Maddocks

Department of the Treasury

CONSUMER DATA RIGHT REGIME

Update 3 to Privacy Impact Assessment

Date of analysis: 17 September 2021

Report finalised on: 29 September 2021

Contents

Part A INTRODUCTION

1. Overview

1.1 On 11 December 2019, the Department of the Treasury (**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]

1.2 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.[2]

1.3 Responsibility for making the CDR Rules, including continually reviewing, considering and revising those CDR Rules as required, has now passed from the Australian Competition and Consumer Commission (**ACCC**) to the Minister for Superannuation, Financial Services and the Digital Economy (**Minister**).

1.4 The CDR Rules commenced on 6 February 2020. Since that time, the ACCC has undertaken several privacy impact update processes to analyse the impact of any proposed amendments to the CDR Rules (**PIA Update reports**).

1.5 In accordance with the recommendation in the Original CDR PIA report, Maddocks has been engaged by Treasury to consider the privacy impacts of a further round of proposed amendments to the CDR Rules and prepare this third updated privacy impact assessment report (**PIA Update 3 Report**).

1.6 The PIA Update 3 process has been a systematic assessment of the proposed amendments to the CDR Rules, identifying the potential impact that these amendments might have on the privacy of individuals, and setting out recommendations for managing, minimising or eliminating that impact.[3]

1.7 This PIA Update 3 Report is designed to:

1.7.1 assist the Minister in identifying and assessing any potential privacy risks to individuals presented by particular proposed amendments to the CDR Rules, so that those risks can be properly considered, and then balanced against all other relevant considerations and benefits associated with the proposed amendments;

1.7.2 present options that could be implemented to reduce or eliminate any identified potential privacy risks, in the form of recommendations for consideration by the Minister; and

1.7.3 illustrate the focus and value being given to privacy risks and risk mitigation.

[1] The Original CDR PIA report, and the responses made to the recommendations in that report, are available at: https://treasury.gov.au/publication/p2019-41016.
[2] Recommendation 1 in the Original CDR PIA report.
[3] *Guide to undertaking privacy impact assessments (May 2014),* published by the Office of the Australian Information Commissioner (**OAIC**) (https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/).

1.8 We have based our discussion and analysis in this PIA Update 3 Report on a consolidated version of the draft CDR Rules (version 34) provided to us by Treasury on 10 September 2021, which includes:

1.8.1 changes relating to how CDR Data may be accessed (**Access Changes**), including through:

(a) 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;

(b) 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;

(c) the introduction of changes that will allow for a person to apply for a new level of accreditation, being 'sponsored accreditation'; and

(d) the introduction of changes that will allow for CDR Data to be handled by non-accredited CDR Representatives; and

1.8.2 the introduction of a default pre-approval option for all joint accounts, and the general application of the joint account CDR Rules for all Sectors unless specifically amended by a Sector-specific Schedule to the CDR Rules (**Joint Account Changes**).

2. Structure of, and approach to, this PIA Update 3 Report

2.1 This PIA Update 3 Report should be read in conjunction with draft 34 (dated 10 September 2021) of the CDR Rules provided by Treasury.

2.2 This PIA Update 3 Report is comprised of the following sections:

2.2.1 **Part A – Introduction:** This section describes the PIA processes that have been undertaken to date, explains the purpose of the PIA Update 3 Report, and introduces the key changes that will be introduced if the proposed amendments to the CDR Rules are made.

2.2.2 **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.

2.2.3 **Part C – Methodology:** This section details how we have undertaken this PIA Update 3 Report, and includes information about the scope of this PIA Update 3 Report.

2.2.4 **Part D – Project Description:** This section contains a high-level summary of the further proposed changes to the CDR Rules discussed in paragraph 1.8 of this **Part A [Introduction]**, and discusses the various concepts and information flows relevant to those proposed changes.

2.2.5 **Part E – Analysis of Risks (Section 1: Access Changes):** This section sets out our analysis of the potential privacy risks that we have identified as being associated with the proposed changes to the CDR Rules in relation to the Access Changes. We have identified current mitigation strategies and conducted a gap analysis to identify any areas of concern, and included recommendations to mitigate any privacy risks.

2.2.6 **Part E – Analysis of Risks (Section 2: Joint Account Changes):** This section sets out our analysis of the potential privacy risks that we have identified as being associated with the proposed changes to the CDR Rules in relation to the Joint Account Changes. We have identified current mitigation strategies and conducted a gap analysis to identify any areas of concern, and included recommendations to mitigate any privacy risks.

2.2.7 **Part F – Glossary:** This section sets out a list of capitalised terms that we have used in this PIA Update 3 Report, and their definitions.

2.2.8 **Part G – List of Submissions:** This section contains a list of stakeholders who provided written submissions as part of Treasury's stakeholder consultation process, which we have considered as part of this PIA Update 3 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 to address privacy risks that we have identified.

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

4. Summary of findings

4.1 Over the course of the development of the proposed amendments to the CDR Rules, we have been very pleased to note how some strategies, particularly designed to mitigate or identified privacy risks have been included or strengthened in the CDR Rules as the drafting of the amendments has progressed over time.

4.2 However, we consider that the proposed amendments to the CDR Rules will still have some impacts involving potential privacy risk for individuals who are CDR Consumers. These are set out in detail in **Part E [Analysis of Risks]**, but include the following key risks:

General key risks

4.2.1 We consider that the complexity of the framework underpinning the CDR regime means that entities participating in the CDR regime (such as Data Holders, Accredited Persons and Accredited Data Recipients) and CDR Consumers may not understand, or take steps to action, their obligations or rights under the legislative framework.

Key risks in relation to Trusted Advisers

4.2.2 These changes will mean that CDR Data will be disclosed outside the CDR regime, where the data will have fewer privacy protections (or potentially no privacy protections if the recipient is not an APP entity for the purposes of the Privacy Act) than the same data will have when being held by an entity within the CDR regime, and CDR Consumers may not understand the implications of consenting to disclosure of their CDR Data to a recipient outside of the CDR regime.

4.2.3 It is possible that an Accredited Data Recipient may disclose CDR Data to an entity which does not fall within a class of Trusted Advisers (and is therefore not subject to appropriate professional or regulatory obligations in relation to the handling of that data), or to a Trusted Adviser who has been banned or disqualified, or is subject to an enforceable undertaking (and is therefore not a suitable person to be handling CDR Data which may be inherently sensitive).

Key risks in relation to CDR Insights

4.2.4 Again, CDR Data will be disclosed outside the CDR regime and CDR Consumers may not understand the implications of consenting to disclosure of their CDR Data to a recipient outside of the CDR regime.

Key risks in relation to Sponsored Accreditation

4.2.5 CDR Consumers may not understand the impact of an Affiliate being involved in the handling of their CDR Data (i.e. that an Affiliate has not been subject to as thorough an accreditation process as a person who has been accredited at the unrestricted level, in that an Affiliate can self-attest that it has appropriate information security capabilities, while an Accredited Data Recipient that is accredited at the unrestricted level must provide independent assurance of those capabilities).

Key risks in relation to CDR Representatives

4.2.6 Although CDR Principals will be liable for a breach by a CDR Representative of certain provisions in a CDR Representative Arrangement, the CDR Rules do not require a CDR Representative Arrangement to include a provision that requires the CDR Representative to only use and disclosure the CDR Data they receive in accordance with the consent given by the CDR Consumer (or another 'permitted use' under the CDR Rules).

4.2.7 The scope of a CDR Consumer's consent, and any subsequent withdrawal or expiry of that consent, may not be appropriately communicated between the CDR Principal and the CDR Representative.

Key risks in relation to Joint accounts

4.2.8 We are concerned that applying the default pre-approval disclosure option means that a joint account holder's CDR Data may be disclosed without that joint account holder having taken active steps to give informed consent to the sharing of that CDR Data. Such joint account holders may be unaware of the default pre-approval option on their joint accounts before the default setting takes effect;

4.2.9 We suggest there is likely to be uncertainty for Data Holders about how to determine whether joint account holders need to be informed about the sharing of their joint account CDR Data where it is alleged that doing so may cause physical, psychological or financial harm or abuse to another person. This may mean that data is shared without, or not shared with, proper knowledge and authorisation.

4.2.10 CDR Consumers may not understand the implications of 'opting out' of receiving important notifications regarding Consumer Data Requests on joint accounts.

4.2.11 The joint account CDR Rules, which will apply for all designated Sectors, may not be 'fit for purpose' for all Sectors.

5. Recommendations to address general risks

Recommendation 1 Complexity of the CDR regime

We recommend that detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules be issued, or previously issued guidance amended, in order to explain the proposed changes.

We suggest that different forms of guidance could be developed and specifically tailored to assist:

- CDR Consumers;
- Data Holders;
- Accredited Persons at both the unrestricted level and the sponsored level; and
- persons receiving CDR Data who are outside of the CDR regime (including CDR Representatives, Trusted Advisers and recipients of CDR Insights).

Recommendation 2 Transfer of CDR Data

We recommend that Treasury consider whether it is appropriate to amend the Data Standards, and/or ensure that appropriate guidance is provided, so that it is clear that all CDR Data (including CDR Insights) must be appropriately encrypted in accordance with Schedule 2 to the CDR Rules, from the time the data leaves the Accredited Data Recipient's CDR data environment until it reaches the recipient's IT environment.

6. Recommendations to address risks associated with Trusted Advisers

Recommendation 3 Trusted Advisers

We recommend that Treasury consider:

- only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who are APP entities for the purposes of the Privacy Act;
- if the above is not possible or practical (e.g. it would defeat the policy objective by excluding many small businesses who are Trusted Advisers (and not Accredited Data Recipients) from receiving the CDR Data), only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who have agreed (through a contractual arrangement with the Accredited Data Recipient) to effectively comply with the requirements of APP 1, APP 6 and APP 11, and the Notifiable Data Breach scheme; or

- if the above is not possible or practical, requiring the Accredited Data Recipient to tell the Trusted Adviser of the scope of the CDR Consumer's consent, and to remind the recipient (i.e. the Trusted Adviser) of their fiduciary or regulatory obligations in relation to the CDR Consumer.

Additionally, we recommend that Treasury consider undertaking an analysis of whether each of the proposed classes of Trusted Adviser will at least be subject to obligations that will require the recipient to use CDR Data that it receives consistently with the consents provided by the CDR Consumer (e.g. if they would be required to do so as part of ethical obligations).

Recommendation 4 Transparency for CDR Consumers

We recommend that Treasury consider whether it would be appropriate to continue, in consultation with the Data Standards Body, to conduct consumer research on what is the best way to present a CDR Consumer with information on the implications of providing a disclosure consent which permits the disclosure of their CDR Data to Trusted Advisers (and therefore outside of the CDR regime), 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.

We suggest this could be achieved by expanding proposed Rule 8.11(1A) to require the Data Standards to include provisions that cover ensuring that CDR Consumers are made aware that if they provide a TA disclosure consent, their CDR Data will leave the CDR system.

We also recommend that Treasury consider whether the CDR Rules should allow the Data Standards to specify different standards for obtaining consent to disclose CDR Data to Trusted Advisers, depending on whether:

- the CDR Consumer is an individual or sole trader and consenting to disclosure of their CDR Data; and
- the CDR Consumer is a company or other business and is consenting to disclosure of CDR Data about their business.

Recommendation 5 Classes of Trusted Advisers

We recommend that further guidance be provided about what constitutes the 'reasonable steps' that an Accredited Data Recipient is required to take to establish that a Trusted Adviser falls within a class of persons to which CDR Data can be transferred. For example, we suggest that it might be best practice for the CDR Rules, or the Data Standards, to require the Accredited Data Recipient to:

- obtain evidence that the Trusted Adviser falls within a class specified in proposed Rule 1.10C(2); or
- check a public register for the relevant class of Trusted Adviser.

We also recommend that Treasury confirm that proposed Rule 1.10C(2) will not have the unintended effect of allowing persons who have been banned or disqualified by their profession, or who are subject to an enforceable undertaking, being included in a class of Trusted Adviser.

7. Recommendations to address risks associated with CDR Insights

Recommendation 6 Clarity regarding the CDR Rules

We recommend that Treasury consider whether it is appropriate for the CDR Rules to be further developed and refined for further clarity regarding the definition of CDR Insights, and/or that Treasury work with the relevant regulators of the CDR regime to ensure that further detailed guidance is issued about CDR Insights, before the proposed amendments to the CDR Rules are introduced.

Recommendation 7 Disclosing CDR Insights

We recommend that Treasury consider:

- only allowing CDR Insights to be disclosed outside of the CDR regime to recipients who are APP entities for the purposes of the Privacy Act; or
- if the above is not possible or practical, only allowing CDR Insights to be disclosed outside of the CDR regime to recipients who have agreed (through a contractual arrangement with the Accredited Data Recipient) to effectively comply with the requirements of APP 1, APP 6 and APP 11, and the Notifiable Data Breach scheme.

Recommendation 8 Transparency regarding CDR Insights

We recommend that Treasury consider amending the proposed CDR Rules to specify that Data Standards must be made to ensure that, in addition to the fact that the CDR Data will leave the CDR system, the CDR Consumer is made aware of the implications and consequences of their CDR Data leaving the CDR system (such as that their data will be afforded fewer privacy protections).

Additionally, we recommend that Treasury consider:

- whether different rules should be able to apply for CDR Consumers who are individuals or sole traders, and for CDR Consumers who are businesses;
- providing clear and detailed guidance to the market to ensure that potential recipients of CDR Insights understand that they must not seek to pressure a CDR Consumer to consent to the disclosure of their CDR Insight;

- whether (through the Data Standards) CDR Consumers should be made aware of the implications and consequences of their CDR Data leaving the CDR system;

- working with the Data Standards Body to develop appropriate Data Standards (in consultation with industry and informed by consumer research), to ensure that CDR Consumers fully understand what it is they are consenting to in relation to their CDR Insights; and

- CDR Consumers should be required to be shown the particular CDR Insight before it is disclosed (as opposed to simply being provided with an explanation of the CDR Insight or the purpose for its disclosure), so that they can decide not to provide their consent if they do not wish it to be disclosed. For example, CDR Insights in relation to verifying credits and debits on an account may potentially disclose information which an individual CDR Consumer may be uncomfortable about disclosing.

We also recommend that Treasury consider requiring that further consumer research be conducted on whether CDR Consumers understand the difference between a one-off versus an ongoing use and disclosure consent in relation to CDR Insights, and based on this research, determine whether it would be appropriate for the CDR Rules and/or Data Standards to prescribe how such consent must be sought from CDR Consumers.

Finally, we recommend that Treasury consider whether it would be appropriate to:

- consolidate the requirements on Accredited Persons to update Consumer Dashboards in relation to CDR Insights (as there is some overlap in requirements); and

- similar to the information provided when a CDR Consumer provides their consent, include a requirement for an Accredited Person to provide the preview (if that is the approach adopted) of the CDR Insight disclosed in its Consumer Dashboard.

8. Recommendations to address risks associated with Sponsored Accreditation

Recommendation 9 Role of Affiliates

We recommend that Treasury 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 information on the implications of providing a consent which will permit the collection of CDR Data by a Sponsor at the request of an Affiliate, and the disclosure of that CDR Data to the Affiliate.

Recommendation 10 Compliance by Affiliate

We recommend that Treasury takes steps to ensure that there is appropriate guidance about what is required for a Sponsor in relation to its Affiliate (particularly in relation to actively monitoring and ensuring that the Affiliate is suitable to handle CDR Data). For example, it is not clear whether a Sponsor would satisfy the test by simply including appropriate warranties or obligations in the Sponsorship Arrangement.

