Australian Banking Association

30 July 2021

Ms. Kate O'Rourke
First Assistant Secretary
Treasury Consumer Data Right Division
By email: data@treasury.gov.au

Dear Kate

Consumer Data Right rules amendments (version 3) consultation

The Australian Banking Association (**ABA**) makes this submission in response to Treasury's consultation, Consumer Data Right rules amendments (version 3) (**draft Rules 3.0**).

ABA notes the intention of draft Rules 3.0 is to promote growth of the Consumer Data Right (**CDR**) by offering new alternative pathways for entities to participate as recipients of CDR data. Whilst the ABA fully supports the growth of the CDR, we are deeply concerned that Treasury's proposals are unjustifiably detrimental to consumer choice, a consumer's control over their data and privacy, data security and most importantly weaken consumer protections.

Consumers who choose to share their data through the CDR presently have protection that their data is securely transferred and stored. This is because CDR data is governed by the Privacy Safeguards and the method of data transfer has been built in accordance with appropriately specified information security standards.

The ABA has considered the four expansion arrangements proposed by Treasury: Affiliate-Sponsor, Principal-Representative, unaccredited Outsourced Service Provider, and Trusted Adviser. The ABA does not support the proposals, as none of the four models proposed provide sufficient levels of consumer or data protection.

The four proposals, fail to meet core consumer protection parameters, namely:

- 'Foundational Consumer Protection Measures'
    - Appropriate obligations under the Privacy Safeguards
    - Obligations to maintain information security standards appropriate for banking data

- Supporting Consumer Protection Measures
    - Clear liability framework which leaves the consumer in no doubt as to which entity is accountable for any losses the consumer may incur.
    - Defined complaints processes.
    - Specified required insurances.

The ABA's conclusion is that draft Rules 3.0 seeks to achieve growth through the unacceptable diminution consumer protections – the ABA does not support this proposed weaking of consumer protections. None of the four proposed arrangements provide sufficient level the foundational consumer protections measures mentioned above. Further, draft rules 3.0 introduces and relies on incomplete secondary consumer protection measures to mask the absence of the foundational consumer protection measures. The proposed secondary consumer protection measures should not and cannot be the first line of defence for consumer banking data.

Australian Banking Association

Each of the proposals are flawed and present an unacceptable risk to consumers, their data, and the success of the CDR, for example:

- Affiliate-Sponsor arrangement lacks the obligation for the secure transfer of data between Sponsor and Affiliate.
- Principal-Representative arrangement makes no obligation for the Representative to adhere to the Privacy Safeguards or information security standards.
- The unaccredited Outsourced Service Provider arrangement is especially concerning because secure banking data will be accessed directly from the data holder by an entity that is not held accountable under the Privacy Safeguards nor obligated to maintain the information security standards of the CDR.
- The Trusted Adviser arrangement makes no obligations on Trusted Advisers for CDR data.

In this submission, the ABA makes several recommendations in respect to building the consumer protections of the first three arrangement types. However, it is the firm view of the ABA that the Trusted Adviser arrangement poses significant risk to consumer banking data and should not proceed. Within seconds, under draft Rules 3.0, a customer's data will travel from the most secure setting at the bank to no or uncertain security with Trusted Advisers. The ABA recommends the Trusted Adviser arrangement be deemed a particular use-case under of the Principal-Representative arrangement - provided the recommended enhancements to the foundational consumer protection measures are enacted for that Principal-Representative arrangement. As an advocate for the CDR, a laudable government initiative, the future of the CDR is in lifting the standards of data sharing to underpin a safe and secure digital economy.

In respect to opt-out model for joint accounts, the ABA reaffirms our strong opposition to Treasury removing the rights of certain Australians to fully control where their data is shared. Further detail of this ABA position is contained in our submission of 26 May 2021, which was in response to the first Treasury consultation *Opt-Out Joint Accounts Data Sharing Model*[1]. The views of the ABA remain aligned with others who advocate for and represent the rights of ordinary Australians when it comes to their data and privacy.

The ABA accepts that the current method of consent for joint account is complex and can be improved, the ABA holds that improving the government's technical standards for joint account consent is the appropriate solution, not as Treasury propose, removing the right of certain Australians to have full control over their personal data and privacy. The ABA notes that should government proceed with this opt-out model for joint accounts – then in promoting the CDR, it can no longer claim that every consumer has full and equal control of their right to transfer their data to third parties of their choice. It is unreasonable and concerning the opt-out Rules are underpinned by a policy, that being married or opening a joint account would automatically remove some of the CDR rights that person had when unmarried with their own bank account.

The proposed opt-out model removes informed positive consent by consumers for less friction in the consent process. The Treasury proposal goes against the core principle of the CDR that consumers should be in control of their data. In addition to our 26 May submission the attachment to this letter includes additional concerns, including those relating to consumer privacy, both submissions should be read together.

The ABA recommendation remains that the current approach to joint account management be retained, and Treasury should allocate resources to improve the technical standards for joint account consent model. The CDR is a young technology, it is not unexpected that improvements need to be made to the customers' experience – but these improvements should not be detrimental to the security and data rights Australians now hold under the CDR

[1] https://www.ausbanking.org.au/submission/opt-out-joint-account-data-sharing-model/

The ABA recommends that with the growth of the ecosystem it is now the right time for Treasury to introduce the principle of reciprocity per Scott Farrell's recommendation 6.9, 'Accredited data recipients should be obliged to comply with a consumer's request to share data which is the subject of a sectoral designation as well as equivalent data held by them in relation to sectors which are not yet designated'[2] The ABA looks forward to this additional expansion of the CDR as soon as possible.

