent skills and knowledge of those completing the assessment.”*

- **SISS Data Services** stated that: *“What are reasonable steps? Given our liability, if they are deemed non-compliant. We could ask for them to detail what is reasonable, but it might make the process more complex.”*

- **Quantium** stated that: *“There is no need for direct regulatory burdens upon the affiliate (a person accredited at the restricted level) as regulation may leverage from the direct exposure of the sponsor. Reputational, legal and client exposure of the sponsor creates appropriate incentive for that regulated entity to ‘regulate by contract’ with prospective affiliates with whom...”*
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>it deals. We query therefore whether direct regulation of an affiliate is necessary or desirable, beyond ‘fit and proper person’ accreditation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>... Of course, the sponsor should have a legal obligation to take active and reasonable steps (in addition to extracting contractual commitments) to ensure affiliates comply with accreditation requirements, coupled with sufficient liability exposure in respect of failures by affiliates that could have been avoided if the sponsor had taken appropriate steps, to in order to ensure the integrity of the sponsor/affiliate model.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Australian Business Software Industry Association</strong> stated that: “For sponsors, ABSIA believes that their obligations are currently too onerous. They should be limited to receiving their affiliate's annual self assessments along with any underlying evidence to support their assessment and sharing this information with the ACCC…”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>EnergyAustralia</strong> stated that: “The Enclave Provider and Sponsor should also be liable for the breaches of the Data Enclave Accredited person and Affiliate irrespective of whether the Enclave Provider or Sponsor has acted in accordance with an arrangement in place with the restricted ADR. This liability requirement should be an additional requirement to the existing requirement of taking reasonable steps to ensure compliance by the Data Enclave Accredited person and Affiliate. We share the concerns in Updated PIA that reasonable steps could be taken to mean a condition in a contract that requires compliance with the CDR Rules which would be insufficient.”</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Imposing the liability requirement will mean the Enclave Provider and Sponsor will take more thorough and comprehensive steps in their due diligence and compliance monitoring of Data Enclave Accredited Persons and Affiliates. It also has the second benefit of providing better enforceability for the ACCC across Enclave and Affiliate Restriction arrangements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To further strengthen the incentive, we propose that the arrangement/contract between the Enclave Provider and Sponsor and the Data Enclave Accredited Person and Affiliate, could be regulated in a similar way to how Outsourced Service Provider CDR arrangements/contracts are regulated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This regulated contract should address further outsourcing by the Enclave Provider and Sponsor. For instance, where the Provider/Sponsor is to collect CDR data under the contract, the provider must not further outsource that collection; the provider must not disclose any CDR data to another person, otherwise than under a further regulated contract; and if the provider does disclose such CDR data it must ensure that the other person complies with the requirements of the regulated contract. Applying similar protections of Outsourced Service Providers to Enclave Providers and Sponsors appears proportionate and appropriate where they are effectively providing outsourced ADR services to Data Enclave Accredited persons and Affiliates.&quot;</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>NEW LEVELS AND KINDS OF ACCREDITATION</td>
<td></td>
<td>Some stakeholders also voiced the concern that requiring affiliates to have several sponsors increased the potential for confusion, including around apportioning liability. For example, one stakeholder (FinTech Australia) stated that: “It is not clear why an affiliate is required to only receive data from a sponsor and why, where the affiliate receives data from multiple sources, that each source would need to be a sponsor. Not only does this create additional complexity, it also creates the issue of there being confusion around who would have liability if there was a breach or data incident.”</td>
</tr>
<tr>
<td>29.</td>
<td>The CDR Rules do not deal with a situation where the relevant CAP agreement is terminated, or suspended, or expires</td>
<td>An affiliate must have a sponsor (Rule 5.1D(1)), and a Data Enclave Accredited Person must have an enclave provider (Rule 5.1B(1)). In order to be a sponsor or enclave provider, the Unrestricted Accredited Person must be a provider in a CAP arrangement. An Accredited Person has an obligation to notify the Data Recipient Accrder of any certain matters that might affect the decision to grant accreditation (Rule 5.14).</td>
<td>We note that the CDR Rules will provide that on suspension or revocation of the accreditation of a sponsor or enclave provider, the Data Recipient Accrder may suspend or revoke the accreditation of the affiliate or Data Enclave Accredited Person (as applicable) (Rule 5.17(1), Items 11 and 12 of the table). We consider that this is appropriate and enhances the protection for CDR Consumers. However, if the relevant CAP arrangement between the principal and the provider is suspended, terminated or expires, the Unrestricted Accredited Person will no longer be a ‘enclave provider’ or a ‘sponsor’, but there does not appear to be mechanism for the lower level accreditation to end. We <strong>recommend</strong> that the ACCC consider whether there should be a requirement in the CDR Rules (or perhaps a condition of accreditation) to notify the Data Recipient Accrder if the relevant CAP arrangement is suspended or terminated or expires, and for the Data Recipient Accrder to have the ability to suspend or revoke the restricted accreditation in such a situation (Recommendation 21).</td>
</tr>
</tbody>
</table>
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>It is also not clear what mechanisms would be used if a restricted level Accredited Person wishes to ‘switch’ enclave provider or sponsor after accreditation (e.g. whether they must surrender their existing accreditation and seek a new accreditation in relation to the new sponsor/enclave provider).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We <strong>recommend</strong> that the ACCC consider clarifying the mechanisms available to a restricted level Accredited Person who wishes to ‘switch’ enclave provider or sponsor after accreditation (<strong>Recommendation 22</strong>).</td>
</tr>
<tr>
<td>30.</td>
<td>Risk that CDR Consumer does not know that a provider under a CAP arrangement has been used to collect their CDR Data</td>
<td>The CDR Consumer will be informed that a specific provider will collect their CDR Data when they are asked to provide their consent (Rule 4.11(3)(i)). Rule 7.2(4) will mean that the affiliate or Data Enclave Accredited Person’s CDR policy must contain information about their relationship with the Unrestricted Accredited Person (either an enclave provider or sponsor) If CDR Data may be collected by a provider under a CAP arrangement, the proposed amendments will require an Accredited Person to be a privacy-enhancing feature of the proposed amendments.</td>
<td>We consider that the requirements to inform the CDR Consumer of the specific provider that will be collecting (and/or storing) their CDR Data on behalf of the restricted level Accredited Person to be a privacy-enhancing feature of the proposed amendments.</td>
</tr>
</tbody>
</table>
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>to ensure that their consumer dashboard includes the provider’s name and accreditation number (Rule 1.14(3)(i)).</td>
<td></td>
</tr>
<tr>
<td>31.</td>
<td>Deletion of redundant data</td>
<td>There is a risk that a provider under a CAP arrangement may not comply with a direction by the principal to delete redundant data.</td>
<td>It is not clear whether Rule 7.12(2)(b) will apply to a CAP arrangement for data enclave accreditation arrangements, or for affiliate accreditation arrangements, since the rule will only apply if the principal has been ‘provided with a copy’ of the redundant data. Although the provider will have collected the CDR Data on behalf of the restricted level Accredited Person (and in the case of an enclave provider, the CDR Data will be stored on its ICT infrastructure), it is difficult to see how they will have been ‘provided with a copy’ of that CDR Data. In addition, there does not appear to be any legislative requirement for the provider to comply with a direction by the principal in respect of redundant data. Unlike contractual arrangements for outsourced service providers, the CDR Rules are silent about the matters that must be contained in a CAP arrangement. For example, there is no requirement that it must include provisions which will require the provider to comply with any directions by the principal about deletion or de-identification of redundant data. Without this clarity, there is a risk that a CDR Consumer’s CDR Data will continue to be inappropriately held in an identified form after it becomes redundant.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rule 7.12(2)(b) will mean that the principal to a CAP arrangement must give directions to the provider in relation to deletion of redundant data.</td>
<td></td>
</tr>
</tbody>
</table>
We recommend that the ACCC consider:

- clarifying the intended application of Rule 7.12(2)(b) to CAP arrangements for data enclave accreditation arrangements and for affiliate accreditation arrangements; and

- including matters that must be included in a CAP arrangement, including that the provider must comply with a direction by the principal in respect of redundant data.

(Recommendation 23)

Some stakeholders who provided submissions agreed with the identified risk and supported this Recommendation. For example, one stakeholder (the Commonwealth Bank of Australia) stated that: "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”.

Another stakeholder (SISS Data Services) supported the need for CAP arrangements to specify roles and responsibilities, stating that: “…we believe the written CAP arrangement should specify the roles and responsibilities around the various requirements. As principal recipient is the client-facing service we feel they are they hold the default responsibility. While we acknowledge the ACCC don’t want to determine the text of a CAP arrangement, we do believe a list of minimum requirements that CAP should cover be developed. The list of minimum requirements would be documentation and agreement around requirements like

- Incident management
- Customer complaints
- Dispute resolution
- ACCC Reporting compliance

… Under the CAP arrangement, we acknowledge the requirement for a consumer complaints process. We believe the primary requirement for this to be held by the principal as they are the consumer-facing service provider. Fundamentally all participants have access. As the CAP arrangement is required to be a written document, we believe this document should include a reference
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>to how the complaint process will be handled within the context of the CAP. We understand (and agree) that ACCC don't wish to specify the actual text of these arrangements, but we do believe that ACCC should specify that certain requirements are documented, and roles assigned.”</td>
</tr>
<tr>
<td>32.</td>
<td>Risk of overlap or inconsistency between contractual CAP arrangements and legislative liability</td>
<td></td>
<td>Another stakeholder (FinTech Australia) provided a differing view, stating that: “FinTech Australia questions the ongoing need for CAP arrangements within the rules. This concept was an attempt at allowing multiple parties to collaborate to provide services, however the level of prescription involved in CAP arrangement is unnecessary and restrictive… we do not see the need for the CDR Rules to prescribe incident management arrangements between the parties. In many respects, the level of prescription involved in the CAP arrangements concept should be reduced. We do note the complexity of shared responsibility reporting obligations.”</td>
</tr>
</tbody>
</table>

As discussed above (**Item 31**), the proposed amendments do not specify any requirements for a CAP arrangement, but leave it to the parties to reach a suitable agreement on all matters. For example, a Data Enclave Accredited Person may negotiate a CAP arrangement which clearly allocates all liability for a failure of the relevant ICT environment to adequately protect CDR Data stored in the data enclave to the enclave provider. The Data Enclave Accredited Person may therefore not appreciate that it may still bear responsibility or liability under the legislative requirements as an Accredited Data Recipient, and as a consequence may not take appropriate action to ensure compliance with those requirements, therefore exposing the CDR Consumer to the risk of harm.