9. Recommendations to address risks associated with CDR Representatives

Recommendation 11 Disclosure of CDR Data to CDR Representatives

We recommend that Treasury consider strengthening the requirements for CDR Representative Arrangements, to further ensure that a CDR Representative will only use and disclose CDR Data after receipt from the CDR Principal (i.e., the Accredited Data Recipient) in accordance with the consent of the CDR Consumer.

This could be achieved by:

- extending the matters that must be in a CDR Representative Arrangement to include a contractual obligation on the CDR Representative to comply with section 56EI (Privacy Safeguard 6) of the CC Act, in respect of Service Data, as if it were an Accredited Person; or
- including a requirement that the CDR Representative Arrangement must include an obligation on CDR Representative to comply with APP 6 of the Privacy Act (as if it were an 'organisation' under the Privacy Act).

Recommendation 12 CDR Representative Arrangements

We recommend that Treasury consider amending the draft CDR Rules so that CDR Representative Arrangements are expressly required to contain an obligation:

- upon the CDR Representative to accurately communicate the CDR Consumer's consent to the CDR Principal; and
- in relation to withdrawal of a CDR Consumer's consent or authorisation:
    - upon the CDR Representative to notify the CDR Principal if the CDR Representative becomes aware that the CDR Consumer has withdrawn their consent; and
    - upon the CDR Principal to notify the CDR Representative if they otherwise become aware that the consent or authorisation has been withdrawn or expired,

so that the CDR Representative and the CDR Principal do not inadvertently continue to collect, use or disclose CDR Data without an appropriate consent and authorisation.

Recommendation 13	**Continued use of CDR Data by a CDR Representative**

We recommend that Treasury consider amending the draft CDR Rules to provide that CDR Representative Arrangements must include a requirement for Accredited Data Recipients to notify a CDR Representative if their accreditation ends, and:

- notify the CDR Representative that any consents it has collected in relation to the CDR Consumer's CDR Data expire (explaining the consequences of this i.e. the CDR Representative can no longer use the CDR Data, nor further disclose this CDR Data); and
- promptly direct them to delete any CDR Data (in accordance with the CDR Data deletion process).

We also recommend that similar protections could be imposed if a CDR Consumer subsequently withdraws their consent (or the consent otherwise expires), so that both the CDR Principal and the CDR Representative are made aware of the status of the consent and required to take appropriate actions.

10. Recommendations to address risks associated with Joint Accounts

Recommendation 14 Implementation of the default pre-approval model

We recommend that the decrease in privacy protections that would be afforded to joint account holders under the proposed changes to the CDR Rules be carefully considered by Treasury, as part of the balancing of relevant factors.

We also recommend that if a decision is made to implement the default pre-approval model despite the impact on privacy rights, consideration be given to implementing a process (if technically possible) so that:

- after one joint account holder (JAH A) makes a Consumer Data Request in respect of joint account CDR Data, the data is not immediately shared;
- after JAH A makes the Consumer Data Request, the other joint account holder(s) (JAH B) is notified of the request and given a reasonable window of time in which to select a disclosure option (and notified that if the pre-approval option (or no option) is selected in the given timeframe, the joint account CDR Data will be shared in accordance with the Consumer Data Request); and
- the joint account CDR Data is then:
    - if JAH B selects the pre-approval option (or does not select an option in the given timeframe), shared in accordance with the Consumer Data Request;
    - if JAH B selects the co-approval option and consents to the disclosure of the CDR Data, shared in accordance with the Consumer Data Request;
    - if JAH B selects the co-approval option and does not consent to the disclosure of the CDR Data, not shared (i.e. the Consumer Data Request is not given effect); and
    - if JAH B selects the no disclosure option, not shared (i.e. the Consumer Data Request is not given effect).

Recommendation 15 Protecting joint account holders from harm

We recommend that Treasury consider amending the draft CDR Rules to provide more detail about the standard to which the Data Holder must be satisfied that a joint account holder is at risk of physical, psychological or financial harm or abuse (e.g. an obligation for them to be reasonably satisfied or to reasonably believe this), so that the protection of that joint account holder from harm outweighs the impact on another joint account holder's right to know how their joint account CDR Data is being shared.

Recommendation 16 Giving effect to elections made through DOMS

We recommend that Treasury work with the regulators of the CDR regime to ensure that appropriate guidance (including guidance about technical requirements) is provided to Data Holders to ensure that they understand what 'as soon as practicable' means in the context of an election made through DOMS (which we consider should be as near real time as is technically possible).

Recommendation 17 Ensuring CDR Consumers who are joint account holders are aware of the default pre-approval setting

We recommend that if Treasury implements the proposed amendments to the CDR Rules, Treasury ensure that all CDR Consumers are made aware, prior to the commencement of the amended CDR Rules, of the change to the default disclosure option setting. For example, a broad education campaign could be a mechanism to:

- advise joint account holders of the default data setting for data sharing on joint accounts being set to 'pre-approval';
- inform joint account holders about what options are available in relation to joint accounts;
- explain the effect of each disclosure option and how it operates;
- inform joint account holders about how they can change the default sharing setting on their joint accounts.

Additionally, we recommend that Treasury implement the above a reasonable amount of time before the default disclosure option is implemented. This will give joint account holders the opportunity to consider the impact of the various disclosure options and make an informed choice.

Recommendation 18 Notifications for joint account holders

We recommend that Treasury consider whether it would be appropriate to:

- ensure that CDR Consumers who are joint account holders are provided with appropriate guidance about what type of notifications they can disable, and the impacts of disabling those notifications; and
- regularly remind joint account holders if they have disabled notifications, such that they are prompted to consider whether they should re-enable the notifications.

Recommendation 19	**Application of the joint account CDR Rules to other designated Sectors**

We recommend that, because the privacy risks and issues for joint account holders may be very different for different Sectors, the privacy implications of joint accounts for any new Sector(s) are considered by Treasury for each current and new Sector, including whether it is necessary to adjust the application of the general joint account CDR Rules for a new sector (through a Sector-specific schedule.

(For example, if all Data Holders in a Sector are not likely to already have mature processes in place to consider the likelihood that a joint account holder may suffer physical, psychological or financial harm or abuse, Treasury should consider whether proposed Rule 4.15A should be further supplemented by way of a Sector-specific Schedule).

Part C METHODOLOGY

11. Our methodology

11.1 We conducted our PIA Update 3 process broadly in accordance with the OAIC's *Guide to undertaking privacy impact assessments*. This involved the following steps:

Stage	Description of steps
1.	**Plan for the PIA Update 3 Report:** We were provided with initial instructions about the proposed amendments to the CDR Rules, including in an initial workshop with Treasury. We were provided with the drafting instructions to amend the CDR Rules, to assist us to gain an understanding of Treasury's intentions for the proposed amendments to the CDR Rules. We also agreed on the scope of this PIA Update 3 Report (discussed further in this **Part C [Methodology]** below), the approach to undertaking stakeholder consultation, and the timeframes for the necessary activities involved in conducting this PIA Update 3 Report.
2.	**Privacy impact analysis and compliance check:** In this stage, we identified and critically analysed how the proposed amendments to the CDR Rules will impact upon privacy, both positively and negatively. For the reasons elaborated in the Original PIA report, we took the same approach to risk assessment which was adopted in the original CDR regime analysis, and have not endeavoured to quantify or label the level of risk associated with each of the identified privacy risks.
3.	**Privacy management and addressing risks:** We considered potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
4.	**Recommendations:** From the stages referred to above, we prepared indications of potential recommendations to remove or reduce identified avoidable privacy risks.
5.	**Draft issues paper:** From the stages referred to above, we prepared a draft issues paper to assist Treasury with its stakeholder consultation process.
6.	**Stakeholder consultation**: We facilitated a stakeholder consultation process, in the form of a 'privacy roundtable' organised by Treasury. This was attended by a range of stakeholders, including those from the fintech industry, Data Holders, Accredited Data Recipients, consumer representatives and regulators, who all provided very useful insights into privacy risks associated with the draft CDR Rules. Treasury published a draft of the proposed legislative instrument to amend the CDR Rules, with an invitation to members of the public to provide written submissions to either or both documents. Treasury provided us with those submissions, from which we identified further valuable insights.
7.	**Privacy management and addressing risks:** We further refined the potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
8.	**Recommendations:** From the stages referred to above, we prepared recommendations to remove or reduce identified avoidable privacy risks.

Stage	Description of steps
9.	**Report:** We finalised this PIA Update 3 Report.
10.	**Respond and review:** We understand that Treasury will review this PIA Update 3 Report, in consultation with other stakeholders as required, to include responses to our recommendations.

12. Scope of this PIA Update 3 Report

12.1 The scope of this PIA Update 3 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 PIA report, this PIA Update 3 Report does not include consideration of any possible future versions of the CDR Rules or the Data Standards.

Part D PROJECT DESCRIPTION

SECTION 1: ACCESS CHANGES

13. Introduction of disclosure of CDR Data to Trusted Advisers

13.1 The proposed amendments to the CDR Rules will, if passed, introduce the ability for CDR Consumers to provide consent (which must comply with the requirements for the provision of consent under the CDR regime) for the disclosure of their CDR Data to a Trusted Adviser. This will be achieved by proposed Rule 1.10A(1)(c)(iii), which will allow CDR Consumers to give a 'TA disclosure consent' to an Accredited Data Recipient to disclose CDR Data to a Trusted Adviser.

13.2 Under proposed Rule 1.10C(2), a Trusted Adviser must belong to one of the following classes of persons (each of whom is subject to existing fiduciary or regulatory obligations):

13.2.1 qualified accountants within the meaning of the *Corporations Act 2001* (Cth) (**Corporations Act**);

13.2.2 persons who are admitted to the legal profession (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession;

13.2.3 registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009* (Cth);

13.2.4 financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*;

13.2.5 relevant providers within the meaning of the Corporations Act other than:

(a) provisional relevant providers under section 910A of the Corporations Act; and

(b) limited-service time-sharing advisers under section 910A of the Corporations Act; and

13.2.6 mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009* (Cth).

13.3 Proposed Rule 1.10C(3) clarifies that a person is taken to be a member of a class for the purposes of proposed Rule 1.10C if the Accredited Data Recipient has taken reasonable steps to confirm that a person nominated as a Trusted Adviser was, and remains, a member of a class specified in proposed Rule 1.10C(2).

Obligations of Accredited Data Recipients

13.4 Proposed Rule 7.9(3) will require an Accredited Data Recipient that has disclosed CDR Data to a Trusted Adviser to, as soon as practicable, update each consumer dashboard that relates to the Consumer Data Request to indicate:

13.4.1 what CDR Data was disclosed (proposed Rule 7.9(3)(a));

13.4.2 when the CDR Data was disclosed (proposed Rule 7.9(3)(b)); and

13.4.3 the Trusted Adviser to whom the CDR Data was disclosed (proposed Rule 7.9.3(c)).

13.5 In addition:

13.5.1 under proposed Rule 9.3(2)(eb), Accredited Data Recipients must keep and maintain records about disclosures of CDR Data to Trusted Advisers, and Trusted Advisers to whom CDR Data is disclosed; and

13.5.2 under proposed Rule 9.3(2)(ec), the Accredited Data Recipient must keep and maintain records, including a record of the steps it has taken to confirm that a Trusted Adviser is a member of a class of Trusted Advisers.

Obligations of Trusted Advisers

13.6 Trusted Advisers will not be Accredited Persons and therefore will not be subject to the regulatory obligations that apply to Accredited Data Recipients under the CDR regime.

Data Standards

13.7 Proposed Rule 8.11(1)(c)(iv) will require the Data Standards Chair to make one or more Data Standards about the consumer experience data standards for disclosure of CDR Data to Trusted Advisers.

14. Introduction of disclosure of CDR Insights to non-accredited persons

14.1 The proposed amendments to the CDR Rules will, if passed, introduce the ability for CDR Consumers to provide consent (which must comply with the requirements for the provision of consent under the CDR regime) for the disclosure of a CDR Insight to any person. A CDR Insight, in relation to an 'insight disclosure consent', is defined to mean *'the CDR data subject to the consent'.* This will be achieved by proposed Rule 1.10A(1)(c)(iv), which will allow CDR Consumers to consent to the disclosure of their CDR Data to a specified person in accordance with an 'insight disclosure consent'.

14.2 Proposed Rule 1.10A(3) provides that an insight disclosure consent is a consent given by a CDR Consumer (in accordance with the requirements for the provision of consent under the CDR regime) to an Accredited Data Recipient of particular CDR Data to disclose it to a specified person for one of the following purposes:

14.2.1 verifying the CDR Consumer's identity;

14.2.2 verifying the CDR Consumer's account balance; or

14.2.3 verifying the details of credits to, or debits from, the CDR Consumer's accounts.

14.3 However, proposed Rule 1.10A(3)(b) provides that if the CDR Data relates to more than one transaction, the Accredited Data Recipient is not authorised to disclose an amount or a date in relation to any individual transaction. Additionally, proposed Rule 7.5A(4) provides that the Accredited Data Recipient is only permitted to disclose a CDR Insight under an insight disclosure consent if the CDR Insight does not include or reveal 'sensitive information' (as defined in the Privacy Act).

Obligations of Accredited Data Recipients

14.4 Proposed Rule 4.11(3)(ca) will require that when an Accredited Data Recipient asks a CDR Consumer to give consent, the Accredited Data Recipient must provide an explanation to the CDR Consumer of the CDR Insight about what the CDR Insight would reveal or describe

14.5 Proposed Rule 7.9(3) will require an Accredited Data Recipient that discloses a CDR Insight to, as soon as practicable, update each consumer dashboard that relates to the Consumer Data Request to indicate:

14.5.1 what CDR Data was disclosed;

14.5.2 when the CDR Data was disclosed; and

14.5.3 the person to whom the CDR Data was disclosed.

14.6 Proposed Rule 9.3(2)(ed) will require Accredited Data Recipients to keep and maintain records of disclosures of CDR Insights, including a copy of each CDR Insight disclosed, to whom it was disclosed, and when.

Data Standards

14.7 Proposed Rule 8.11(1)(c)(v) will require the Data Standards Chair to make one or more Data Standards about the consumer experience data standards for disclosure of CDR Insights.

14.8 Additionally, proposed Rule 8.11(1A) will require the Data Standards for obtaining authorisations and consents, and withdrawal of authorisations and consents, that relate to obtaining insight disclosure consents, to include provisions that cover:

14.8.1 how the Accredited Person can meet the requirement to explain a CDR Insight in accordance with proposed Rule 4.11(3)(ca) (proposed Rule 8.11(1A)(a)); and

14.8.2 ensuring that the CDR Consumer is made aware that their data will leave the CDR system when it is disclosed (proposed Rule 8.11(1A)(b)).

15. Introduction of a sponsored level of accreditation

15.1 The proposed amendments to the CDR Rules will, if passed, introduce a new Rule 5.1A to provide that accreditation may be at the unrestricted level, or at the sponsored level (i.e. the proposed Rule 5.1A will introduce the concept of a sponsored level of accreditation). This means that a person may apply for accreditation at the sponsored level, noting that if their application is successful they will become an **Affiliate**. However, before an Affiliate can access CDR Data, they must also have an arrangement (**Sponsorship Arrangement**) in place with a person who has unrestricted accreditation and is a registered sponsor. A person will be considered to be a registered sponsor (**Sponsor**) if:

15.1.1 they have notified the Data Recipient Accreditor in accordance with proposed Rule 5.14(2) (proposed Rule 5.1B(8)(a)); and

15.1.2 the Registrar has recorded on the Register of Accredited Persons that the person is an Affiliate of the Sponsor (proposed Rule 5.1B(8)(b)).

