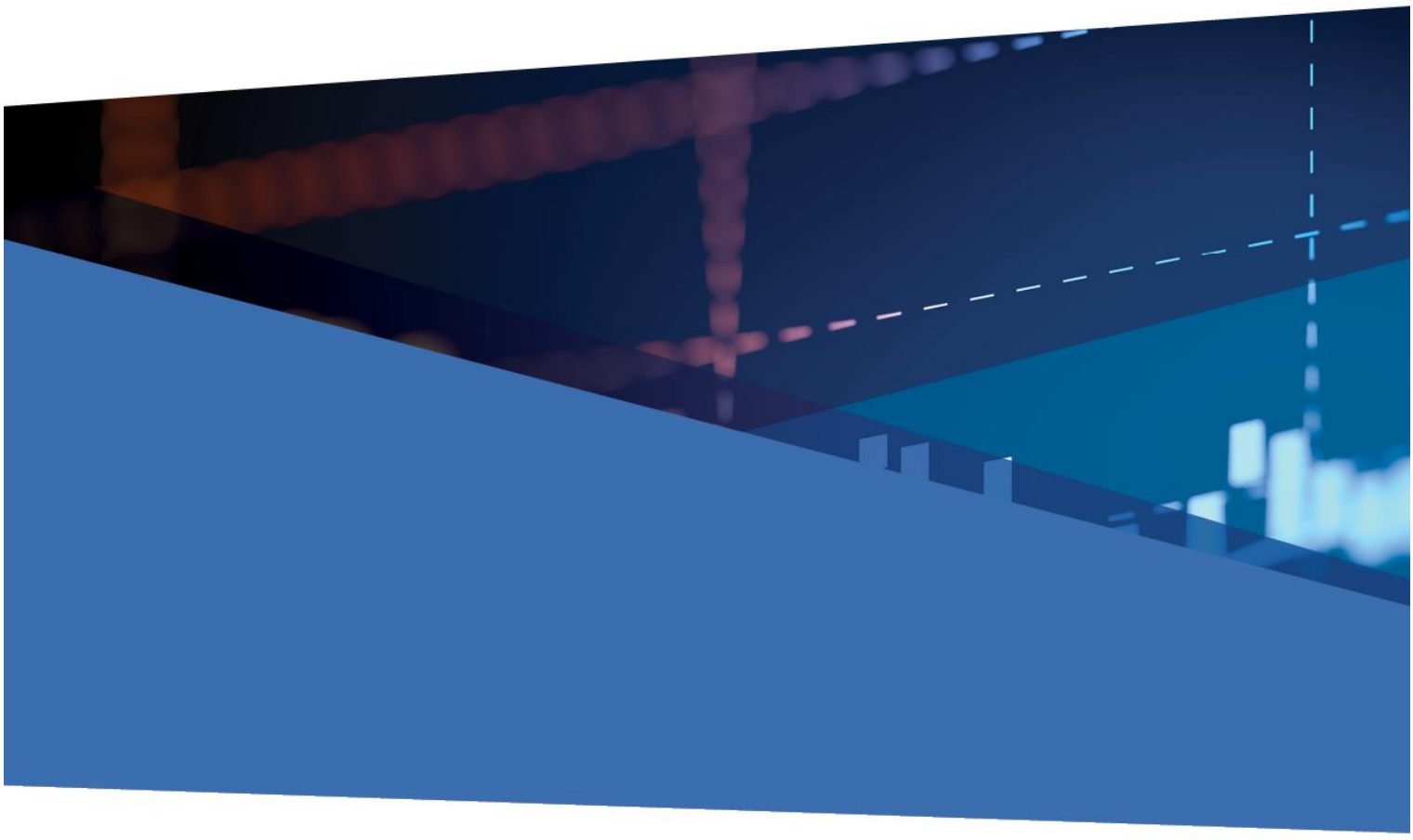
Australian Government
The Treasury

TSY/AU

CONSUMER DATA RIGHT

Privacy Impact Assessment Agency Response

October 2021



Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

TREASURY RESPONSE TO PRIVACY IMPACT ASSESSMENT - VERSION 3 OF THE CDR RULES

On 30 September 2021 the Minister made the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1). The amendments to the Consumer Data Right rules (**version 3 rules**) are an important step in increasing the ways businesses can participate in the CDR and enabling consumers to get the benefit of their data through an increased range of services.