As for **Item 1**, we **recommend** that further guidance is required, to ensure all entities participating in the CDR regime understand their obligations (**Recommendation 1**).
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
|     | NEW LEVELS AND KINDS OF ACCREDITATION                                 |                                                                                                  | In addition, one stakeholder raised the need for additional requirements to be included in Part 1 of Schedule 2 for a Data Enclave Accredited Person in relation to managing data enclaves. This stakeholder (SISS Data Services) stated that these requirements should include: “Joint policy on the services provided by each under CAP arrangement and who is responsible & liable. The joint policy should include:  
- Services provided by each party  
- Disclosure to customers  
- Decoupling of the service  
- Obligations surviving post termination of the agreement”  |
|     | Maintenance of records                                               | Rule 9.3(2)(i) will require an ‘accredited data recipient’ to keep and maintain records of any CAP arrangement in which the accredited data recipient is the principal, including how the provider will use and manage any CDR data shared with it. | We consider that it may be critical for the ACCC and/or the OAIC to have access to all information about the CAP arrangement and its operation, in order to take action to effectively enforce compliance with privacy obligations in the legislative framework. There may be instances in which the principal has failed to keep the relevant records, or those records are otherwise no longer available. We recommend that the ACCC consider whether there would be benefits in broadening Rule 9.3(2)(i) to apply to providers in a CAP arrangement (Recommendation 23). |
| 33. | Risk that the CDR Data that a Limited Data Accredited Person can handle is inherently sensitive, or may be if analysed together with CDR Data obtained in relation to other sectors. | ACCC has received advice from cyber-security experts about the risks associated with the types of CDR Data that may be held for the banking sector. A Limited Data Accredited Person will be required to comply with all protections in Schedule 3. | Although we understand that the risks of the CDR Data types included in Schedule 3 have been comprehensively considered from a security perspective (i.e. the risks of the data being of a nature which would be unlikely to be the subject of a cyber security threat), we note that any banking transactions data is likely to be inherently sensitive and could potentially still expose CDR Consumers to risk if it is mishandled, even if there is little security risk in relation to that CDR Data. |
### NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>
|     |      | CDR legislation for the types of CDR Data that it is permitted to handle. | We **recommend** that the ACCC ensure that it is satisfied that the types of CDR Data that may be handled by Limited Data Accredited Persons is appropriate, including through considering feedback received from stakeholders. This is particularly important once other sectors are introduced, and the CDR Data may (if appropriate consent is obtained) be analysed together with other information about the CDR Consumer (Recommendation 24). Many of the stakeholders who provided submissions agreed with the identified risk and supported this Recommendation. For example:  
  - **EnergyAustralia** stated that: “.. allowing lower accreditation for lower risk data sets may have unintended effects in practice, particularly when applied across sectors and where banking and financial data will be included. Multiple items of low risk data can cumulatively present a high risk data set for a customer and it would be difficult for the ACCC to “future proof” the rules and identify these combinations so as to specifically exclude data points that may present this risk. This points to a weakness in the Limited Data Restriction model.”  
  - The **Commonwealth Bank of Australia** stated that: “[the Commonwealth Bank is] 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’.” |
## NEW LEVELS AND KINDS OF ACCREDITATION

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The <strong>Australian Banking Association</strong> stated that: “consumer's financial and banking data is highly sensitive data and cannot be apportioned into lesser grades of sensitivity.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Another stakeholder (the <strong>Financial Rights Legal Centre</strong>) voiced the need for the ACCC to reconsider this model, stating that: “…we do not have confidence that the proposal will produce positive consumer outcomes and will in fact lead to consumer harm… We believe that the ACCC must go back to the drawing board.”</td>
</tr>
<tr>
<td>35.</td>
<td>Risk that a Limited Data Accredited Person will seek to collect CDR Data that does not fall within one of the permitted types of data</td>
<td>Rule 5.1C expressly prohibits such collection. We understand that the technical implementation will mean that a Limited Data Accredited Person will technically only be able to use the ACCC CDR ICT system to request data of a type that falls within Schedule 3.</td>
<td>There is currently little information about how a Data Holder, or an Accredited Data Recipient, who receives a request for CDR Data will know that the request is from, and/or made on behalf of, a Limited Data Accredited Person, and that the request is for the permitted types of CDR Data, before disclosure. We <strong>recommend</strong> that the ACCC consider whether it should clarify how a Data Holder or an Accredited Data Recipient who receives a request for CDR Data will know that the request is from, and/or made on behalf of, a Limited Data Accredited Person, and that the request is for the permitted types of CDR Data, before disclosure. This will assist in providing assurance that the Data Holder/Accredited Data Recipient will not mistakenly disclose more types of CDR Data than the Limited Data Accredited Person is permitted to handle (<strong>Recommendation 24</strong>).</td>
</tr>
</tbody>
</table>
21. **Risks associated with the changes to joint accounts**

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.</td>
<td>JAMS only applies to the disclosure of CDR Data by a Data Holder to an Accredited Data Recipient</td>
<td>The CDR Rules are currently silent on whether disclosure options must be selected (or confirmed) before an Accredited Data Recipient (or Accredited Person) may disclose CDR Data on a joint account to another Accredited Person, a Trusted Advisor or an Insight Recipient (noting that this would be a CDR Insight based on raw CDR Data relating to a joint account).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In other words, there are currently no mechanisms for JAHs to consent to the disclosure of joint account data once it is held by the Accredited Data Recipient. This means that JAHs have no control over their joint account data at this stage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>We recommend that the ACCC consider ensuring that the CDR Rules prescribe how JAHs can have control and visibility over their joint account data once it is held by an Accredited Data Recipient (Recommendation 14).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Some stakeholders who provided submissions strongly agreed with the identified risk and supported this Recommendation (which we have refined based on stakeholder feedback). In particular, these stakeholders were concerned about JAH B will be unaware about the handling of their CDR Data once it is received by the Accredited Data Recipient (e.g. any further disclosures of this information).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example:</td>
</tr>
</tbody>
</table>
|     |      |                               | • The **Commonwealth Bank of Australia** stated that: “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
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>