15.2 For completeness, pursuant to proposed Rule 5.1B(3), Affiliates will only be able to make Consumer Data Requests to:

15.2.1 Accredited Data Recipients under proposed Rule 4.7A; or

15.2.2 through a Sponsor acting at its request under a Sponsorship Arrangement.

Sponsorship Arrangements

15.3 Proposed Rule 1.10D(1) provides that a Sponsorship Arrangement is a written contract between a Sponsor and an Affiliate, under which:

15.3.1 the Sponsor agrees to disclose to the Affiliate, in accordance with Rule 5.1B(2), CDR Data that it holds as an Accredited Data Recipient; and

15.3.2 the Affiliate undertakes to provide the Sponsor with such information and access to its operations as is needed for the Sponsor to fulfil its obligations as a Sponsor.

15.4 Relevantly, pursuant to proposed Rule 1.10D(2), a Sponsorship Arrangement may also provide for a Sponsor to:

15.4.1 make Consumer Data Requests at the request of the Affiliate; or

15.4.2 use or disclose CDR Data at the request of an Affiliate.

15.5 If CDR Data will be collected by a Sponsor at the request of an Affiliate, the request for consent by the CDR Consumer must specify this fact (proposed Rule 4.3(2A)(a)), and a consent for the Affiliate to collect the CDR Data is taken to be consent for the Sponsor to collect that CDR Data (proposed Rule 4.3(2A)(b)).

15.6 In addition, when the CDR Consumer is asked to provide consent (and the CDR Data will be collected by a Sponsor at the request of an Affiliate), they must be informed of, among other things (proposed Rule 4.11(3)(i)):

15.6.1 the fact that the Affiliate is the Accredited Person and the Sponsor will be collecting the CDR Data on request by the Affiliate;

15.6.2 the Sponsor's name and accreditation number; and

15.6.3 the fact that the CDR Consumer can obtain further information about such collections or disclosures from the Sponsor's CDR policy (noting that a link to this CDR policy must be provided).

15.7 Proposed Rule 7.6(4) will mean that any CDR Data collected by a Sponsor at the request of an Affiliate is taken to also have been collected by the Affiliate.

Obligations of Sponsors

15.8 Proposed Rule 5.14(2) will require Sponsors to notify the Data Recipient Accreditor as soon as practicable (but no later than 5 business days after) if:

15.8.1 the person becomes a Sponsor of an Affiliate; or

15.8.2 where the person is a Sponsor of an Affiliate, the Sponsorship Arrangement is suspended, expires or is terminated.

15.9 Although Sponsors are bound by Privacy Safeguard 5, proposed Rule 7.4(2) will mean that if CDR Data is collected by a Sponsor on behalf of an Affiliate:

15.9.1 the Sponsor and Affiliate may choose which of them will be responsible for updating the CDR Consumer's consumer dashboard; and

15.9.2 the consumer dashboard must also indicate that the CDR Data was collected by a Sponsor on behalf of an Affiliate.

15.10 Proposed Rule 4.20A will mean that if a Sponsor and an Affiliate are both required to provide a notice to a CDR Consumer under Subdivision 4.3.5 (Notification requirements), the Sponsor and the Affiliate may choose who will give the notice.

15.11 Pursuant to proposed Rule 2.2 of Schedule 1:

15.11.1 Accredited Persons that propose to become a Sponsor must:

(a) undertake due diligence to ensure that the proposed Affiliate is a suitable person for that role (proposed Rule 2.2(1)(a));

(b) provide any appropriate assistance or training in technical and compliance matters (proposed Rule 2.2(1)(b)); and

15.11.2 Sponsors must:

(a) continue to provide any appropriate assistance or training in technical and compliance matters; and

(b) take reasonable steps to ensure that their Affiliates comply with their obligations as Accredited Persons.

15.12 Pursuant to proposed amendments to Rule 9.3(2)(i), Sponsors and Affiliates must keep and maintain records that record and explain, amongst other things:

15.12.1 any Sponsorship Arrangement to which the Accredited Data Recipient is a party; and

15.12.2 the use and management by the other party to each such Sponsorship Arrangement of CDR Data collected by it, or provided to it under the Sponsorship Arrangement.

Obligations of Affiliates

15.13 Importantly, Affiliates will be Accredited Persons for the purposes of the CDR regime and will therefore be required to fulfil all obligations of Accredited Persons, unless expressly noted otherwise. In effect, this means that Affiliates will have to comply with a range of obligations, including the dispute resolution obligations, the Privacy Safeguards and the rules regarding consent.

15.14 Affiliates will not be able to engage a provider in an outsourced service arrangement to collect CDR Data from a CDR Participant on their behalf (proposed Rule 5.1B(4)). Additionally, Affiliates will not be able to have a CDR Representative (proposed Rule 5.1B(5)).

15.15 If an Affiliate ceases to have a Sponsor, then for Rule 4.14(1)(f), any collection consents will expire, but any use and disclosure consents continue in effect (proposed Rule 5.1B(6)).

15.16 If an Affiliate has not had a Sponsor for a period of 120 days, the Affiliate's accreditation is taken to have been surrendered (proposed Rule 5.1B(7)).

15.17 Proposed Rule 7.2(4) will require Affiliates to ensure that their CDR policy includes:

15.17.1 a list of Accredited Persons with whom the Affiliate has a Sponsorship Arrangement; and

15.17.2 for each Sponsorship Arrangement, details about the nature of the services one party provides to the other party.

15.18 Pursuant to Rule 2.1(2)(b) of Schedule 1, Affiliates must provide an attestation statement about their compliance with Schedule 2 that is made in accordance with any requirements. This must be provided within three months after the end of the first reporting period, and every second reporting period thereafter. Relevantly, Sponsors must provide a statement in the form of a responsible party's statement on controls and system description that is made in accordance with ASAE 3150.

15.19 Pursuant to Rule 2.1(3)(b) of Schedule 1, Affiliates must provide an assurance report of their capacity to comply with Schedule 2 that is made in accordance with any approved requirements (noting that this does not include the information that must be provided in at attestation statement). This must be provided within three months after the end of the first reporting period, and every second reporting period thereafter. Relevantly, Sponsors must provide a report that is made in accordance with ASAE 3150 or an approved standard, report or framework.

15.20 Pursuant to proposed amendments to Rule 9.3(2)(i), Affiliates must keep and maintain records that record and explain:

15.20.1 arrangements that may result in CDR Data being collected by, or disclosed to, a Sponsor, including copies of Sponsor Arrangements; and

15.20.2 the use and management of CDR Data by those Sponsors.

16. Introduction of disclosure of CDR Data to CDR Representatives

16.1 The proposed amendments to the CDR Rules will, if passed, introduce the concept of a **CDR Representative** and a **CDR Principal**, who will operate under a **CDR Representative Arrangement**. CDR Principals will be accredited at the unrestricted level and CDR Representatives will not be accredited.

16.2 Proposed Rule 1.10A(4) provides that, for a CDR Principal, a consent given by a CDR Consumer under the CDR Rules to the CDR Representative for the CDR Principal to collect particular CDR Data and disclose it to a CDR Representative is a collection consent.

16.3 Relevantly, CDR Consumers will only deal with CDR Representatives as if they were an Accredited Person (i.e. CDR Consumers may not deal directly with CDR Principals). For example:

16.3.1 CDR Consumers will request goods or services from a CDR Representative;

16.3.2 the CDR Representative will identify the CDR Data required to provide the goods and services;

16.3.3 the CDR Consumer will provide their consent to the CDR Representative for the collection and use of the CDR Data.

16.4 If a CDR Consumer asks a CDR Representative to provide goods or services to them (or another person) and the CDR Representative needs to request its CDR Principal to collect the CDR Consumer's CDR Data from a CDR Participant in accordance with the CDR Rules, in order to provide the goods or services, the CDR Representative may, in accordance with Division 4.3 (subject to the modifications noted in proposed Rule 4.3B), ask the CDR Consumer to give:

16.4.1 a collection consent for the CDR Principal to collect their CDR Data from the CDR Participant (proposed Rule 4.3A(2)(a)); and

16.4.2 a use consent for:

(a) the CDR Principal to disclose that CDR Data to the CDR Representative (proposed Rule 4.3A(2)(b)(i)); and

(b) for the CDR Representative to use it in order to provide those goods and services (proposed Rule 4.3A(2)(b)(ii)).

16.5 Additionally, proposed Rule 4.3B(2) will means that if a CDR Representative fails to comply with a provision of Division 3.4 as modified by proposed Rule 4.3B(1), the CDR Principal is taken to breach proposed Rule 4.3B(2), which is a civil penalty provision.

16.6 Importantly, any CDR Data must still only be collected and used in accordance with the data minimisation principle.

16.7 For completeness:

16.7.1 proposed Rule 4.3A(3) provides that in giving the consents, the CDR Consumer gives the CDR Principal a valid request to seek to collect CDR Data from the CDR Participant; and

16.7.2 proposed Rule 4.3A(4) provides that the request ceases to be valid if the relevant collection consent is withdrawn.

16.8 Relevantly, even if a collect consent is withdrawn, if a use consent is not withdrawn, a CDR Principal can continue to disclose CDR Data it has already collected to a CDR Representative, and the CDR Representative can continue to use it to provide the requested goods or services.

CDR Representative Arrangements

16.9 Each CDR Principal must enter into a CDR Representative Arrangement with a CDR Representative. Pursuant to proposed Rule 1.10AA(2), a CDR Representative Arrangement is a written contract between a CDR Principal and a CDR Representative under which:

16.9.1 if the CDR Representative has obtained the consent of a CDR Consumer to the collection and use of CDR Data in accordance with Rule 4.3A:

(a) the CDR Principal will:

(i) make any appropriate consumer data request; and

(ii) disclose the relevant CDR Data to the CDR Representative; and

(b) the CDR Representative will use the CDR Data to provide the relevant goods or services to the CDR Consumer; and

16.9.2 the CDR Representative must not enter into another CDR Representative Arrangement;

16.9.3 the CDR Representative must not engage a person as the provider in an outsourced service arrangement;

16.9.4 the CDR Representative is required to comply with the following requirements in relation to any **Service Data** (being CDR Data that was disclosed to the CDR Representative for the purposes of the CDR Representative Arrangement, or directly or indirectly derives from such CDR Data (proposed Rule 1.10AA(3)).

16.9.5 in holding, using or disclosing the Service Data, the CDR Representative must comply with, as if it were the CDR Principal (e.g. an Accredited Person with accreditation at the unrestricted level):

(i) section 52EE of the CC Act (Privacy Safeguard 2);

(ii) section 52EG of the CC Act (Privacy Safeguard 4);

(iii) section 56EK of the CC Act (Privacy Safeguard 8);

(iv) section 56EI of the CC Act (Privacy Safeguard 9);

(v) section 56EN(2) of the CC Act (Privacy Safeguard 11);

(vi) section 56EO of the CC Act (Privacy Safeguard 12); and

(vii) section 56EP(2) of the CC Act (Privacy Safeguard 13);

16.9.6 the CDR Representative must take the steps in Schedule 2 to protect the Service Data as if it were the CDR Principal;

16.9.7 the CDR Representative must not use or disclose the Service Data other than in accordance with a contract with the CDR Principal;

16.9.8 the CDR Representative must, when so directed by its CDR Principal, do any of the following:

(a) delete any Service Data that it holds in accordance with the CDR Data deletion process; and

(b) provide, to the CDR Principal, records of any deletion that are required to be made under the CDR Data deletion process;

16.9.9 the CDR Representative is required to adopt, and comply with, the CDR Principal's CDR policy in relation to the Service Data; and

16.9.10 the provisions of the CDR Representative Arrangement for the purposes of proposed Rule 1.10AA(2)(a) will not operate unless the details of the CDR Representative have been entered into the Register of Accredited Persons.

16.10 Proposed Rule 1.14(5) provides that if a CDR Principal makes a consumer data request at the request of a CDR Representative, it may arrange for the CDR Representative to provide the consumer dashboard on its behalf.

Obligations of CDR Principals

16.11 Proposed Rule 1.16(1) will require CDR Principals to ensure that their CDR Representatives comply with any requirements that they have under a CDR Representative Arrangement (noting that if a CDR Representative fails to comply with a required provision of the CDR Representative Arrangement, the CDR Principal will breach propose Rule 1.16A, which is a civil penalty provision).

16.12 Proposed Rule 5.14(3) will require a CDR Principal that enters into a CDR Representative Arrangement to notify the Data Recipient Accreditor that they have entered into the arrangement. This must be done as soon as practicable, but no later than 5 business days after entering into the arrangement. Pursuant to proposed Rule 5.14(4), this notification must include:

16.12.1 the date the CDR Representative Arrangement was entered into;

16.12.2 the name, address and ABN (or, if a foreign entity, another unique business identifier) of the CDR Representative;

16.12.3 the names and contact details of the directors or any persons responsible for the CDR Representative;

16.12.4 the nature of any goods and services to be provided by the CDR Representative using CDR Data; and

16.12.5 any information otherwise specified in writing by the Data Recipient Accreditor as necessary for the purposes of evaluating the CDR Representative.

16.13 Importantly, proposed Rule 5.14(5) will require a CDR Principal to notify the Data Recipient Accreditor if the CDR Representative Arrangement terminates or otherwise ends as soon as practicable, but no later than 5 business days after the event.

16.14 Proposed Rule 7.2(4)(d) will require a CDR Principal to ensure that their CDR policy contains a list of their CDR Representatives.

16.15 Finally, if a CDR Representative fails to comply with:

16.15.1 section 56EE of the CC Act (Privacy Safeguard 2) in relation to Service Data of a CDR Consumer as if it were an Accredited Person, its CDR Principal will have been taken to breach proposed Rule 7.3(2);

16.15.2 section 56EG of the CC Act (Privacy Safeguard 4) in relation to Service Data of a CDR Consumer as if it were an Accredited Person and had collected the Service Data, their CDR Principal will have been taken to breach proposed Rule 7.3A(1));

16.15.3 section 56EK of the CC Act (Privacy Safeguard 8) in relation to Service Data of a CDR Consumer as if it were an Accredited Data Recipient of the Service Data, the CDR Principal will breach proposed Rule 7.8A(1);

16.15.4 section 56EL of the CC Act (Privacy Safeguard 9) in relation to Service Data of a CDR Consumer as if it were an Accredited Data Recipient, the CDR Principal will breach proposed Rule 7.8A(2);

16.15.5 section 56EN(2) (Privacy Safeguard 11) of the CC Act in relation to Service Data of a CDR Consumer as if it were an Accredited Person, the CDR Principal will be taken to have breached proposed Rule 7.10A(1) (regardless of whether the action of the CDR Representative in relation to the Service Data is in accordance with the CDR Representative Arrangement);

16.15.6 section 56EO(2) of the CC Act (Privacy Safeguard 12) in relation to Service Data as if it were a CDR entity, the failure is taken to be a failure by the CDR Principal by virtue of proposed Rule 7.12(3); and

16.15.7 section 56EP(2) of the CC Act (Privacy Safeguard 13) in relation to Service Data of a CDR Consumer as if it were an Accredited Person, their CDR Principal will be taken to have breached proposed Rule 7.16(1)) (regardless of whether the action of the CDR Representative in relation to the service data is in accordance with the CDR Representative Arrangement); and

16.15.8 Schedule 2 in relation to Service Data, will be taken to be a failure by the CDR Principal.

16.16 Proposed Rule 7.6(5) will mean that, for the purposes of Rule 7.6, any use or disclosure of service data by a CDR Representative is taken to have been by the CDR Principal (regardless of whether the use or disclosure was in accordance with the CDR Representative Arrangement).