This followed formal consultation on the exposure draft rules in July, which built on an informal joint consultation process conducted with the Data Standards Body on the design of rules and standards relating to changes to the joint account rules. The development of the rules was informed by extensive feedback from a range of stakeholders including banks, energy retailers, industry and professional bodies, fintechs, regulators, and consumer and privacy advocates.

The Privacy (Australian Government Agencies – Governance) APP Code 2017 requires a Privacy Impact Assessment (**PIA**) to be conducted for all high privacy risk projects, and must identify impacts on the privacy of individuals and set out recommendations for managing, minimising or eliminating that impact.

The likely effect of making the rules on privacy or confidentiality of consumers' information must be considered by the Minister before making rules. This must be considered alongside a range of other matters, including the likely effect of making the instrument on the interests of consumers, the efficiency of relevant markets, promoting competition, promoting data driven innovation, any intellectual property in the information to be covered by the instrument, the public interest, as well as the likely regulatory impact of the making of the rules.

Treasury engaged Maddocks to conduct a PIA for the proposed changes to assist the development of the version 3 rules and to inform the Minister's decision to amend the CDR rules. The PIA was informed by submissions to the exposure draft rules and a consumer privacy roundtable held on privacy issues relating to the proposed rules. The PIA was prepared on the basis that it was an update to previous PIAs Maddocks prepared in relation to earlier versions of the CDR Rules.

The final PIA and public submissions are now available on the Treasury website. The final PIA included 19 recommendations. This document provides an agency response to each of these recommendations.

Maddocks 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).

Agency response – **Noted**

In addition to the explanation of the intended operation of the rules in the Explanatory Statement accompanying the version 3 rules, regulatory guidance will be provided in relation to the new rules by the OAIC and the ACCC as relevant to their CDR regulatory functions.

Maddocks 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.

Agency response – **Noted**

The obligations in Schedule 2 require, as a default, an accredited data recipient to have in place security controls to encrypt data-in-transit in accordance with data standards (if any) and industry best practice. This would apply whenever an accredited data recipient makes a disclosure to another entity as permitted by the rules.

New rule 7.5(2)(a) requires disclosures to be done in accordance with data standards. This would require an accredited data recipient to comply with any standards that might be made by the Data Standards Chair in relation to secure disclosure of data to other entities, should such standards be made in the future. If such standards are made, they would apply in addition to the controls in Schedule 2.

Maddocks 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).
Agency response – **Not accepted** The classes of trusted adviser include professions that are regulated and subject to professional duties and oversight that provide an appropriate level of consumer protections. While many trusted advisers will be APP entities under the Privacy Act, requiring all trusted advisers to be subject to the Privacy Act may unduly impede consumer choice in circumstances where professional oversight and regulation exists.

Maddocks 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.
Agency response – **Noted** The rules require consumer experience (**CX**) standards to be made by the Data Standards Chair for the disclosure of CDR data to trusted advisers. CX data standards may also be made about the process for obtaining consents to disclose to trusted advisers. The Data Standards Body routinely conducts consumer research to assist the development of CX data standards. The rules do not preclude the Data Standards Chair from making CX data standards that differ based on the context in which the consent is sought.

Maddocks 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.
Agency response – **Accepted in part** The intended operation of the 'reasonable steps' provision is described in the Explanatory Statement accompanying the version 3 rules. This provides that a person is taken to be a member of a trusted adviser class for the purpose of the rules where the accredited person has taken reasonable steps to confirm that they are a member of the class. The reasonable steps that an accredited person may take to confirm that a nominated trusted adviser is a member of a trusted adviser class is a flexible concept that will depend on the circumstances. It may include seeking confirmation that the person is a member of trusted adviser class or some other form of representation from an adviser, or searching publicly available information.

Maddocks 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.
Agency response – **Not accepted** The intended operation of the rules for the disclosure of CDR insights is described in the Explanatory Statement accompanying the version 3 rules. The rules require CX standards to be made by the Data Standards Chair for the consent and disclosure of CDR insights. Treasury will support the OAIC and the ACCC as needed in the preparation of guidance related to their functions.

Maddocks 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.