- **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).”**

- The **OAIC** stated that: “a data holder [should] be required to notify joint account holder B that their joint account CDR data could be further on-disclosed to other third parties, such as another ADR or trusted advisor, in accordance with joint account holder A’s consent. This could occur, for example, when the data holder asks joint account holder B to indicate what disclosure option they prefer under clause 4.7(2) of Schedule 3 to the Rules. This will ensure joint account holder B is given some visibility over the possibility of further disclosures, and has the opportunity to refuse to allow CDR data to be shared from the joint account if they are not comfortable with the possibility of further disclosures.”

One stakeholder submitted that joint accounts should not be included as part of the CDR Rules. This stakeholder (**Deloitte**) stated that:

“While supporting the inclusion of joint accounts as part of the CDR framework, Deloitte recommends that rather than seeking to create new prescriptive rules, the ACCC should require that the requirements organisations have for consumers to access accounts determine the requirements organisations have for consumers to access information from those accounts.

…This same principle would apply to whether a joint account holder needs to be informed about an authorisation to share information by one of the other joint account holders.
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>…The requirement for joint or several authorisation of payments from bank accounts will have been determined for each bank account. These requirements should be used to determine whether joint or several authorisation or notification is required for disclosure of information about account transactions.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>…As noted in our response to the questions raised in section 6.3 Secondary Users, Deloitte recommends that the process for joint account holders to access information on their accounts, be based on an organisation’s existing requirements to authorise transactions on an account and not be the subject of CDR rules.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Another stakeholder raised an additional risk where, if JAH A amends their consent, JAH B will not have visibility of this, and also no longer be able to withdraw their authorisation for this amended consent. This stakeholder (the Consumer Policy Research Centre) stated that:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“…in the case of joint accounts, we note the loss of account holder B’s visibility over the current state of active CDR consents in situations where such consent is amended by account holder A. In addition to removing awareness over how their data is being handled, this effectively invalidates the right of account holder B to withdraw authorisation for amended permissions in relation to data usage and disclosures that they do not consent to (for the simple reason that they are not aware this consent has been given). Our view is that these are not acceptable consumer trade-offs. We reject the notion that providing better granularity of consent requires removing consumer visibility and control over elements of that consent.”</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 37. | CDR Consumers do not understand the mechanism for selecting a disclosure option in JAMS | The proposed amendments to the CDR Rules will assist to ensure that JAHs make informed decisions about disclosure options. Data Holders will be required to ensure that JAMS includes information about:  
  - the difference between a 'pre-approval' disclosure option and a 'co-approval' option (including the impact of each decision), if the Data Holder offers both 'pre-approval' and 'co-approval' options;  
  - the impact of the disclosure options if the Data Holder offers, and both JAH A and JAH B select in JAMS, the pre-approval' or 'co-approval' option;  
  - the fact that both JAH A and JAH B can remove their disclosure option selection in JAMS at any time. | We support the additional requirements to notify JAHs of certain information about the process of selecting a disclosure option in JAMS. From a privacy perspective, we believe that provision of additional information will help CDR Consumers understand the operation of CDR regime, so that informed consent can be obtained from both JAHs, is a positive privacy step. |

There is a risk that CDR Consumers who are JAHs will not understand why and how they have to select a disclosure option in JAMS (and subsequently authorise the Data Holder to disclose data in respect of the joint account to the Accredited Data Recipient without understanding the implications of the disclosure).
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>time (independently of each other), and the impact of this withdrawal; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the fact that when the CDR Data on the joint account is disclosed by a Data Holder to an Accredited Data Recipient, both JAH A and JAH B will be able to see information about the authorisation on their Data Holder Consumer Dashboard (as is required by the CDR Rules), for both ‘pre-approval’ and ‘co-approval options’ (subject to the particular exemptions).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additionally, when a Data Holder sends a notification to a JAH B, inviting them to make a corresponding JAMS election, that notification must contain particular information. The notification must:</td>
<td></td>
</tr>
</tbody>
</table>
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• provide an outline of what the CDR is;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• inform JAH B of the disclosure option that JAH A has selected, or otherwise inform JAH B that JAH A has indicated that they would not like any disclosure option to apply to the relevant joint account;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• inform JAH B that, at present, no disclosure option applies to the account;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• explain to JAH B that no disclosure option will apply to the account unless both JAH A and JAH B have selected the same disclosure option to apply;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• invite JAH B to select the same disclosure</td>
<td></td>
</tr>
</tbody>
</table>
## JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>option as JAH A in respect of the relevant joint account; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• if JAH A did select a disclosure option, identify the relevant Accredited Person to whom JAH A would like to disclose CDR Data in respect of the relevant joint account.</td>
<td></td>
</tr>
</tbody>
</table>
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Inconsistency between JAMS and the ‘offline’ version of JAMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Noting that there will be an ability for CDR consumers to select a disclosure option in an ‘offline’ version of JAMS, there is a lack of clarity about how data holders will be required to ensure that they accurately and promptly reflect the offline selection in their online version of JAMS. This raises the privacy risk that a disclosure option selected in the offline version will not be properly implemented in the online version of JAMS. This raises the privacy risk that a disclosure option selected in the offline version will not be properly implemented in the online version of JAMS, which is relied upon for processing disclosures of joint account CDR Data.