16.17 Proposed Rule 7.9(5) will mean that, for the purposes of Rule 7.9, if an Accredited Data Recipient is a CDR Principal, a disclosure of Service Data by a CDR Representative is taken to be a disclosure by the CDR Principal.

16.18 Proposed Rule 9.3(2A) will require CDR Principals to keep and maintain records that record and explain the following in relation to each CDR Representative:

16.18.1 the management of data by the CDR Representative;

16.18.2 steps taken to ensure that the CDR Representative complies with their requirements under the CDR Representative Arrangement;

16.18.3 all consents obtained by the CDR Representative, including, if applicable, the uses of the CDR Data that the CDR Consumer has consented to under any use consents;

16.18.4 amendments to or withdrawals of consents by CDR Consumers;

16.18.5 notifications of withdrawals of authorisations received from Data Holders;

16.18.6 CDR complaint data;

16.18.7 collections of CDR Data under the CDR Rules;

16.18.8 elections to delete and withdrawals of those elections;

16.18.9 the use of CDR Data by the CDR Representative;

16.18.10 the processes by which the CDR Representative asks CDR Consumers for their consent and for an amendment to their consent, including a video of each process;

16.18.11 if CDR Data was de-identified in accordance with a consent referred to in Rule 4.11(3)(e), the additional information in Rule 4.15 including:

(a) how the CDR Data was de-identified; and

(b) how the CDR Representative used the de-identified data; and

(c) if the CDR Representative disclosed (by sale or otherwise) the de-identified data to another person as referred to in Rule 4.15(b):

(i) to whom the data was so disclosed; and

(ii) why the data was so disclosed.

16.18.12 if the use is for general research, records of any additional benefit to be provided to the CDR Consumer for consenting to the use;

16.18.13 records that are required to be made for the purposes of the CDR Data de-identification process when applied as part of Privacy Safeguard 12;

16.18.14 records of any matters that are required to be retained under Schedule 2 to the CDR Rules;

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

SECTION 2: JOINT ACCOUNT CHANGES

17. Proposed changes to joint accounts

17.1 If the proposed amendments to the CDR Rules are made, there will be fundamental changes to how joints accounts are treated, and the joint account provisions in the CDR Rules will apply to all Sectors (rather than applying solely to the banking Sector), unless amended by a Sector-specific Schedule to the CDR Rules.

Types of disclosure options

17.2 Proposed Rule 4A.5(1) provides that disclosure of CDR Data relating to a joint account may only be authorised in accordance with one of the following disclosure options:

17.2.1 the pre-approval option – if this option is implemented, CDR Data relating to a joint account may be disclosed in response to a valid Consumer Data Request by one JAH on the authority of that JAH and without the approval of other JAHs (proposed Rule 4A.5(1)(a));

17.2.2 the co-approval option – if this option is implemented, CDR Data relating to a joint account may only be disclosed in response to a valid Consumer Data Request if:

(a) JAH A has authorised the disclosure (proposed Rule 4A.5(1)(b)(i)); and

(b) each JAH B has also approved the disclosure (proposed Rule 4A.5(1)(b)(ii); and

17.2.3 the non-disclosure option – if this option is implemented, CDR Data relating to a joint account may not be shared in response to a valid Consumer Data Request by a JAH (proposed Rule 4A.5(1)(c)).

17.3 Relevantly:

17.3.1 Data Holders must provide the pre-approval and non-disclosure options for a joint account (proposed Rule 4A.5(2)); and

17.3.2 Data Holders may provide the co-approval option for a joint account (proposed Rule 4A.5(3)).

Default disclosure option

17.4 Proposed Rule 4A.5(5) will mean that, unless a Sector-specific Schedule to the CDR Rules provides otherwise, the pre-approval option will apply to all joint accounts by default. However, JAHs will be able to change their disclosure option in accordance with proposed Rule 4A.7 or 4A.8.

Disclosure option management system

17.5 Data Holders will be required to provide a disclosure option management system (**DOMS**). DOMS will allow JAHs to:

17.5.1 change the disclosure option that applies to a joint account, in accordance with proposed Rule 4A.7 (proposed Rule 4A.6(1)(a));

17.5.2 propose a change in the disclosure option to the other JAHs, in accordance with proposed Rule 4A.8 (proposed Rule 4A.6(1)(b)); and

17.5.3 respond to a proposal by another JAH to change the disclosure option (proposed Rule 4A.6(1)(c));

17.6 Additionally, amongst other things, proposed Rule 4A.6(7) will require DOMS to indicate to JAHs what disclosure option currently applies to their joint account.

17.7 At any time, a JAH may select a different disclosure option using DOMS. However, there are different rules depending on whether a JAH selects a more restrictive non-disclosure option.

17.8 If a JAH A selects the non-disclosure option through DOMS, or the pre-approval option applies to a joint account and the JAH A chooses to have the co-approval option apply, the Data Holder must, through its ordinary means for contacting any JAH B:

17.8.1 explain to JAH B what the Consumer Data Right is (proposed Rule 4A.7(3)(a));

17.8.2 inform them which disclosure option previously applied to the joint account (proposed Rule 4A.7(3)(b));

17.8.3 inform them that JAH A has changed the disclosure option, and of the disclosure option that now applies (proposed Rule 4A.7(3)(c)); and

17.8.4 explain to JAH B the mechanisms for changing the disclosure option again (proposed Rule 4A.7(3)(d)).

17.9 If the non-disclosure option or co-approval option applies to an account and JAH A proposes to change the option, the Data Holder will have to, as soon as practicable and through its ordinary methods for contacting any JAH B:

17.9.1 explain to JAH B what the Consumer Data Right is (proposed Rule 4A.8(2)(a));

17.9.2 inform JAH B which disclosure option currently applies to the account (proposed Rule 4A.8(2)(b));

17.9.3 inform them that JAH A has proposed that the co-approval or pre-approval option apply to the joint account (proposed Rule 4A.8(2)(c));

17.9.4 explain to JAH B that this change requires the agreement of all JAHs (proposed Rule 4A.8(2)(d));

17.9.5 explain to JAH B any alternative options for change that are available and how they can be made (proposed Rule 4A.8(2)(e)); and

17.9.6 invite JAH B to either agree to, or reject, the proposal within a specified period of time (proposed Rule 4A.8(2)(f)).

17.10 Proposed Rule 4A.8(3) will require the Data Holder to, at the end of the period specified in accordance with proposed Rule 4A.8(2)(f), inform the JAHs (as soon as practicable) whether:

17.10.1 all JAHs have approved the change, and as a result the new disclosure option applies to the joint account; or

17.10.2 not all the JAHs have approved the change, and as a result the disclosure option is unchanged.

Managing consumer data requests

17.11 If a Data Holder receives a Consumer Data Request, the Data Holder must:

17.11.1 if the pre-approval disclosure option applies to the joint account, comply with Rules 4.5 to 4.7 (proposed Rule 4A.10(2));

17.11.2 if the co-approval option applies to the joint account:

(a) ask JAH A for authorisation in accordance with Rule 4.5 and Division 4.4 (proposed Rule 4A.10(4)(a));

(b) if the authorisation is given, invite the approval of any JAH B in accordance with proposed Rule 4A.11 (proposed Rule 4A.10(4)(b)); and

(c) if all JAH Bs give their approval, comply with Rules 4.6 and 4.7 (proposed Rule 4A.10(4)(c)); and

17.11.3 if the non-disclosure option applies, refuse to disclose the requested CDR Data (proposed Rule 4A.10(6)).

17.12 If a Data Holder is required to invite the approval of JAH B, the Data Holder must, through its ordinary methods for contacting each JAH B:

17.12.1 indicate that an Accredited Person has requested disclosure of CDR Data about a joint account on behalf of JAH A (proposed Rule 4A.11(a));

17.12.2 indicate that:

(a) JAH A has authorised the disclosure of the data about the joint account in accordance with Division 4.4 (proposed Rule 4A.11(b)(i)); and

(b) a co-approval option applies to the joint account (proposed Rule 4A.11(b)(ii));

17.12.3 indicate the matters referred to in Rule 4.23(1)(a) to (e) so far as they relate to the request (proposed Rule 4A.11(c));

17.12.4 ask the JAH B to approve or not approve disclosure of the CDR Data about the joint account (proposed Rule 4A.11(d));

17.12.5 specify the time by which the Data Holder needs to receive any approval, and notify the JAH B that if an approval is not received within the specified time, the joint account CDR Data will not be disclosed (proposed Rule 4A.11(e));

17.12.6 inform JAH B that any JAH may, at any time, withdraw the approval using their consumer dashboard (proposed Rule 4A.11(f)); and

17.12.7 indicate what the effect of removing the approval would be (proposed Rule 4A.11(g)).

Consumer dashboards

17.13 A Data Holder must provide each JAH with a consumer dashboard if Division 4A.3 applies in relation to a Consumer Data Request and either the co-approval option or the pre-approval option applies, or has applied, to the joint account (proposed Rule 4A.13(1)). This consumer dashboard must:

17.13.1 contain the details referred to in Rule 1.15(1)(b) that relate to CDR Data about a joint account (proposed Rule 4A.13(1)(c));

17.13.2 have a functionality that:

(a) can be used by the JAH to manage approvals in relation to each authorisation to disclose CDR Data about a joint account made by a JAH A (proposed Rule 4A.13(1)(d)(i));

(b) allows for withdrawal of such an approval, at any time (proposed Rule 4A.13(1)(d)(ii));

(c) is simple and straightforward to use (proposed Rule 4A.13(1)(d)(iii));

(d) is prominently displayed (proposed Rule 4A.13(1)(d)(iv)); and

(e) as part of the withdrawal process, displays a message relating to the consequences of the withdrawal in accordance with the Data Standards (proposed Rule 4A.13(1)(d)(v)).

Notifications to JAHs

17.14 A Data Holder must give, in accordance with the Data Standards and through its ordinary means of contacting JAHs:

17.14.1 JAH As a notification if:

(a) one or more JAH Bs have not given their approval for disclosure within the specified timeframe; or

(b) a JAH B has withdrawn an approval previously given; and

17.14.2 JAH Bs a notification if a JAH A has given, amended or withdrawn an authorisation, or that the authorisation has expired.

17.15 Data Holders must provide these notifications to JAHs as soon as practicable after an event specified in paragraph 17.14 above occurs, unless the JAH has selected an alternative schedule of notifications.

17.16 Proposed Rule 4A.13(3) will require Data Holders to, in accordance with any Data Standards:

17.16.1 provide for alternative notification schedules (including reducing the frequency of notifications or not receiving notifications); and

17.16.2 give each JAH a means of selecting such an alternative, and of changing a selection.

Protections for JAHs

17.17 Proposed Rule 4A.15 will mean that a Data Holder is not liable under the CDR Rules for a failure to comply with Part 4a (joint accounts) if it considered that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse to any person.

Part E ANALYSIS OF RISKS

SECTION 1: ACCESS CHANGES

18. Introduction

18.1 This **Section 1** of **Part E [Analysis of Risks]** contains our analysis of the risks that we have identified as a result of the proposed amendments to the CDR Rules in relation to the Access Changes.

18.2 For convenience, we have grouped the proposed amendments to the CDR Rules into the following concepts, which may involve new or changed privacy considerations in addition to those identified in the Original CDR PIA report and previous PIA Update reports:

18.2.1 the disclosure of CDR Data to Trusted Advisers;

18.2.2 the disclosure of CDR Insights to non-accredited persons;

18.2.3 the introduction of a sponsored level of accreditation; and

18.2.4 the introduction of non-accredited CDR Representatives.

18.3 We have described and considered the high-level privacy risks associated with these information flows and concepts in the tables below. 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.

19. General risks

19.1 As raised in previous PIA Update reports, the proposed amendments will significantly add to the already complex legislative framework underpinning the CDR regime. The proposed amendments will introduce a number of new definitions, concepts, and information flows, all at the same time.

19.2 The very complexity itself raises privacy risks associated for entities participating in the CDR regime (such as Data Holders, Accredited Persons and Accredited Data Recipients) and CDR Consumers. This has been discussed in previous PIA Update reports, including because entities may not understand, or take steps to action, their obligations or rights under the legislative framework.

19.3 We therefore **recommend** that Treasury work with the regulators to ensure that detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules is issued, or previously issued guidance amended, in order to explain the proposed changes. We suggest that different forms of guidance could be developed and specifically tailored to assist:

19.3.1 CDR Consumers;

19.3.2 Data Holders;

19.3.3 Accredited Persons at both the unrestricted level and the sponsored level; and

19.3.4 persons receiving CDR Data who are outside of the CDR regime (including CDR Representatives, Trusted Advisers and recipients of CDR Insights).

20. Risks associated with the disclosure of CDR Data to Trusted Advisers

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**CDR Data is disclosed outside of CDR regime** The proposed amendments will result in CDR Data being disclosed outside of the CDR regime, where the data will have fewer privacy protections (or potentially no privacy protections if the recipient is not an APP entity for the purposes of the Privacy Act) than the same data will have when being held by an entity within the CDR regime. In addition, CDR Consumers may not have a right of recourse if their CDR Data is misused after it is disclosed to the Trusted Adviser, or if their CDR Data is involved in a data breach.	Under proposed Rule 1.10C(2), a Trusted Adviser must belong to one of the following classes: • qualified accountants within the meaning of the Corporations Act; • persons who are admitted to the legal profession (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession; • registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009* (Cth); • financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*; • relevant providers within the meaning of the Corporations	We note that the proposed amendments will allow the disclosure of CDR Data to recipients who are not Data Holders or Accredited Persons (and therefore 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 may be a small business who is not an APP entity and therefore has no obligation to comply with the requirements of the Privacy Act). This concern about the disclosure of CDR Data outside the CDR regime was also raised by a number of stakeholders. For example, the Australian Banking Association has stated that *'the Trusted Adviser arrangement poses significant risk to consumer banking data and should not proceed. Within seconds, under* [the proposed amendments to the Rules], *a customer's data will travel from the most secure setting at the bank to no or uncertain security with the Trusted Adviser'.* Additionally, the OAIC has suggested that the '*draft Rules be amended to ensure CDR data may only be provided to a trusted adviser outside the CDR system where that trusted adviser is subject to the Privacy Act.'* However, a number of stakeholders did note that they consider it appropriate to enable CDR Data to be disclosed to Trusted Advisers. For example, VISA has stated: *'We agree with Treasury that consumers should have the choice to share their CDR data with regulated parties outside the CDR system, pursuant to commercial terms that*

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		Act, other than provisional relevant providers and limited-service time-sharing advisers under section 910A of the Corporations Act; and • mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009* (Cth). Each class of Trusted Advisers included in these proposed amendments to the CDR Rules is subject to existing fiduciary or regulatory obligations. Additionally, a person is only taken to be a member of a class for the purposes of proposed Rule 1.10C if the Accredited Data Recipient has taken reasonable steps to confirm that a person nominated as a trusted adviser was, and remains, a member of a class mentioned in proposed Rule 1.10C(2). Under the CDR Rules, the CDR Consumer must provide consent (which must comply with the requirements for the provision of consent under the CDR regime) for the	*address important issues like data security, safety, and consumer preference. Ultimately, a more inclusive environment will encourage more innovators to participate in Australia's data ecosystem, making it both more competitive and responsive to consumer and business needs.'* Additionally, a number of stakeholders suggested that the classes of entities who can be Trusted Advisers should be broadened. We do note that the limitation of the classes of entities who can be Trusted Advisers, where those classes will have fiduciary or regulatory obligations, does somewhat mitigate this risk. However, as was pointed out to us during stakeholder consultations, those obligations can offer less protection for CDR Consumers than the strong privacy protections imposed under the CDR regime, or under the Privacy Act. ***Recommendation**: We recommend that Treasury consider:* • *only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who are APP entities for the purposes of the Privacy Act;* • *if the above is not possible or practical (e.g. it would defeat the policy objective by excluding many small businesses who are Trusted Advisers (and not Accredited Data Recipients) from receiving the CDR Data), only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who have agreed (through a contractual arrangement with the Accredited Data Recipient) to effectively comply with the requirements of APP 1, APP 6 and APP 11, and the Notifiable Data Breach scheme; or*

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		disclosure of their CDR Data to a Trusted Adviser. Finally, under proposed Rule 1.10C(4), an Accredited Person must not make any of the following a condition for the supply of the goods and services requested by the CDR Consumer: • the nomination of a Trusted Adviser; • the nomination of a particular person as a Trusted Adviser; or • the giving of a TA disclosure consent.	• *if the above is not possible or practical, requiring the Accredited Data Recipient to tell the Trusted Adviser of the scope of the CDR Consumer's consent, and to remind the recipient (i.e. the Trusted Adviser) of their fiduciary or regulatory obligations in relation to the CDR Consumer.* *Additionally, we recommend that Treasury consider undertaking an analysis of whether each of the proposed classes of Trusted Adviser will be at least subject to obligations that will require the recipient to use CDR Data that it receives consistently with the consents provided by the CDR Consumer (e.g. if they would be required to do so as part of ethical obligations).* We note that our proposed strategies described in relation to Risk 3 below would also assist in mitigating the risk by further ensuring that CDR Consumers understand the reduction in privacy protections once their CDR Data is disclosed to the Trusted Adviser, before they provide their consent.
2.	**Trusted Adviser discloses CDR Data to other entities** There is a risk that once CDR Data is disclosed to a Trusted Adviser, there will be no restriction on the Trusted Adviser to not further disclose CDR Data to other individuals or entities that are not subject to the CDR regime, and in particular who may	See above.	Implementing the recommendations described in relation to Risk 1 and Risk 3 would also assist in mitigating this risk.