Agency response – **Not accepted**

The CDR insights model allows consumers to consent to insights generated or derived from CDR data being shared outside the system for a range of prescribed purposes. The rules also facilitate informed consumer consent by requiring CX standards to be made to ensure consumers understand the nature of the information they are agreeing to disclose outside the CDR regime.

Maddocks 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.

Agency response – **Accepted in part**

The rules require CX standards to be made in relation to disclosure of insights to ensure consumers properly understand the nature of the information they are agreeing to disclose as an insight and that their data will leave the CDR system when disclosed. They do not preclude the Data Standards Chair from making CX data standards that differ based on the context in which the consent is sought. Additionally, the Data Standards Body routinely conducts consumer research to assist the development of CX data standards.

Consent dashboards allow a consumer to easily track how they have shared their CDR data. Requiring the consumer to be shown the CDR insight before it is disclosed may not aid consumer comprehension in all circumstances.

Maddocks 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.

Agency response – **Noted**

The Data Standards Body routinely conducts consumer research to assist the development of data standards as appropriate.

Maddocks 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.
Agency response – **Noted** Treasury will support the OAIC and the ACCC as needed in relation to the preparation of guidance relating to their functions.

Maddocks 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).
Agency response – **Not accepted** Any use or disclosure by a CDR representative is taken to have been by the unrestricted accredited data recipient principal, including those that occur outside the scope of the CDR representative arrangement. Principals are therefore incentivised to ensure CDR representatives only make permitted uses or disclosures of CDR data, as they would be liable for contraventions of Privacy Safeguard 6 in the event of any non-permitted uses or disclosures.

Maddocks 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.

Agency response – **Not accepted**

The liability framework for the conduct of CDR representatives ensures that it is incumbent on the principal to ensure CDR representatives do not use or disclosure data when there is no legal basis for them to do so (i.e. where consent has been withdrawn).

Maddocks 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.

Agency response – **Not accepted**

See Recommendation 12 response. A principal is in breach of the rules if it does not direct its representative to cease (or the representative does not cease) using data when there is no longer a relevant consent. Similarly, if the principal does not direct the representative to delete data, or the representative does not delete data in response to the instruction, in accordance with the rules, the principal is in breach of the rules.

Maddocks 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).

Agency response – **Not accepted**

The consumer privacy protections provided to joint account holders have been considered carefully and have been balanced with the other statutory factors that must be considered in relation to the making of the CDR rules. The single consent model has privacy-enhancing features compared to data sharing on joint accounts that exists outside of the CDR. The CDR provides a safe and secure means of sharing data and also provides consumers with control and visibility over data sharing that does not exist outside of the CDR. In particular, data holders must provide notifications that ensure all joint account holders are aware of when sharing arrangements commence, are amended or cease.

Introducing a delay in data sharing to give time for the other joint account holder(s) to either agree to or disagree to the proposed sharing would be technically complex and would not achieve the intended policy outcome of ensuring that joint account data sharing is convenient for consumers and does not impose undue friction.

Maddocks 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.
Agency response – **Not accepted** The rules provide exceptions to the joint account provisions that data holders can rely on where they consider it necessary to prevent physical, psychological or financial harm or abuse. Making this rule more prescriptive by specifying a standard to which the Data Holder must be satisfied that the joint account holder is at risk of harm would increase complexity of this provision and consequentially risk poorer outcomes for consumers.

Maddocks 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).
Agency response – **Noted** Treasury will support the OAIC and the ACCC as needed in relation to the preparation of guidance relating to their functions.

Maddocks 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.
Agency response – **Not accepted** Following consultation Treasury considers that a specific consumer awareness campaign in advance of the single consent model commencing in CDR would create undue confusion for consumers having regard to the nature of data sharing that currently occurs in relation to joint accounts now outside of the CDR and because it would occur without the context of a consumer commencing a CDR data sharing process.

Maddocks 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.
Agency response – **Accepted in part** The rules enable data standards to be developed about how data holders must present information to consumers about managing their notification preferences. The rules also require data holders to allow consumers to reverse any decision relating to their notification preferences. With respect to including requirements to regularly remind consumers about disabled notifications and prompting consumers to reconsider their decision, this is likely to undermine consumers' preference to receive fewer notifications, and may contribute to 'notification fatigue'.

Maddocks 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).
Agency response – **Noted** The amended rules allow for sector-specific rules to be made in relation to joint accounts.