We note that it is important that the online version of JAMS displays the correct disclosure option selected by a JAH at any point in time. This is because the processing of disclosures of CDR Data on joint accounts relies upon the disclosure options recorded in JAMS.

We recommend that the ACCC consider:

- requiring Data Holders to promptly input any disclosure option selected in an offline version of JAMS into the online version of JAMS; and
- implementing measures to ensure that the disclosure option selected in the offline version of JAMS is correctly reflected in the online version of JAMS.

(Recommendation 15)

One stakeholder supported the inclusion of both online and offline versions of JAMs, and providing ‘preapproval’ and ‘co-approval’ options. This stakeholder (Visa) stated that:

“...requiring data holders to offer joint account management services both online and offline, and allowing consumers to set preferences as part of the authorisation process, will be an important step towards improving consumer experiences. The proposed rule changes to offer both ‘preapproval’ and ‘co-approval’ will provide consumers with a greater level of individual control over sharing CDR data from their joint accounts.”
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td>Vulnerable CDR Consumers</td>
<td>As discussed in Step 1B in the Original CDR PIA report.</td>
<td>We note that the proposed amendments to the CDR Rules will provide further clarity around joint accounts and, if implemented, will afford JAHs further privacy protections and ensure that JAHs cannot see the personal information of another JAH. Additionally, important amendments have been introduced that will allow Data Holders to disclose joint account data without a disclosure option having been selected by both JAHs, if the Data Holder considers that asking JAH B to make a disclosure option (or alerting JAH B to the fact that JAH A has selected a disclosure option) may result in financial or physical abuse to JAH A by JAH B. These are privacy-enhancing steps.</td>
</tr>
</tbody>
</table>

   The risks discussed in the Original CDR PIA report in relation to vulnerable CDR Consumer have been, to an extent, mitigated through the proposed amendments to the CDR Rules.

   However, the proposed amendments to the CDR Rules will allow a Data Holder to disclose CDR Data relating to a joint account with only JAH A having selected a disclosure option, if the Data Holder considers that asking JAH B to make a disclosure option (or alerting JAH B to the fact that JAH A has selected a disclosure option) may result in financial or physical abuse to JAH A by JAH B.

   Further, as an additional mitigation strategy to protect vulnerable CDR Consumers, the proposed amendments to the CDR Rules will prohibit Data Holders from displaying CDR Data that comprises of personal information (i.e. name and address) on the Data Holder Consumer Dashboard of another CDR Consumer. This will mean, in effect, that JAHs will not be able to see personal information of another JAH.

   We note that the proposed amendments to the CDR Rules will provide further clarity around joint accounts and, if implemented, will afford JAHs further privacy protections and ensure that JAHs cannot see the personal information of another JAH. Additionally, important amendments have been introduced that will allow Data Holders to disclose joint account data without a disclosure option having been selected by both JAHs, if the Data Holder considers that asking JAH B to make a disclosure option (or alerting JAH B to the fact that JAH A has selected a disclosure option) may result in financial or physical abuse to JAH A by JAH B. These are privacy-enhancing steps.

   However, we note that the proposed amendments to the CDR Rules do not oblige the Data Holder to require a particular, clear and standardised level of evidence, if an exception to the JAMS election process is to apply.

   We recommend that the ACCC:

   - consider ensuring that the CDR Rules prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure option process in JAMS is to apply (or that a notification need not be given);

   - continue to monitor the appropriateness of the measures in place in the CDR Rules to protect vulnerable CDR Consumers, including to investigate any additional measures that could be implemented to afford further protections.

(Recommendation 16)
## Joint Accounts

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>able to see the personal information of another JAH on their joint account via their Data Holder Consumer Dashboard. We understand that this proposed amendment to the CDR Rules reflects extensive consumer experience testing and research, which suggested that being able to see the personal information of another JAH could trigger fear and anxiety in a JAH.</td>
<td>We have refined this Recommendation based on stakeholder feedback. Whilst the majority of stakeholders who provided submissions supported the measures provided for in the proposed amendments to the CDR Rules to ensure the protection of vulnerable CDR Consumers, there was an underlying consensus across the stakeholders regarding the effectiveness of the proposed amendments CDR Rules as currently drafted. For example:</td>
</tr>
</tbody>
</table>

- **AGL Energy Limited** stated that: “The ACCC is proposing rules to allow data holders to refuse the disclosure of CDR data on a joint account or to update a dashboard if they consider it necessary to prevent physical or financial harm. This will allow vulnerable consumers to share CDR data on a joint account as if their account was held in their name alone. We strongly support this proposal as it will allow retailers to put in measures to protect the most vulnerable consumers such as those that are impacted by family violence. AGL has a strong family violence supports program for customers, including flagging accounts of potentially impacted customers to ensure that additional safety measures are placed to prevent any nefarious or unlawful account information access.”

- The **Consumer Policy Research Centre** stated that: “We note the proposed Rules changes that effectively allow data holders to treat joint accounts flagged for abuse as if they were not joint accounts, to better protect the account holder experiencing abuse. We support this safeguard as an important and valuable protection; however, we also feel it is important to also acknowledge its limitations. These are:

  1) reliance on the ability of vulnerable consumers to confirm or self-disclose abuse (which is not always possible, particularly in relationships characterised by coercive control or violence);
### JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) reliance on there being sufficient cultural and technical capacity within organisations to recognise and accommodate such disclosures and to apply protocol for implementation of associated safeguards; and 3) practical implementation being contingent on technical provisions that are declared to be optional rather than mandatory (ie, co-approval on joint accounts).”</td>
</tr>
</tbody>
</table>

They also stated that: “We support amendments that will require making clear in a Joint Account Management Service (JAMS) that data sharing activity/consent would be seen by the other account holder(s). However, we also wish to amplify a clear message from domestic and family violence services conveyed in our recent research into CDR and joint accounts: this alone does not go far enough in fulfilling a duty of care to people experiencing abuse.”