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	not fall within the prescribed classes for Trusted Advisers.		
3.	**CDR Consumers do not understand what they are consenting to** The proposed amendments will mean that it may make it difficult for CDR Consumers to understand the implications of consenting to disclosure of CDR Data to a recipient outside of the CDR regime (including that Trusted Advisers do not need to comply with the security, accreditation and governance processes prescribed by the CDR regime). These implications also include that their information, once disclosed, will not be afforded the protections offered by the CDR Rules, including the Privacy Safeguards, and may not also be subject to other privacy protections (such as under the Privacy Act).	Rule 4.10(1) 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; and • 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).	Given the importance of CDR Consumers understanding this risk, it is key that CDR Consumers are presented with the appropriate amount of information about the fact that once CDR Data is disclosed to the Trusted Adviser, it will not be afforded the protections of the CDR regime (and potentially, the Privacy Act). This need for information will need to be balanced against the risk of CDR Consumers experiencing "information overload", meaning they do not give an Accredited Person properly informed consent. ***Recommendation**: We recommend that Treasury consider whether it would be appropriate to continue, in consultation with the Data Standards Body, to conduct consumer research on what is the best way to present a CDR Consumer with information on the implications of providing a disclosure consent, permitting the disclosure of their CDR Data to Trusted Advisers (and therefore outside of the CDR regime), 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.* *We suggest this could be achieved by expanding proposed Rule 8.11(1A) to require the Data Standards to include provisions that cover ensuring that CDR Consumers are made aware that if they provide a TA disclosure consent, their CDR Data will leave the CDR system.*

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			We also recommend that Treasury consider whether the CDR Rules should allow the Data Standards to specify different standards for obtaining consent to disclose CDR Data to Trusted Advisers, depending on whether: • *the CDR Consumer is an individual or sole trader and consenting to disclosure of their CDR Data; and* • *the CDR Consumer is a company or other business and is consenting to disclosure of CDR Data about their business.*
4.	**Risk relating to the transfer of CDR Data to Trusted Advisers** In transferring CDR Data to a Trusted Adviser, an Accredited Person does not need to comply with the CDR Rules or Data Standards. This may increase the risks of loss or unauthorised access and disclosure during that transfer.	Accredited Data Recipients are required to comply with the requirements of Schedule 2 to the CDR Rules, which specify minimum security requirements related to CDR Data held by Accredited Data Recipients.	Schedule 2 requirements for "encryption in transit" only apply to networks and systems "within the CDR data environment". We consider there is a risk that Accredited Data Recipients will not understand the intention that they must ensure that all CDR Data is encrypted in accordance with Schedule 2 to the CDR Rules, from the time the CDR Data leaves the Accredited Data Recipient's CDR data environment, until it reaches the recipient's system. This is because it appears that Accredited Data Recipients can define the boundaries of their CDR data environments (e.g. an Accredited Data Recipient can determine that once CDR Data has left its systems, it is outside the CDR Data environment). This raises the risk that there may be more scope for unauthorised access or disclosure of the CDR Data during transfer. Some stakeholders (e.g. the Australian Banking Association) also raised this risk. Proposed Rule 7.5(2)(a) will mean that permitted uses or disclosures must be done in accordance with the Data Standards. The Data Standards could therefore include mechanisms that

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			ensure CDR Data is appropriately protected during transit to Trusted Advisers. ***Recommendation**: We recommend that Treasury consider whether it is appropriate to amend the Data Standards, and/or ensure that appropriate guidance is provided, so that it is clear that all CDR Data (including CDR Insights) must be appropriately encrypted in accordance with Schedule 2 to the CDR Rules, from the time the data leaves the Accredited Data Recipient's CDR data environment until it reaches the recipient's IT environment.*
5.	**CDR Consumer does not remember details of their disclosure consent** There is a potential risk that the CDR Consumer may not remember details relating to the consent they provided to the Accredited Data Recipient in relation to the disclosure of their CDR Data to a Trusted Adviser.	Rule 1.14(3) requires an Accredited Person to include details on their Consumer Dashboard relating to the disclosure consent (including information about the CDR Data to which the consent relates and the period of the consent). Under Rule 4.18, the CDR Consumer will also receive a CDR receipt, which includes details about the name of the person to whom the CDR Consumer has consented to the disclosure of CDR Data. Proposed Rule 7.9(3) requires the Accredited Person to update their Consumer Dashboard as soon as practicable after it discloses CDR Data to a Trusted Adviser to indicate what CDR Data was disclosed, when it was	We are satisfied that the draft CDR Rules have appropriately mitigated this risk and that no further action is required.

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		disclosed and to whom it was disclosed. Proposed amendments to Rule 1.14(1)(b) and proposed Rule 1.14(3A) also require an Accredited Person's Consumer Dashboard to contain information about how a CDR Consumer can request records (in accordance with Rule 9.5).	
6.	**Accredited Data Recipient discloses CDR Data to an entity that does not fall within a class of Trusted Advisers**	Proposed amendments to Rule 7.5a provides that the Accredited Data Recipient is only permitted to disclose CDR Data to a Trusted Adviser under a disclosure consent: • on the earlier of 1 February 2022 or when the Data Standards Chair makes consumer experience Data Standards for disclosure of CDR Data to Trusted Advisers; and • the Accredited Data Recipient has taken reasonable steps to ensure the Trusted Adviser was, and remains, a member of a class mentioned in proposed Rule 1.10C(2) (as	Given the reliance on Trusted Advisers being subject to separate fiduciary and regulatory obligations to protect CDR Data after it is disclosed by the Accredited Data Recipient, it is critical that the CDR Data is in fact disclosed to an entity that falls within a class of Trusted Advisers specified in proposed Rule 1.10C(2). A number of stakeholders (e.g. the Australian Energy Council and SISS Data) have suggested that further guidance needs to be provided about what constitutes 'reasonable steps' by an Accredited Data Recipient to ensure that an entity falls within a class of Trusted Advisers specified in proposed Rule 1.10C(2). Additionally: • SISS Data has suggested that there should be a 'Trusted Adviser register' that is updated daily – noting that the intention is that Accredited Data Recipients could use this register as a 'source of truth' to determine whether an entity falls within a specified class; • Red Energy and Lumo have suggested that *'the obligation on data recipient should be strengthened to require them to*

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		specified in proposed Rule 1.10C(3)). In addition, under proposed Rule 9.3(2)(ec), the Accredited Data Recipient must keep and maintain records that record the steps it has taken to confirm that a Trusted Adviser is a member of a class of Trusted Advisers (as specified in Rule 7.5A(3)).	*determine whether a trusted adviser is in the prescribed class, rather than just take reasonable steps'.* We assume that creating and maintaining a centralised 'Trusted Adviser register' with all persons who fall within a class of Trusted Advisers is likely to involve considerable time and resources. However, we believe that it would increase certainty for CDR Consumers, if Accredited Data Recipients are required to have a level of certainty that a particular person or entity does in fact will within a class of Trusted Advisers (e.g. where the class is regulated and a public register available, to actively take active steps to determine that the relevant person or entity is listed on that register). ***Recommendation:*** *We recommend that further guidance be provided about what constitutes 'reasonable steps' that an Accredited Data Recipient is required to take. For example, we suggest that it might be best practice for the CDR Rules, or the Data Standards, to require the Accredited Data Recipient to:* • *obtain evidence that the Trusted Adviser falls within a class specified in proposed Rule 1.10C(2); or* • *check a public register for the relevant class of Trusted Adviser.*
7.	**Trusted Adviser may have been banned or disqualified, or be subject to an enforceable undertaking**	Accredited Data Recipient must have taken reasonable steps to ensure that a Trusted Adviser remains a member of a class mentioned in proposed Rule 1.10C(2).	There is a risk that a Trusted Adviser: • may be banned or disqualified, or subject to an enforceable undertaking, so that the Trusted Adviser may no longer be in a class specified by proposed Rule 1.10C(2); or

DISCLOSURE OF CDR DATA TO TRUSTED ADVISERS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• may no longer be a suitable person to whom to disclose CDR Data. ***Recommendation:*** *We recommend that Treasury confirm that proposed Rule 1.10C(2) will not have the unintended effect of allowing persons who have been banned or disqualified by their profession, or who are subject to an enforceable undertaking, being included in a class of Trusted Adviser.*

21. Risks associated with disclosure of CDR Insights to non-accredited persons

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
8.	**Uncertainty of the proposed amendments**		As discussed in paragraph 19 of this **Part E [Analysis of Risks]** above, we are concerned that entities involved with the CDR regime (including Accredited Data Recipients, CDR Consumers and recipients of CDR Insights) may not understand and therefore, appreciate, their obligations in relation to CDR Insights. For example: • in our view, it is difficult to apply the definition of CDR Insight to obtain a clear understanding of what is, and what is not, captured by the definition; and • it is important that relevant entities (and CDR Consumers) understand who is responsible for determining that the proposed use of a CDR Insight will fall within one of the limited purposes described in proposed Rule 1.10A(3), and any consequences (or lack of consequences) if the actual use of this CDR Insight does not fall within the limited purposes. This risk has been raised by stakeholders. For example, Illion has noted: *'We are also concerned about the lack of clarity on the nature and extent of the data that can be disclosed as a CDR insight. The examples given in the Explanatory Memorandum refer to low risk data and other insights which are yes/no flags. The definition in the legislation is somewhat circular and relies on consumer consent, if the insight is explained and the consumer consents then the*

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			data that is explained to them may leave the CDR system as a consented disclosure. *Section 1.10A limits the purposes for which consent can be given - identity verification, account balance verification, income verification and expense verification, but does not limit the data that forms the insight. Once the consumer consents, the insight leaves the CDR regime. The standards around that data are yet to be set – see sections 7.5A and 8.11A. This creates uncertainty as there are no clear and current guidelines to align to the Explanatory Memorandum description of "low risk". Without sufficient clarity, the CDR insights could be misused, eroding consumer trust and confidence in the integrity of the CDR system.'* We note that where an insight disclosure consent is sought in relation to CDR Data that relates to more than one transactions, that consent cannot authorise the disclosure of an amount or date for any individual transaction (proposed Rule 1.10A(3)(b)) (however, this will not prevent the disclosure of an amount or date for a single transaction). ***Recommendation**: We recommend that Treasury consider whether it is appropriate for the CDR Rules to be further developed and refined for further clarity, and/or that Treasury work with the regulators of the CDR regime to ensure that further detailed guidance is issued before the proposed amendments to the CDR Rules are introduced.*

9.	**CDR Insights are disclosed outside of CDR regime** The proposed amendments will result in CDR Insights being disclosed outside of the CDR regime, where the data will have fewer privacy protections (or potentially no privacy protections if the recipient is not an APP entity for the purposes of the Privacy Act) than the same data will have when being held by an entity within the CDR regime. In addition, CDR Consumers may not have a right of recourse if their information in the CDR Insights is misused after it is disclosed to the recipient, or if their CDR Insights are involved in a data breach.	Under the CDR Rules, the CDR Consumer must provide consent (which must comply with the requirements for the provision of consent under the CDR regime) for the disclosure of the CDR Insight. Proposed Rule 4.11(3)(ca) requires a CDR Consumer to be provided with an explanation of the CDR Insight that will make clear to the CDR Consumer what the CDR Insight would reveal or describe. Under proposed Rule 8.11(1A), the Data Standards Chair must make Data Standards to: • cover how the Accredited Person can meet the requirement to explain a CDR Insight in accordance with proposed Rule 4.11(3)(ca); and • ensure that the CDR Consumer is made aware that their CDR Data will leave the CDR system when it is disclosed. In addition, under proposed Rule 8.11(1)(c)(v), the Data Standards Chair must make consumer experience Data Standards for disclosure of CDR Insights. These Data Standards must include provisions to ensure that CDR Consumers are made aware that their data will leave the CDR system when it is disclosed.	We note that the proposed amendments will allow the disclosure of 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 may be a small business who is not an APP entity and therefore has no obligation to comply with the requirements of the Privacy Act). For example, the OAIC has recommended: *'That ADRs are prohibited from disclosing CDR insights to entities not covered by the Privacy Act. Further, that Treasury considers whether there are other types of entities to which ADRs must not disclose CDR insights to under the draft Rules.'* ***Recommendation**: We recommend that Treasury consider implementing similar mitigation strategies in relation to CDR Insights as set out in Risk 1 (in relation to disclosure of CDR Data to Trusted Advisers). In other words, we recommend that Treasury consider:* • *only allowing CDR Insights to be disclosed outside of the CDR regime to recipients who are APP entities for the purposes of the Privacy Act; or* • *if the above is not possible or practical, only allowing CDR Insights to be disclosed outside of the CDR regime to recipients who have agreed (through a contractual arrangement with the Accredited Data Recipient) to effectively comply with the requirements of APP 1, APP 6 and APP 11, and the Notifiable Data Breach scheme.* We support the proposed amendments requiring a CDR Consumer being made aware *that* their CDR Data will leave the CDR system when it is disclosed. We also support that consumer experience Data Standards must be made, and that these Data Standards must include provisions that will ensure that CDR Consumers are made

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		Proposed Rule 7.5A(4) provides that the Accredited Data Recipient is only permitted to disclose a CDR Insight under an insight disclosure consent if the CDR Insight does not include or reveal sensitive information (as defined in the Privacy Act). CDR Insights may only be disclosed for a limited number of purposes (Rule 1.10A(3)).	aware that their data will leave the CDR system when it is disclosed. Despite this, we consider there is a risk that CDR Consumers will not understand the *implications* of their CDR Data leaving the CDR system. ***Recommendation:*** *We recommend that Treasury consider amending the proposed CDR Rules to specify that Data Standards must be made to ensure that the CDR Consumer is made aware of the implications and consequences of their CDR Data leaving the CDR system (such as that their data will be afforded fewer privacy protections), in addition to being made aware of the simple fact that the CDR Data will leave the CDR system.* We appreciate that entities who are likely to receive CDR Insights may currently be obtaining personal information from CDR Consumers in order to create insights about the CDR Consumer (e.g. requiring the provision of payslips or bank statements to verify income). This current practice effectively means that recipients are already collecting personal information in circumstances where CDR Consumers may not have any privacy protections (e.g. the recipient is not an APP entity), and where the recipient receives more personal information than is required to provide the good or service to the CDR Consumer. We note that the proposed amendments to the CDR Rules would restrict the amount of personal information about a CDR Consumer being provided to the recipient.

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
10.	**Recipient of CDR Insights discloses this information to other entities** There is a risk that once CDR Insights are disclosed to a recipient, there will be no restriction on the recipient further disclosing the CDR Insights to further entities that are not subject to the CDR regime, and who may not have any obligations under the Privacy Act.		If Accredited Data Recipients were required to enter into a contractual arrangement with recipients of CDR Insights (see Risk 9 above), this could require the recipient to agree not to disclose CDR Insights it receives from the Accredited Data Recipient to another entity, without the consent of the CDR Consumer (this may need to be subject to suitable exceptions, e.g. the recipient was otherwise required or authorised by law to disclose it). *See recommendations in relation to Risk 9.*
11.	**CDR Consumers do not understand what they are consenting to** The proposed amendments involve the risk that it may be difficult for CDR Consumers (including vulnerable CDR Consumers) to understand the implications of consenting to disclosure of their CDR Insights to a recipient outside of the CDR regime. This raises a risk that a disclosure consent provided by CDR Consumers (especially	As specified in Risk 9 above, when asking a CDR Consumer for a consent to disclose their CDR Insights, the Accredited Person must, under proposed Rule 4.11(3)(ca), provide a CDR Consumer with an explanation of the CDR Insight that will make clear to the CDR Consumer what the CDR Insight would reveal or describe (and this must meet the Data Standards, as also specified in Risk 9). Proposed Rule 7.5A(3) provides that the Accredited Data Recipient is only	We support the proposed amendments to the CDR Rules which require CDR Consumers to be provided with information relating to their CDR Insights before they provide their insight disclosure consent, and the limiting of CDR Insights to information that does include sensitive information (as defined in the Privacy Act). The Consumer Policy Research Centre has suggested this these risks could also be mitigated, to a degree, by ensuring that the CDR Consumer is provided with a copy of the proposed CDR Insight *before* consenting to the disclosure of the CDR Insight. *'In particular, the rules focus on providing only a description of the CDR insight to the consumer and do not require the insight to be shown to the consumer prior to disclosure. It inherently expects the consumer to give*

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	vulnerable CDR Consumers) may not be free nor fully-informed. These implications also include that their information, once disclosed, will not be afforded the protections offered by the CDR Rules, including the Privacy Safeguards, and may not also be subject to other privacy protections (such as under the Privacy Act). The ability to provide on-going consent may raise the risk of CDR Insights being used by the recipient over time to draw further insights about the CDR Consumer, where the CDR Consumer may not be aware of this and will have no control over the use of those further insights.	permitted to disclose a CDR Insight under an insight disclosure consent: • on the earlier of 1 February 2022 or when the Data Standards Chair makes consumer experience Data Standards for disclosure of CDR Insights; and • if the CDR Insight does not include or reveal sensitive information (as defined in the Privacy Act). The Data Standards must, under proposed Rule 8.11(1A): • cover how the Accredited Person can meet the requirement to explain a CDR Insight in accordance with proposed Rule 4.11(3)(ca); and • ensure that the CDR Consumer is made aware that their CDR Data will leave the CDR system when it is disclosed. In addition, under proposed Rule 8.11(1)(c)(v), the Data Standards Chair must make consumer experience Data Standards for disclosure of CDR Insights.	*consent without complete awareness of that information being disclosed…* *We recommend that instead of an explanation of the insight, the consumer should be provided with the exact insight that would be shared to remove any ambiguity and provide consumers with the opportunity to make an informed decision of whether to give consent.'* We consider that there is merit in this proposal, because it would increase transparency, and control for CDR Consumers. ***Recommendation**: We recommend that Treasury consider:* • *as discussed in relation to Risk 3, whether different rules should be able to apply for CDR Consumers who are individuals or sole traders, and for CDR Consumers who are businesses;* • *working with the regulators to ensure clear and detailed guidance is provided to the market so that potential recipients of CDR Insights understand that they must not seek to pressure a CDR Consumer to consent to the disclosure of their CDR Insight;* • *as discussed in relation to Risk 9, whether (through the Data Standards) CDR Consumers should be made aware of the implications and consequences of their CDR Data leaving the CDR system;* • *working with the Data Standards Body to develop appropriate Data Standards (in consultation with industry and informed by consumer research), to ensure that CDR*

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Consumers fully understand what it is they are consenting to in relation to their CDR Insights; and • *whether CDR Consumers should be required to be shown the particular CDR Insight before it is disclosed (as opposed to simply being provided with an explanation of the CDR Insight or the purpose for its disclosure), so that they can decide not to provide their consent if they do not wish it to be disclosed. For example, CDR Insights in relation to verifying credits and debits on an account may potentially disclose information which an individual CDR Consumer may be uncomfortable about disclosing.* We also note that the proposed amendments to the CDR Rules will not prescribe whether and/or how an Accredited Data Recipient may seek a CDR Consumer's ongoing consent to use CDR Data (for the purposes of creating CDR Insights) and disclose CDR Insights. This is especially important given this may mean ongoing disclosure of valuable CDR Insights outside of the CDR regime (and therefore this information will not be afforded the protections of the CDR regime, as discussed extensively above). ***Recommendation**: We recommend that Treasury consider requiring that further consumer research be conducted on whether CDR Consumers understand the difference between a one-off versus an ongoing use and disclosure consent in relation to CDR Insights, and based on this research, determine whether it would be appropriate for the CDR Rules and/or Data Standards to prescribe how such consent must be sought from CDR Consumers.*

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
12.	**CDR Insights may be more invasive than sharing raw CDR Data** 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. This is because CDR Insights contain the results of the analysis of raw CDR Data.	Under proposed Rule 1.10(3), a CDR Consumer may only provide an insight disclosure consent (i.e. for their CDR Insights to be disclosed to a specified person) for a limited number of purposes, which include the following: • identifying the CDR Consumer; • verifying the CDR Consumer's account balance; • verifying credits to, and debits from, the CDR Consumer's account. As discussed in Risk 9, under proposed Rule 7.5A(4), an Accredited Data Recipient is only permitted to disclose a CDR Insight under an insight disclosure consent if the CDR Insight does not include or reveal sensitive information (as defined in the Privacy Act).	Based on the limited purposes listed in the proposed amendments to the CDR Rules, we consider that it may be sufficient if only information that does not include sensitive information (as defined in the Privacy Act) would achieve the desired policy objectives associated with permitting CDR Insights to be disclosed outside of the CDR regime. We support this limitation in the proposed amendments to the CDR Rules, which may assist in mitigating against the invasive nature of CDR Insights, which may be more inherently sensitive than raw CDR Data. In addition, if the definition of 'CDR insight' is further clarified (e.g. if it is further narrowed to be a 'yes' or 'no' answer to a question), then this risk may be further mitigated.

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
13.	**Risk relating to the transfer of CDR Insights to recipients** In transferring CDR Insights to a recipient, an Accredited Person does not need to expressly comply with the CDR Rules or Data Standards in relation to such transfers. This may increase the risks of loss or unauthorised access and disclosure during that transfer.	Accredited Data Recipients are required to comply with the requirements of Schedule 2 to the CDR Rules, which specify minimum security requirements related to CDR Data held by Accredited Data Recipients.	As discussed in relation to Risk 4, we are concerned that there may be uncertainty about the application of the encryption requirements in Schedule 2 to the transfer of CDR Insight by Accredited Data Recipients Again, this raises the risk that there may be more scope for unauthorised access or disclosure of the CDR Data during transfer. ***Recommendation**: We recommend that Treasury consider whether it is appropriate to amend the Data Standards and/or ensure that appropriate guidance is provided, so that it is clear that all CDR Data (including CDR Insights) must be appropriately encrypted in accordance with Schedule 2 to the CDR Rules, from the time the data leaves the Accredited Data Recipient's CDR data environment until it reaches the recipient's IT environment.*
14.	**CDR Consumer does not remember of disclosure of CDR Insights** There is a risk that after a CDR Consumer gives their consent to the disclosure of their CDR Insights, they are unaware of, and/or do not remember, the details of this disclosure (including what information was included in the CDR Insights and to whom it was disclosed).	Under proposed Rule 7.9(4), if an Accredited Data Recipient discloses a CDR Insight, it must, as soon as practicable, update its Consumer Dashboard to include: • what CDR Data was disclosed; • when the CDR Data was disclosed; and • the person to whom it was disclosed.	We support CDR Consumers being provided with information about their CDR Insights on their Consumer Dashboards. We are conscious that Accredited Persons are required to update their Consumer Dashboards in accordance with two sets of requirements under the proposed amendments to the CDR Rules, which runs the risk of "information overload" for CDR Consumers. ***Recommendation:** We recommend that Treasury consider whether it would be appropriate to:* • *consolidate the requirements on Accredited Persons to update Consumer Dashboards in relation to CDR Insights (as there is some overlap in requirements); and* • *similar to the information provided when a CDR Consumer provides their consent, include a requirement for an*

DISCLOSURE OF CDR INSIGHTS TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		Under proposed Rule 1.14(3)(ea), it must also include in its Consumer Dashboard a description of the CDR Insight and to whom it was disclosed. In addition, the requirements in relation to the provision of a CDR receipt under Rule 4.18 will apply, providing CDR Consumers with information on the disclosure consent they provide to the Accredited Person (as CDR Insights will include CDR Data).	*Accredited Person to provide the preview (if that is the approach adopted) of the CDR Insight disclosed in its Consumer Dashboard.*

22. Risks associated with the introduction of a sponsored level of accreditation

INTRODUCTION OF SPONSORED LEVEL OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
15.	**Risk that CDR Consumer does not know or understand the different requirements for accreditation of the Affiliate who will be handling their CDR Data**	If CDR Data will be collected by a Sponsor at the request of an Affiliate, the request for consent by the CDR Consumer must specify this fact (proposed Rule 4.3(2A)(a)) (and a consent for the Affiliate to collect the CDR Data is taken to be consent for the Sponsor to collect that CDR Data (proposed Rule 4.3(2A)(b)). In addition, when the CDR Consumer is asked to provide consent, they must be informed of (among other things) (proposed Rule 4.11(3)(i)): • the fact that the Affiliate is the accredited person and the Sponsor will be collecting the CDR Data on request by the Affiliate; • the Sponsor's name and accreditation number;	We consider that the requirements to inform the CDR Consumer of the entity (i.e. the Sponsor) that will be collecting their CDR Data at the request of the Affiliate (proposed Rule 4.3(2A)(a)) to be a privacy-enhancing feature of the proposed amendments. However, it will be important to ensure that the CDR Consumer understands the effect of a person being described as a Sponsor or Affiliate. For example, if phrases such as *"Powered by [sponsor name]"* are permitted, they are unlikely to convey much meaning. While it is privacy-enhancing that CDR Consumers will be provided with a link to a Sponsor's CDR policy, and told that they can obtain further information about collections or disclosures from that policy, we consider there is still a risk that CDR Consumers will not understand the effect of an Affiliate being involved. We note that risk has also been identified by stakeholders. For example, the Australian Energy Council has noted: *'The constitution of the sponsorship model, and its related elements (CDR representatives and OSPs), is complex and technical, so there will need to be explanatory material written in plain English to improve the ability of customers to understand what their data can be used for, liability arrangements, and the complaints process.'* ***Recommendation:*** *We recommend that Treasury 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 information on the implications of providing a consent which will permit the collection of*

INTRODUCTION OF SPONSORED LEVEL OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• the fact that the CDR Consumer can obtain further information about such collections or disclosures from the Sponsor's CDR policy (noting that a link to this CDR policy must be provided). If CDR Data will be collected by a Sponsor at the request of an Affiliate, the proposed amendments will require the Affiliate to ensure that their consumer dashboard includes the Sponsor's name and accreditation number (proposed Rule 1.14(3)(ha)). Similarly, an Affiliate's consumer dashboard must reflect this fact (proposed Rule 7.4(d)). Details of the Sponsor of an Affiliate (and vice versa) must be made available in the public Register of Accredited Persons (proposed Rule 5.24). Proposed Rule 7.2(4) will mean that the Affiliate's CDR policy must contain information about their Sponsorship Arrangement with the Sponsor.	*CDR Data by a Sponsor at the request of an Affiliate, and the disclosure of that CDR Data to the Affiliate.*

INTRODUCTION OF SPONSORED LEVEL OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
16.	**Incentive on Sponsor to ensure compliance by Affiliate** We query whether the obligations on a Sponsor in connection with their Affiliate's accreditation are sufficiently robust.	Before becoming a Sponsor, the Accredited Person must undertake 'due diligence' in respect of the proposed Affiliate. The Sponsor must also take 'reasonable steps' to ensure ongoing compliance by the Affiliate. An Affiliate may only make consumer data requests to the Sponsor or through the Sponsor acting on its behalf under a Sponsorship Arrangement (an Affiliate cannot engage an Outsourced Service Provider to collect CDR Data on its behalf) (proposed Rule 5.1B). An Affiliate is an Accredited Person, and therefore responsible in its own right for compliance with the CC Act and 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 are concerned as to whether the current amendments provide a Sponsor with enough incentive for it to actively monitor and otherwise ensure that the Affiliate is suitable to be an Accredited Person. Additionally, we note that whether an Affiliate or proposed Affiliate is suitable is subjective and could be difficult for Sponsors to determine. As one stakeholder, Adatree, has noted: *'suitable is not measurable and is subject to interpretation'.* Adatree has suggested that there should be guidelines or requirements in place to assist Sponsors to determine whether their proposed Affiliate is 'suitable'. ***Recommendation:*** *We recommend that Treasury takes steps to ensure that there is appropriate guidance about what is required for a Sponsor in relation to its Affiliate (particularly in relation to actively monitoring and ensuring that the Affiliate is suitable to handle CDR Data). For example, it is not clear whether a Sponsor would satisfy the test by simply including appropriate obligations and warranties in the Sponsorship Arrangement.*

23. Risks associated with the introduction of non-accredited CDR Representatives

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
17.	**CDR Data is disclosed outside of CDR regime** As extensively discussed in relation to Risk 1 and Risk 9 above, the proposed amendments will result in CDR Data being disclosed outside of the CDR regime, where the data will have fewer legislative privacy protections (or potentially no legislative privacy protections if the CDR Representative is not an APP entity for the purposes of the Privacy Act) than the same data will have when being held by an entity within the CDR regime.	Under proposed Rule 1.16A, the Accredited Data Recipient: • is responsible for ensuring the CDR Representative's compliance with the requirements under the CDR Representative Arrangement; and • must keep and maintain records in relation to each CDR Representative Arrangement, including the use and management of data by each CDR Representative, and the steps taken to ensure any CDR Representatives comply with their requirements under the arrangements. CDR Representative Arrangements are required to impose a number of obligations on CDR Representatives, including compliance with a number of Privacy Safeguards and Schedule 2 to the CDR Rules. Additionally, the CDR Principal will be responsible for any breach by the CDR Representative of these Privacy Safeguards or of any	We note that the proposed amendments will allow the disclosure of CDR Data to recipients who are not Data Holders or Accredited Persons (and do not have any direct obligations under the CDR legislative framework). We appreciate that entities who are likely to be CDR Representatives may currently be using unsafe data access, transfer and handling technologies to obtain information about CDR Consumers from Data Holders (such as through "screen-scraping"). The proposed amendments to the CDR Rules provide a greater degree of privacy protections for CDR Consumers than would otherwise exist. We support the requirement for CDR Representative Arrangements to include privacy protections, including applicable Privacy Safeguards. This is an important protection in ensuring that CDR Representatives who are not themselves Accredited Data Recipients, and are therefore not bound by the Privacy Safeguards, have contractual obligations in respect of CDR Data (and are made aware of those obligations). However, arguably one of the most important of these obligations is contained in Privacy Safeguard 6 (effectively, to only use and disclose CDR Data in accordance with the CDR Consumer's consent). Under Rule 1.16A, the CDR Principal (i.e. the Accredited Data Recipient) must ensure that the CDR Representative complies with its requirements under the CDR Representative Arrangement, but is only in breach of this obligation if the CDR Representative breaches a "required provision". There is no such provision requiring inclusion of an obligation to use/disclose CDR Data in accordance with the CDR Consumer's consent.