- The Financial Rights Legal Centre stated that: “Financial abuse and harm can take many forms... and can happen over an extended period of time. It could include spending money without permission, accessing finances like early release superannuation payments, forging signatures, coercing someone to sign something, pension-skimming; using the person’s bank account or credit card without their consent; denying them access to their money or bank statements, or opening and closing account to benefit one party over another.

It can also involve a loan that is never paid back, threatening or pressuring someone to invest in something on their behalf, or forcing someone to provide services without being paid or fairly compensated, or expects you to pay their expenses. It can also involve the use or misuse of joint account information particularly in terms of granting one account holder information relating to the other account holder which can lead to the threat of physical
JOINT ACCOUNTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>The proposal when Joint Account Holder (JAH) A selects a disclosure option in the Joint Account Management System (JAMS), the Data Holder must notify JAH B that JAH A has selected a disclosure option and invite JAH B to select a corresponding disclosure option in JAMS. The notification includes a range of information including what the CDR is; that the disclosure option has been selected by JAH A and no disclosure would take place until the JAH B selects the same option as JAH A. If there are no physical or financial harm or abuse flags in place held by a Data Holder, then there is the risk that a perpetrator JAH A may be able to simply force JAH B to agree to the request to disclose, or agree on their behalf. This is a common occurrence where there is a power imbalance or threat of physical violence. The safety/privacy mechanism is therefore dependent on the Data Holder having a flag in place. This is not guaranteed.”</td>
</tr>
</tbody>
</table>

violence. Financial abuse unfortunately materialises in multiple and ever shifting forms.

It is therefore vital to ensure that:

- people experiencing family violence are not prevented from sharing their banking data due to requiring consent of the other party; and
- joint account holders are not unduly exposed by one party making decisions unilaterally about where joint personal information and data (banking transaction, payment and account data) goes.
Another stakeholder submitted that the ACCC should consider reflecting the wording of the Privacy Act in the CDR Rules. This stakeholder (the OAIC) stated that:

“The OAIC appreciates the need to balance the protection of a vulnerable consumer with another consumer’s right to privacy (for example, receiving notifications in relation to how their data is handled). The OAIC notes that the Privacy Act framework recognises that the right to privacy is not absolute, and must give way, for example where the entity ‘reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety’ (Item 1 of the Table, s 16A(1))… The OAIC therefore supports these draft Rule amendments. However, we would recommend that the ACCC consider whether the wording outlined above from section 16A could be adopted in these Rules (and potentially at other points in the Rules, where the same formulation is used). The OAIC considers that the Privacy Act formulation may be preferable, as it requires the entity to have a ‘reasonable belief’ as to the necessity of the action to be taken. Further, as most data holders will be APP entities, this would have the additional benefit of increasing consistency and leveraging a data holder’s existing frameworks for compliance with their Privacy Act obligations.”
22. Risks associated with the introduction of Secondary Users being able to authorise the sharing of CDR Data

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.</td>
<td>Account Holder no longer wishes a Secondary User to be able to authorise the sharing of CDR Data</td>
<td>Under Rules 1.13(1)(e)(ii) and Rule 1.15(5)(b)(ii), Data Holders must provide Account Holders with the ability to revoke or withdraw a Secondary User Instruction.</td>
<td>We consider the requirements for provision of a Secondary User Instruction by the Account Holder, and an easy way for Account Holders to withdraw a Secondary User Instruction (so that CDR Data which relates to their account can no longer be shared as requested by the Secondary User), to be privacy-enhancing features of the proposed changes to the CDR Rules. Stakeholders broadly supported the introduction of the ability for Secondary Users to authorise the disclosure of their CDR Data, with one stakeholder (EnergyAustralia) noting that: “The Secondary User mechanism appears to be a flexible way to allow additional persons to share CDR data relating to an account, while retaining appropriate authorisations by the Account Holder.” However, we are concerned that there may be a lack of clarity about whether, once an Account Holder provides their Secondary User Instruction to a Data Holder (to permit a Secondary User to authorise the disclosure of their CDR Data by the Data Holder to an Accredited Person), the Secondary User is permitted to then also request the Accredited Data Recipient of that CDR Data to further disclose that data to an additional Accredited Person, Trusted Advisor or an Insight Recipient. If so, this would mean that the Account Holder would not have oversight or control over these further disclosures. The amendments are also silent on whether, if an Account Holder withdraws their Secondary User Instruction, an Accredited Data Recipient who has already received the CDR Data can still disclose it to another Accredited Person, a Trusted Advisor or an Insight Recipient.</td>
</tr>
<tr>
<td>No.</td>
<td>Risk</td>
<td>Existing mitigation strategies</td>
<td>Gap analysis and Recommendations</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Several stakeholders recommended that these implications be further considered, with one stakeholder (<em>EnergyAustralia</em>) stating that: “Separately, the Rules should clarify if the Secondary User instruction will apply to disclosures by an ADR (A1) (and not Data Holder) to Accredited Providers (A2) and non-accredited parties.”</td>
</tr>
<tr>
<td>41.</td>
<td>Consequence of withdrawing Secondary User Instruction unclear</td>
<td>We understand that the policy intent is that if an Account Holder withdraws a Secondary User Instruction, this will in effect mean that the Secondary User can no longer request for any sharing of CDR Data from the relevant account to Accredited Persons (i.e. the account that relates to both the Account Holder and the Secondary User). However, it is intended:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• this withdrawal will not consequentially withdraw <em>all</em> authorisations given by the Secondary User to the Data Holder (as some of those authorisations may relate to accounts that do not relate to the Secondary User Instruction and are not relevant to the Account Holder); and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• an ‘all or nothing’ approach applies – if the Account Holder withdraws a Secondary User Instruction, the Secondary User will be unable to authorise the Data Holder to share the relevant CDR Data with <em>any</em> Accredited Persons (i.e. the Account Holder will not be able to stop the sharing with one Accredited Person but not another).</td>
</tr>
</tbody>
</table>
### SECONDARY USERS

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>We are concerned that the drafting of the proposed amendments may not sufficiently capture the policy intent, especially in relation to Rule 1.15(5)(b)(i), which may suggest that the Account Holder does have more granular control over withdrawing a Secondary User’s authorisations. We <strong>recommend</strong> that the ACCC consider whether the wording of the proposed amendments could more clearly clarify the consequences of withdrawal or revocation of a Secondary User Instruction on authorisations that have been already given by the Secondary User (<strong>Recommendation 25</strong>).</td>
</tr>
<tr>
<td>42.</td>
<td>Lack of clarity where there are two or more individuals with account privileges for a single account</td>
<td></td>
<td>Given the desirability for transparency about how CDR Data is handled in accordance with the CDR regime, we <strong>recommend</strong> that the ACCC further consider this issue and whether it would be appropriate to, for example, include in the legislative framework a mechanism so that all individuals with account privileges for an account are notified that a Secondary User Instruction has been given by an Account Holder (which would provide User B with notice that their CDR Data may be shared, so that they can discuss this with the Account Holder if desired) (<strong>Recommendation 25</strong>).</td>
</tr>
</tbody>
</table>

For example, if there are two individuals who have account privileges (User A and User B) for an account, a Secondary User Instruction given in respect of User A may result in information that relates to User B being shared, without User B having any knowledge about or control over that sharing.
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.</td>
<td>Secondary User unaware that Secondary User Instruction has been withdrawn or revoked</td>
<td></td>
<td>The proposed amendments do not seek to introduce additional requirements about what must be included on a Secondary User’s Consumer Dashboard with Data Holders. To ensure that Secondary Users are sufficiently made aware of the fact that an Account Holder has withdrawn a Secondary User Instruction (meaning they are unable to further request for CDR Data to be shared from that account), we recommend that the ACCC consider whether it would be appropriate for the CDR Rules to include a requirement for Data Holders to notify the Secondary User if a relevant Secondary User Instruction has been revoked or withdrawn through its Consumer Dashboard for the Secondary User (Recommendation 25).</td>
</tr>
</tbody>
</table>
| 44. | Secondary User unable to authorise the disclosure of their CDR Data to Accredited Persons if the relevant account is a joint account with a co-approval option selected |                                | We note that the currently proposed amendments will require both joint account holders to have previously indicated that they are comfortable with only one joint account holder undertaking transactions in relation to the CDR Regime (including deciding whether or not to issue, or withdraw, a Secondary User Instruction). As detailed below, some stakeholders were of the view that Secondary Users should be able to share CDR Data relating to joint accounts, irrespective of whether a pre-approval or co-approval option has been selected for the account. One stakeholder (OAIC) supported Secondary Users being able to share CDR Data on joint accounts, stating that: “The OAIC is broadly supportive of the proposal to allow joint account holders to approve secondary users to share CDR data in relation to joint accounts”. However, the OAIC also supported the notion that Secondary Users should be able to authorise the sharing of their CDR Data irrespective of whether the joint account has a pre-approval or co-approval option attached to it, stating: “…we consider that a secondary user
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
</table>

should be able to be approved to share CDR data in relation to a joint account, regardless of the disclosure option chosen by the account holders. The OAIC therefore recommends that cl 2.1(2)(c) of Schedule 3, Part 2 be amended to include joint accounts that have both pre-approval and co-approval arrangements in place.”

In addition, this stakeholder submitted that: “…the processes for providing a secondary user instruction be made consistent with the disclosure option selected on the joint account. For example, if a co-approval disclosure option is in place, the OAIC considers that both joint account holders should be required to give the secondary user instruction. Similarly, if a pre-approval disclosure option is in place, it would be appropriate for one of the joint account holders to give the secondary user instruction on the other’s behalf.”

Another stakeholder (Commonwealth Bank of Australia) voiced the need for all Account Holders to be required to enable any Secondary Users to share CDR Data, stating: “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.”

It was also raised by another stakeholder (Australian Banking Association) that: “…the intersection between joint accounts and secondary users is potentially complex from a Rules (and thus an implementation) perspective.”