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		mandatory requirements for CDR Representatives. If an Accredited Data Recipient has disclosed CDR Data in accordance with a CDR Representative Arrangement (as required under proposed Rule 1.10AA), it will remain responsible for use and disclosure of the CDR Data by the CDR Representative, irrespective of whether the use or disclosure is in accordance with the CDR Representative Arrangement (proposed Rule 7.6(3)).	Separately, we understand that the CDR Principal (i.e. the Accredited Data Recipient) will be in breach of the CDR legislative framework if it discloses CDR Data to the CDR Representative other than in accordance with a consent from the CDR Consumer (this would not be a permitted use under PS6 and Rule 7.7). In addition, under Rule 7.6(5), use or disclosure of service data by the CDR Representative is taken to be by the CDR Principal (even if that use or disclosure was permitted by the CDR Representative Arrangement). In such a case the CDR Principal will be in breach (and liable), but if an appropriate obligation is not in the CDR Representative Arrangement, the CDR Representative may not understand their obligations or have incentive to comply. From the CDR Consumer's perspective, a regulator taking action against a CDR Principal may not assist if the CDR Data has already been incorrectly used/disclosed. ***Recommendation**: We recommend that Treasury consider strengthening the requirements for CDR Representative Arrangements, to further ensure that a CDR Representative will only use and disclose CDR Data after receipt from the CDR Principal (i.e. the Accredited Data Recipient) in accordance with the consent of the CDR Consumer.* *This could be achieved by:* • *extending the matters that must be in a CDR Representative Arrangement to include a contractual obligation on the CDR Representative to comply with section 56EI (Privacy Safeguard 6) of the CC Act, in respect of Service Data, as if it were an Accredited Person; or* • *including a requirement that the CDR Representative Arrangement must include an obligation on CDR*

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Representative to comply with APP 6 of the Privacy Act (as if it were an 'organisation' under the Privacy Act).
18.	**CDR Consumers are unaware that their CDR Data is being handled by the Accredited Data Recipient** From the point of view of a CDR Consumer, they will only deal with the CDR Representative (and will give their consent to the CDR Representative). There is a potential risk that CDR Consumers will not be aware that their CDR Data will be collected from the Data Holder, and provided to the CDR Representative, by the Accredited Data Recipient.	Under proposed Rule 4.3A(5)(c), if a CDR Representative asks for a CDR Consumer's consent for the purposes of the Accredited Data Recipient making a consumer data request to the Data Holder on the CDR Representative's behalf, it must provide the CDR Consumer with the information in Rule 4.11(3) (subject to some modifications). This information includes: • notifying the CDR Consumer that the person is a CDR Representative and that their CDR Data will be collected by its Principal at its request; • informing the CDR Consumer of the Principal's name; • informing the CDR Consumer of the Principal's accreditation number; • providing the CDR Consumer with a link to the Principal's CDR Policy; and	We are satisfied that the draft CDR Rules have appropriately mitigated this risk and that no further action is required.

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• providing the CDR Consumer with a statement that the CDR Consumer can obtain further information about such collections or disclosures from the Principal's CDR Policy if desired. PS 1 requires an Accredited Data Recipient's CDR Policy to include a list of its CDR Representatives (proposed Rule 7.2(4)(ac)). In addition, under proposed Rule 1.14(5), if a Principal makes a consumer data request at the request of a CDR Representative, the Principal may arrange for the CDR Representative to provide the Consumer Dashboard on its behalf.	
19.	**The CDR Rules do not expressly require CDR Representative Arrangements to deal with communication between the Accredited Data Recipient and the CDR Representative about a CDR Consumer's consent** The CDR Rules contain requirements for what should	The penalties for a breach by an Accredited Data Recipient will be an incentive for the parties to ensure that their CDR Representative Arrangement contains all necessary requirements to ensure compliance with their legislative obligations.	***Recommendation:*** *Given the importance of effectively and accurately communicating the CDR Consumer's consent (and the role of their consent in the CDR regime), we recommend that Treasury consider amending the draft CDR Rules so that CDR Representative Arrangements are expressly required to contain an obligation:* • *upon the CDR Representative to accurately communicate the CDR Consumer's consent to the Principal;* • *in relation to withdrawal of a CDR Consumer's consent or authorisation:*

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	be contained in CDR Representative Arrangements, but do not specify any mandatory provisions relating to communication of information about a CDR Consumer's consent or withdrawal of their consent.		○ *upon the CDR Representative to notify the CDR Principal if the CDR Representative becomes aware that the CDR Consumer has withdrawn their consent; and* ○ *upon the CDR Principal to notify the CDR Representative if they otherwise become aware that the consent or authorisation has been withdrawn or expired,* *so that the CDR Representative and the Principal do not inadvertently continue to collect, use or disclose CDR Data without an appropriate consent and authorisation.*
20.	**Uncertainty around disclosure consents for the Accredited Data Recipient to disclose their CDR Data to the CDR Representative**	Under Rule 4.3A, a CDR Representative may ask the CDR Consumer to give: • a collection consent for the CDR Principal to collect their CDR Data from the Data Holder; and • a ***use consent*** for: ○ the CDR Principal to ***disclose*** that data to the CDR Representative; and ○ for the CDR Representative to ***use*** it in order to provide those goods or services.	Under the proposed amendments to the CDR Rules (Rule 4.3A), a CDR Consumer will provide: • a collection consent for the Principal to collect the CDR Data from the Data Holder or another Accredited Data Recipient; and • a ***use*** consent for: ○ the CDR Principal to ***disclose*** the CDR Data to the CDR Representative; and ○ the CDR Representative to ***use*** the CDR Data to provide the relevant goods or services to the CDR Consumer.

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			In addition, it is unclear how proposed Rule 1.10A(4) will operate with proposed Rule 4.3A. We are uncertain why a disclosure consent is not required for the Principal to disclose CDR Data to the CDR Representative. We maintain that, consistently with the operation of the rest of the CDR Rules, the CDR Consumer will conceptually need to provide three types of consents (a collection consent for the Accredited Data Recipient to collect the CDR Data from the Data Holder, a disclosure consent for the Accredited Data Recipient to disclose the collected CDR Data to the CDR Representative, and consent for the collection and use/further disclosure by the CDR Representative) – even if in practice it is acceptable for all to be given at the same time. ***Recommendation**: We note that implementation of the recommendation discussed at Risk 1 may address any potential confusion for CDR Consumers and CDR participants.*
21.	**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 their collection consent. The proposed amendments provide that a consumer data	Rule 4.18A provides that if a CDR Consumer's collection consent expires (including because the CDR Consumer withdraws that consent), the CDR Representative must notify the CDR Consumer that they may: • withdraw the use consent; and • make the election to delete redundant data in respect of that CDR Data.	Given the uncertainty as identified in Risk 20, we are concerned that a CDR Consumer may not understand that only if they withdraw their ***use*** consent, the Principal must stop ***disclosing*** CDR Data to the CDR Representative. ***Recommendation:** We note that implementation of the recommendation discussed at Risk 1 may address any potential confusion for CDR Consumers and CDR participants*

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	request ceases to be valid if the collection consent is withdrawn. However, these amendments also provide that so long as the use consent is not also withdrawn, the Principal could continue to disclose CDR Data it had already collected to the CDR Representative, and the CDR Representative could use it in order to provide the requested goods or services.		
22.	**Continued use of CDR Data by CDR Representative, after Accredited Data Recipient's accreditation ends** There is a risk that a CDR Representative continues to use CDR Data it has collected from an Accredited Data Recipient after the suspension, revocation or surrender of the accreditation of the Accredited Data Recipient, meaning that there may no longer be a relevant use consent.	Under proposed Rule 4.3B(j)(2) if an Accredited Data Recipient's accreditation is revoked or surrendered, all of the consents of any CDR Representative expire when the revocation or surrender takes effect. The CDR Rules provide that if an Accredited Data Recipient's accreditation has been surrendered or revoked, they must delete or de-identify the CDR Data by taking the steps specified in Rules 7.12 and 7.13. The proposed amendments to the CDR Rules require the CDR Representative to, if directed by the Accredited Data Recipient in accordance with the CDR Representative Arrangement (see proposed Rule 1.10AA(2)(d)(iv)) delete CDR Data in	***Recommendation:*** *We recommend that Treasury consider amending the draft CDR Rules to provide that CDR Representative Arrangements must include a requirement for Accredited Data Recipients to notify a CDR Representative if their accreditation ends, and:* • *notify the CDR Representative that any consents it has collected in relation to the CDR Consumer's CDR Data expire (explaining the consequences of this i.e. the CDR Representative can no longer use the CDR Data, nor further disclose this CDR Data); and* • *promptly direct them to delete any CDR Data (in accordance with the CDR Data deletion process).* *We also recommend that similar protections could be imposed if a CDR Consumer subsequently withdraws their consent (or the consent otherwise expires), so that both the CDR Principal and the*

INTRODUCTION OF CDR REPRESENTATIVES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		accordance with the CDR Data deletion process (proposed Rule 7.12(2)(b)). The Data Recipient Accreditor must notify the Accreditation Registrar about information relating to accreditations of Accredited Data Recipients, including of any surrender, suspension or revocation (Rule 5.15). The Accreditation Registrar must then update the Accreditation Register to reflect these details (Rule 5.24).	*CDR Representative are made aware of the status of the consent and required to take appropriate actions.*

SECTION 2: JOINT ACCOUNT CHANGES

24. Introduction

24.1 In this **Section 2** of **Part E [Analysis of Risks]**, we have analysed risks that we have identified as being associated with the proposed amendments to the CDR Rules in respect of the Joint Account Changes (i.e. the proposed implementation of the default pre-approval option for all joint accounts, and the general application of the joint account CDR Rules for all Sectors unless specifically amended by a Sector-specific Schedule to the CDR Rules).

24.2 In the table below we have described and considered the privacy risks associated with the proposed amendments and have identified some of the key existing mitigation strategies that have been included in the legislative framework, or are intended to be included in the proposed amendments to the CDR Rules, together with our analysis of any identified gaps.

24.3 For each identified gap, we have then considered whether any additional mitigation strategies could be implemented, to further protect the privacy of individuals. These recommendations are referenced in this **Part E [Analysis of Risks]** but are more fully discussed in **Part A [Executive Summary]**.

24.4 In our analysis below, we have only considered privacy impacts and risks that arise directly as a result of the proposed amendments to the CDR Rules, and we have not sought to revisit risks and recommendations that were discussed in the Original PIA report or the PIA Update 2 report[4], unless they have been changed as a result of the currently proposed amendments to the CDR Rules.

[4] For completeness, we note that the PIA Update 1 report did not discuss proposed amendments to the CDR Rules in respect of joint accounts.

25. Risks associated with the introduction of default pre-approval option for joint accounts

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
23.	**JAH B will not always have to take active steps to give informed consent to the sharing of their joint account CDR Data prior to the CDR Data being shared** If the default pre-approval model is implemented, JAH B will not have to actively give informed consent to the sharing of CDR Data on their joint account(s) prior to the relevant data being shared by JAH A.	As discussed in more detail in Risk 26 below, it is proposed that Data Holders will be required to provide a range of information to all JAHs about the default data sharing setting on joint accounts and how to change them. JAHs will have the ability to change the default data sharing option (from pre-approval to another option). Data Holders must give effect to this change, as soon as practicable.	If the default pre-approval model is implemented and JAH A makes a Consumer Data Request, JAH B will not be required to actively provide their informed consent to the disclosure of the joint account CDR Data unless the co-approval option has been selected in DOMS by either JAH. Under the current CDR Rules, JAH B must actively give their informed consent to the sharing of their joint account CDR Data. This can occur on a one-off basis (by selecting the pre-approval option in DOMS for all future Consumer Data Requests to share CDR Data), or for each future Consumer Data Request. Under the proposed changes, it will be assumed that a JAH B will have decided to apply the pre-approval default setting, and (if they are happy with that option) decided not to change it in DOMS. Inaction by JAH B will be assumed to be implied consent by JAH B to the default setting (i.e. pre-approval). However, it will not be possible to know whether JAH B actually did know about, consider, and make an informed decision, to not change the default setting. We note that obtaining appropriate consent from CDR Consumers before sharing their CDR Data represents best privacy practice and is a key feature of the current CDR Rules (specified in Division 4.3 of the CDR Rules) The benefits of this protection have been communicated to the public as a fundamental principle of the CDR regime.