Accordingly, we recommend that the ACCC consider to investigate whether it would be appropriate for Secondary Users to be able to authorise the disclosure of their CDR Data to Accredited Persons in situations where the account is a joint account with a co-approval option selected (meaning that it would require both JAH A and JAH B making a Secondary User Instruction for the relevant account) (Recommendation 25).
<table>
<thead>
<tr>
<th>No.</th>
<th>Risk</th>
<th>Existing mitigation strategies</th>
<th>Gap analysis and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td>Account Holders may experience information overload when viewing their Data Holder Consumer Dashboards</td>
<td>Given the possibility for several Secondary Users to be attached to an account, there is a risk that, given the requirements for what must be included on an Account Holder’s Consumer Dashboard with a Data Holder, in addition to details of their own selections and requests, they will be presented with a significant amount of detail on each of the authorisations made by each Secondary User.</td>
<td>Given the significant risk of information overload (as described extensively above in relation to consents and as strongly supported by stakeholders), we recommend that the ACCC continue to conduct consumer research to ensure that, with the additional information Account Holders will be presented in relation to any Secondary Users attached to their account, they will not experience information overload. In addition, the ACCC should consider whether it would be appropriate to provide Data Holders with CX Guidelines detailing how this information should be presented to Account Holders (which reflects the findings of the consumer research) (see Recommendation 2).</td>
</tr>
</tbody>
</table>
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCC</td>
<td>means the Australian Competition and Consumer Commission.</td>
</tr>
<tr>
<td>Accreditation Register</td>
<td>means the register to be established in accordance with subsection 56CE(1) of the CC Act.</td>
</tr>
<tr>
<td>Accredited Data Recipient (ADR)</td>
<td>has the meaning given by section 56AK of the CC Act.</td>
</tr>
<tr>
<td>Accredited Person</td>
<td>means a person who holds an accreditation under section 56CA(1) of the CC Act.</td>
</tr>
<tr>
<td>Australian Privacy Principles (APPs)</td>
<td>means the Australian Privacy Principles at Schedule 1 to the Privacy Act.</td>
</tr>
<tr>
<td>CC Act</td>
<td>means the <em>Competition and Consumer Act 2010</em> (Cth).</td>
</tr>
<tr>
<td>CDR Consumer(s)</td>
<td>has the meaning given by subsection 56AI(3) of the CC Act.</td>
</tr>
<tr>
<td>CDR Data</td>
<td>has the meaning given by subsection 56AI(1) of the CC Act.</td>
</tr>
<tr>
<td>CDR Participant</td>
<td>has the meaning given by subsection 56AL(1) of the CC Act.</td>
</tr>
<tr>
<td>CDR Policy</td>
<td>means a policy that a CDR entity must have and maintain in compliance with subsection 56ED(3) of the CC Act.</td>
</tr>
<tr>
<td>Consumer Dashboard (a)</td>
<td>(a) in relation to an accredited person, has the meaning given by Rule 1.13 of the <em>Competition and Consumer (Consumer Data) Rules 2019</em>.</td>
</tr>
<tr>
<td></td>
<td>(b) in relation to a Data Holder, has the meaning given by Rule 1.14 of the <em>Competition and Consumer (Consumer Data) Rules 2019</em>.</td>
</tr>
<tr>
<td>Consumer Experience Guidelines (CX Guidelines)</td>
<td>means the guidelines of that name, as published by Data61.</td>
</tr>
<tr>
<td>Data Holder</td>
<td>has the meaning given by subsection 56AJ of the CC Act.</td>
</tr>
<tr>
<td>Data Recipient Accrder</td>
<td>means the person appointed to the role of Data Recipient Accrder in accordance with subsection 56CG of the CC Act.</td>
</tr>
<tr>
<td>Data Standards Body</td>
<td>means the body holding an appointment under subsection 56FJ(1) of the CC Act.</td>
</tr>
<tr>
<td>Data Standards</td>
<td>means the data standards made under subsection 56FA of the CC Act.</td>
</tr>
<tr>
<td>CDR Rules</td>
<td>means the <em>Competition and Consumer (Consumer Data Right) Rules 2020</em>.</td>
</tr>
<tr>
<td>OAIC</td>
<td>means the Office of the Australian Information Commissioner.</td>
</tr>
</tbody>
</table>
Open Banking Designation | means the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (Cth).
Privacy Act | means the Privacy Act 1988 (Cth).
Privacy Safeguards (PSs) | means the provisions in Subdivision B to F of Division 5 of Part IVD of the CC Act.
Attachment 2  List of Stakeholder submissions

Written submissions in relation to a draft of this PIA Update report were received from the following entities:

1. AGL Energy Limited
2. Australian Banking Association
3. Australian Business Software Industry Association
4. Australian Energy Council
5. Australian Finance Group Ltd
6. Australian Retail Credit Association (ARCA)
7. BGL Corporate Solutions
8. Chartered Accountants Australia and New Zealand
9. Citi Australia
10. Commonwealth Bank
11. Consumer Policy Research Centre
12. CPA Australia Ltd
13. Cuscal
14. Customer Owned Banking Association (COBA)
15. Data Action Pty Ltd
16. Deloitte
17. EnergyAustralia
18. Envestnet Yodlee
19. Equifax
20. Experian
21. FDATA
22. Financial Planning Association of Australia
23. Financial Rights Legal Centre
24. Finder.com.au
25. FinTech Australia
26. Frollo
27. Gadens
28. Gateway Network Governance Body (GNGB)
29. Home Loan Experts
30. HSBC
31. illion (formerly Dun & Bradstreet)
32. IMB Bank
33. Institute of Certified Bookkeepers
34. Institute of Public Accountants
35. Intuit
36. Judobank
37. Moneytree
38. Mortgage Finance Association of Australia
39. National Australia Bank
40. Office of Australian Information Commissioner
41. Office of Victorian Information Commissioner
42. Origin Energy
43. Plaid
44. Prospa
45. Quantum
46. Regional Australia Bank
47. RSM Australia Pty Ltd
48. SISS Data Services
49. SMSFA
50. TrueLayer
51. Ultradata
52. Visa
53. Xero