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			A number of stakeholders have raised significant concerns about this fundamental principle potentially being eroded: • The OAIC has stated: *'The proposed opt-out approach would allow data holders to share a non-requesting joint account holder's CDR data without their express consent (or prior approval). This is inconsistent with the fundamental principle of express consent for data sharing that is central to the operation of the CDR system. It would also appear contrary to both Australian and international best practice regarding consent, where the trend is towards requiring a positive act by an individual to indicate consent…For example, under Article 20 of the General Data Protection Regulation, individuals have a right to data portability, but only where consent has been given (and processing is by automated means). Similarly, Singapore and New Zealand have placed emphasis on the importance of consumer choice and control in the development of their respective data portability rights. In the Australian context, a number of reviews including the ACCC's Digital Platforms Inquiry Final Report, have recommended that consent requirements be strengthened, including the potential to require consent for all handling of personal information and the need to ensure consent is valid, i.e. freely given, specific, unambiguous and informed, and in particular is not the result of pre-selected default settings or 'bundled' consent.'* • The Australian Energy Council '*remains principally opposed to an opt-out data sharing model, or "pre-approval" option as it is now called, for joint accounts. This fundamentally*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			goes against the principle of customer consent that underpins the CDR. It is concerning that some of the terminology used to justify this option, such as reducing "friction" or minimising "inconvenience", appears to imply that obtaining customer consent is a burden rather than an important customer protection.' • The National Australia Bank has stated: *'NAB has concerns that the proposed changes to joint accounts undermine a central principle of the CDR regime, being that consumers should be in control of their CDR data, and any movement of CDR data should be based on consent…the default 'pre-approval' setting raises concerns in relation to privacy, the protection of vulnerable customers, as well as general customer friction and poor experience'.* • The Consumer Policy Research Centre has stated that '*establishing an opt-out solution further distances consumers from feeling empowered and in control of their data'*. • Origin Energy has stated: *'A fundamental consumer protection in energy is the concept of explicit informed consent. This means that a customer must actively provide consent before a retailer can make changes to their plan or whether information on their account is shared. We believe this principle must be preserved under CDR regime.'*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			The proposed change would have the impact of implementing an implied consent model, rather than the current express consent model. OAIC guidance indicates that an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, and that, generally, express consent should be sought where the personal information that will be handled has a degree of sensitivity. We are concerned that the proposed CDR Rules have serious consequences for the privacy rights of JAH B. For example, even if JAH B later decides to change the disclosure option in DOMS, it is not clear that JAH B will be able to request that any previously shared joint account CDR Data be deleted by the relevant recipient. Removing the need for an active step that clearly indicates informed consent to the disclosure of CDR Data may be inconsistent with community expectations about the CDR regime. We do appreciate that whilst moving away from a purely express consent model in respect of joint accounts may not represent privacy best practice, this must be balanced against other factors (e.g. whether the implementation of the default pre-approval model will increase participation in the CDR regime and allow CDR Consumers to access the benefits that might arise from the sharing of CDR Data). ***Recommendation**: We recommend that the decrease in privacy protections that would be afforded to JAH Bs under the proposed changes to the CDR Rules be carefully considered by Treasury, as part of the balancing of relevant factors.*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			We also recommend that if a decision is made to implement the default pre-approval model despite the impact on privacy rights, consideration be given to implementing a process (if technically possible) so that: • *after JAH A makes a Consumer Data Request in respect of joint account CDR Data, the data is **not** immediately shared;* • *after JAH A makes the Consumer Data Request, JAH B is notified of the request and given a reasonable window of time in which to select a disclosure option (and notified that if the pre-approval option (or no option) is selected in the given timeframe, the joint account CDR Data will be shared in accordance with the Consumer Data Request); and* • *the joint account CDR Data is:* ○ *if JAH B selects the pre-approval option (or no option is selected in the given timeframe), shared in accordance with the Consumer Data Request;* ○ *if JAH B selects the co-approval option and consents to the disclosure of the CDR Data, shared in accordance with the Consumer Data Request;* ○ *if JAH B selects the co-approval option and does not consent to the disclosure of the CDR Data, not shared (i.e. the Consumer Data Request is not given effect); and*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			○ *if JAH B selects the no disclosure option, not shared (i.e. the Consumer Data Request is not given effect).*
24.	**JAH B (or both JAH A and JAH B if a request is made by a Secondary User) may not be informed about the sharing of their joint account CDR Data**	Proposed Rule 4A.15 will mean that a Data Holder is not liable under the CDR Rules for a failure to comply with Part 4a (joint accounts) if it considered that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse to any person.	We note that proposed Rule 4A.15 will effectively allow Data Holders not to provide information to JAH B about the sharing of their joint account CDR Data if the Data Holder considers that this is necessary to prevent physical, psychological or financial harm or abuse to any person. We appreciate the need to protect vulnerable JAHs (this has been considered at length in previous PIA Reports). However, we are concerned that proposed Rule 4A.15: • does not indicate the standard to which the Data Holder must be satisfied that a joint account holder is at risk of physical, psychological or financial harm or abuse (e.g. an obligation for them to be reasonably satisfied or to reasonably believe this). We believe this is important where the protection of that person from harm needs to outweigh the impact on another joint account holder's right to know how their joint account CDR Data is being shared; and • will apply generally to all Sectors, unless modified by a Sector-specific schedule – and all Data Holders in all Sectors will necessarily have processes in place to identify and consider issues of vulnerability and weigh up the factors discussed above. ***Recommendation**: We recommend that Treasury consider amending the draft CDR Rules to require the Data Holder to be reasonably satisfied that the protection of a person (e.g. JAH A)*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			from harm outweighs the impact on JAH B's right to know how their joint account CDR Data is being shared. *Additionally, we suggest that Treasury consider, for each Sector, whether all Data Holders will have processes in place to identify and consider issues of vulnerability and weigh up the factors discussed above. If Treasury considers that all Data Holders in a Sector will not have mature processes in place to consider such matters, we recommend that Treasury consider whether it would be appropriate to amend proposed Rule 4A.15 by way of a Sector-specific Schedule to the CDR Rules.*
25.	**Delay between JAH B selecting the co-approval option or no disclosure option and the cessation of sharing the relevant CDR Data** If the pre-approval option is enabled (either via default or by request) and JAH A makes a Consumer Data Request and JAH B subsequently selects a co-approval or no-disclosure option in DOMS, there is a risk that there will be a delay between the election being made in DOMS by JAH B and the Data Holder ceasing to share the joint account CDR Data.	Under the CDR Rules, a Data Holder must give effect to an election by a JAH to change a data sharing option in DOMS, 'as soon as practicable'.	While the existing mitigation strategy will continue to apply, if the proposed amendments occur it will be even more important to ensure that if JAH B has selected the co-approval option (if this is offered by the Data Holder) or no-disclosure option in DOMS, this is given practical effect by the Data Holder from a technical perspective as soon as possible, to ensure that CDR Data is not shared after such an option is exercised (for the reasons described in Risk 23 above). ***Recommendation**: We recommend that Treasury work with the regulators of the CDR regime to ensure that appropriate guidance (including guidance about technical requirements) is provided to Data Holders to ensure that they understand what 'as soon as practicable' means in the context of an election made through DOMS (which we consider should be as near real time as is technically possible).*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	In other words, there is a risk that joint account CDR Data may be shared where JAH B has expressly selected that they want: • joint account CDR Data to only be shared with their consent (i.e. the co-approval option); or • no joint account CDR Data to be shared (i.e. the no disclosure option).		
26.	**CDR Consumers may not be aware of the default pre-approval option on their joint accounts** There is a risk that CDR Consumers will not be aware of the default pre-approval setting on their joint accounts.	It is proposed that the CDR Rules will be amended to require Data Holders to keep JAHs informed about which disclosure option currently applies (proposed Rule 4A.6(7)).	We consider it important that all JAHs understand that the default data setting for data sharing on joint accounts will be set to pre-approval, and also understand how to change this default setting. We note that the proposed amendments to the CDR Rules will achieve this by obliging Data Holders to keep JAHs informed about which disclosure option currently applies to their joint account (proposed Rule 4A.6(7)). We consider that it is privacy enhancing that Data Holders will be required to provide this information, although it is not clear how regularly this information must be provided to JAHs. However, the proposed amendments to the exposure draft of the CDR Rules have removed the details about what information must be provided to JAHs about disclosure options on their joint account, and mean that CDR Consumers who already have joint accounts will not have a window of time in which to actively select a co-

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			approval or no disclosure option on their joint accounts (in place of the default pre-approval option). We consider that these changes reduce the privacy protections afforded to JAHs and that it would be preferable for JAHS to be: • regularly informed of the default data setting for data sharing on joint accounts being set to 'pre-approval'; • regularly informed about how they can change the default sharing setting on their joint account; and • given a window of time, before the commencement of the default disclosure option, in which to actively select a co-approval or no disclosure option (i.e. to override the default pre-approval option). ***Recommendation**: We recommend that if Treasury implements the proposed amendments to the CDR Rules, Treasury ensure that all CDR Consumers are made aware, prior to the commencement of the amended CDR Rules, of the change to the default disclosure option setting. For example, a broad education campaign could be a mechanism to:* • *advise JAHs of the default data setting for data sharing on joint account being set to 'pre-approval';* • *inform JAHs about what options are available in relation to the joint account;* • *explain the effect of each disclosure option and how it operates;*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• *inform JAHs about how they can change the default sharing setting on their joint account.* *Additionally, we recommend that the above is undertaken a reasonable amount of time before the default disclosure option is implemented. This will give JAHs the opportunity to consider the impact of the various disclosure options and make an informed choice.*
27.	**CDR Consumers may not understand the implications of 'opting out' of receiving important notifications regarding Consumer Data Requests on joint accounts**		The proposed amendments to the CDR Rules will allow CDR Consumers to 'opt out' of receiving particular notifications regarding Consumer Data Requests on joint accounts, subject to the Data Standards. There is therefore a risk that CDR Consumers will: • not understand the impacts of choosing not to receive such notifications; and/or • will forget that they have 'turned off' such notifications. ***Recommendation**: We recommend that Treasury consider whether it would be appropriate to:* • *ensure that CDR Consumers who are joint account holders are provided with appropriate guidance about what type of notifications they can disable, and the impacts of disabling those notifications; and*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• *regularly remind joint account holders if they have disabled notifications, such that they are prompted to consider whether they should re-enable the notifications.*
28.	**The CDR Rules regarding joint accounts in the banking Sector may not be 'fit for purpose' for other designated Sectors**		The proposed changes to the CDR Rules mean that the joint account CDR Rules will apply across all designated Sectors (as opposed to just the banking Sector, as is currently the case), but they may be modified by a Sector-specific Schedule to the CDR Rules. Each designated Sector is likely to have privacy considerations in relation to joint accounts that may be different from the banking Sector. This is because in respect of each designated (or to be designated) Sector: ▪ it is not necessarily known what data will be designated as CDR Data; and ▪ it is not understood whether joint accounts practically operate in the same manner as they do in the banking Sector. In short, the privacy (and other) impacts of extending the joint accounts CDR Rules to other Sectors cannot currently be precisely defined or considered. It is not possible to quantify the magnitude of this risk at this stage. ***Recommendation**: We recommend that, because the privacy risks and issues for joint account holders may be very different for different Sectors, the privacy implications of joint accounts for any new Sector(s) are considered by Treasury for each current and new Sector, including whether it is necessary to adjust the application of*

DEFAULT PRE-APPROVAL OPTION FOR JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			the general joint account CDR Rules for a new sector (through a Sector-specific schedule).

Part F GLOSSARY

Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
Access Changes	means changes relating to how CDR Data may be accessed as outlined in the proposed amendments to the CDR Rules.
Accreditation Register	means the register established in accordance with section 56CE(1) of the CC Act.
Accredited Data Recipient	has the meaning given by section 56AK of the CC Act.
Accredited Person	means a person who holds an accreditation under section 56CA(1) of the CC Act.
Affiliate	means a person with accreditation at the sponsored level.
Australian Privacy Principles (APPs)	means the Australian Privacy Principles at Schedule 1 to the Privacy Act.
CC Act	means the *Competition and Consumer Act 2010* (Cth).
CDR Consumer(s)	has the meaning given by section 56AI(3) of the CC Act.
CDR Data	has the meaning given by section 56AI(1) of the CC Act.
CDR Insight(s)	has the meaning give in proposed Rule 1.7(1) of the CDR Rules.
CDR Participant	has the meaning given by section 56AL(1) of the CC Act.
CDR Principal	has the meaning given by proposed Rule 1.10AA of the CDR Rules.
CDR Representatives	has the meaning given by proposed Rule 1.10AA of the CDR Rules.
CDR Representative Arrangement	has the meaning given by proposed Rule 1.10AA of the CDR Rules.
CDR Rules	means the *Competition and Consumer (Consumer Data Right) Rules 2020*.
Consumer Dashboard	(a) in relation to an Accredited Person, has the meaning given by Rule 1.14 of the CDR Rules. (b) in relation to a Data Holder, has the meaning given by Rule 1.15 of the CDR Rules.
Consumer Data Request	means a request made by a CDR Consumer, or by an Accredited Data Recipient on behalf of a CDR Consumer, to a Data Holder to obtain CDR Data about a CDR Consumer.

Data Holder(s)	has the meaning given by section 56AJ of the CC Act.
Data Recipient Accreditor	means the person appointed to the role of Data Recipient Accreditor in accordance with section 56CG of the CC Act.
Data Standards Body	means the body holding an appointment under section 56FJ(1) of the CC Act.
Data Standards	means the data standards made under section 56FA of the CC Act.
DOMS	means a disclosure option management service.
Joint Account Changes	means the introduction of a default pre-approval option for all joint accounts, and the general application of the joint account CDR Rules for all Sectors unless specifically amended by a Sector-specific Schedule to the CDR Rules.
JAH A	means a CDR Consumer that makes a Consumer Data Request in respect of a joint account.
JAH B	means another CDR Consumer on a joint account.
Minister	means the Minister for Superannuation, Financial Services and the Digital Economy.
Notifiable Data Breach scheme	means the scheme described in Part IIIC of the Privacy Act.
OAIC	means the Office of the Australian Information Commissioner.
Open Banking Designation	means the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth).
Original CDR PIA report	means the Privacy Impact Assessment report in relation to the Consumer Data Right Regime published on 11 December 2019.
PIA Update reports	means the previous privacy impact update processes undertaken by the ACCC to analyse the impact of any proposed amendments to the CDR Rules.
PIA Update 3 Report	means this the third updated privacy impact report prepared by Maddocks.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Safeguards	means the provisions in Subdivision B to F of Division 5 of Part IVD of the CC Act.
Sector	means a Sector that has been designated to be subject to the CDR regime.
Service Data	means CDR Data that was disclosed to a CDR Representative for the purposes of a CDR Representative Arrangement, or directly or indirectly derives from such CDR Data.
Sponsor	means a person with unrestricted accreditation under rule 5.1A of the proposed CDR Rules.
Sponsorship Arrangement	means an arrangement between an Affiliate and a Sponsor for the purpose of the Affiliate accessing CDR Data.

Treasury	means the Department of the Treasury.
Trusted Adviser(s)	has the meaning in Rule 1.10C of the CDR Rules

Part G LIST OF SUBMISSIONS

We reviewed submissions from the following entities who submitted a response to Treasury's call for submissions on an exposure draft of the proposed amendments to the CDR Rules. Please note entities that have been grouped together submitted a joint submission.

1. Afterpay
2. FinTech Australia;
3. Financial Data and Technology Association;
4. The: Financial Rights Legal Centre, Consumer Action Law Centre, Australian Privacy Foundation, Public Interest Advocacy Centre, Australian Privacy Foundation and Australian Communications Consumer Action Network;
5. Illion;
6. Yodlee;
7. Australian Competition & Consumer Commission;
8. Office of the Australian Information Commissioner;
9. Origin Energy;
10. Cuscal;
11. Australian Banking Association;
12. Adatree;
13. National Australia Bank;
14. Commonwealth Bank;
15. Energy Australia;
16. Customer Owned Banking Association;
17. Salestrekker;
18. TrueLayer;
19. Loan Market Group;
20. Council of Small Business Organisations Australia;
21. SISS Data Services;
22. American Express;
23. Tax Practitioners Board;

24. RSM Australia;
25. Consumer Policy Research Centre;
26. Visa;
27. Mastercard;
28. Astero;
29. Australian Retail Credit Association;
30. Digital Service Providers Australia New Zealand;
31. Biza;
32. Regional Australia Bank;
33. Australian Finance Group;
34. Alinta;
35. Quantium;
36. Australian Small Business and Family Enterprise Ombudsman;
37. Red Energy and Lumo Energy;
38. ANZ;
39. Frollo;
40. WeMoney;
41. Basiq;
42. Financial brokers Association of Australia;
43. Mortgage and Finance Association of Australia;
44. Chartered Accountants, CPA Australia, Institute of Public Accountants and the Institute of Certified Bookkeepers;
45. Energy Queensland;
46. AGL Energy;
47. Payble;
48. Bendigo Adelaide Bank;
49. Intuit;
50. Commercial and Asset Finance Brokers Association of Australia;
51. MYOB;
52. Xero;

53. AssuranceLab; and

54. The Centre for Financial Regulation and Innovation.