The ABA thanks Treasury for the opportunity to make this submission; we look forward to discussing this submission in further detail.

Regards,

Emma Penzo
Policy Director

[2] Scott Farrell ,2020, Future Directions for the Consumer Data Right.

Australian Banking Association

Annexure

1. ABA position on CDR security and consumer protection

The ABA supports the Government's objective to increase participation in the CDR and therefore to grow the data economy. We understand the intention of draft Rules 3.0 is to promote this growth by offering alternative mechanisms for entities to participate in the CDR. We note the four CDR growth principles used by Treasury in designing these new Rules include:

- Facilitate greater participation in the CDR regime by participants and consumers,
- Provide greater control and choice to consumers in sharing their data,
- Promote innovation of CDR offerings including intermediary services,
- Enable services to be more effectively provided to customers.

Consumer Protection

Whilst the ABA supports the growth principles, we are concerned that equal weight has not been given to these principles, particularly, providing greater control and choice to consumers and associated consumer protections. Consumers who choose to share their data through the CDR presently have protection that their data is securely transferred and stored because of the comprehensive and robust information security which comprises information security technical standards (**InfoSec Standards**) and their ability to control their data through reliance on the Privacy Safeguards.

For the purposes of responding to the consultation on draft Rules 3.0, the ABA has distinguished between two necessary layers of consumer protection: foundational; and supporting.

Foundational consumer protection measures are those which provide critical assurance to consumers regarding the security of their CDR data. Supporting consumer protection measures are those which provide essential assurance to all CDR participants, and therefore give indirect protection to consumers. Supporting measures alone are insufficient protections for consumers and should not be relied upon in the absence of foundational measures.

Foundational consumer protection measures: The ABA considers information security standards and the Privacy Safeguards as foundational consumer protections of the CDR (see table 1), which should not be diluted.

Table 1: Foundational principles for consumer protection in the CDR

Principle	Why it matters to consumers	When it goes wrong
InfoSec Standards	• Ensures that the consumer's data is safe and cannot be intercepted as it travels from data holder to accredited data recipient to the other participant • Ensure that the consumer's data cannot be stolen or tampered with when it is at rest at the other participant.	We refer to the cyber security incident that took place within Service NSW in September 2020 where the personal information of 180,000 customers was stolen from the email in-box of Service NSW staff. This example demonstrates the need for strong information security protocols and standards[3].
Privacy safeguards	The Privacy Safeguards establish the legal basis for use of consumer data	We refer to two recent relevant cases:

[3] https://www.service.nsw.gov.au/cyber-incident and https://www.abc.net.au/news/2020-09-07/service-nsw-customer-personal-details-hacked-in-security-breach/12637502

	can be by entities with which consumers have trusted their data. They include the InfoSec requirements set by Privacy Safeguard 12. The Privacy Safeguards provide consumers the right to withdraw consent if they are not satisfied with the service or the way their data has been used.	Queensland's law enforcement who used COVID-19 check-in data for purposes other than that for which it was intended[4]. A large technology company that was held to mislead consumers about the use of the personal location data[5].

Supporting consumer protection measures: The ABA considers that to ensure ongoing clarity, efficiency, and trust of the CDR, both consumers and CDR participants need the following supporting consumer protection measures to be clearly articulated under the proposed participation variations:

- Liability – when things go wrong the consumer and CDR participants need to know which party is to be held accountable.
- Complaint's process – CDR participants need to understand their obligations to establish and maintain internal complaints processes and record keeping. Consumers need to know which external dispute resolution body will accept consumer complaints involving other participants.
- Insurance – CDR participants need to know which insurances other participants are required to hold (for example, cyber security insurance).

ABA analysis of the draft Rules 3.0 indicates that the consumer protection measures set out above have not been extended to proposed participation variations (see table 2). Therefore, it is our view that the draft Rules 3.0 do not contain sufficient consumer protections or clarity.

Table 2: ABA analysis of consumer protection measures for the CDR

	Affiliate	**Representative**	**U-OSP [(3)]**	**Trusted Adviser**
Foundational consumer protection measures:				
InfoSec Standards	× insufficient	× absent	× absent	× absent
Privacy Safeguards	✓All PS[(1)]	× insufficient	× absent	× absent
Supporting consumer protection measures:				
Liability	× insufficient	✓ ADR obligation	✓ ADR obligation	× absent
Complaints	× unclear	✓ADR[(2)] obligation	✓ ADR obligation	× absent
Insurance	× unclear	× unclear	× unclear	× unclear

(1) PS refers to Privacy Safeguards (2) ADR, or accredited data recipient, under this arrangement is referred to as the 'Principal' (3) U-OSP refers to unaccredited outsourced service providers.

Security of Banking Data

The ABA notes the diminishing quality of security for banking data in the CDR under the proposed draft Rules 3.0. Australian banks are required to maintain the strictest standards of data security under APRA's Prudential Standard CPS 234 Information Security (**CPS 234**).

The current rules associated with Privacy Safeguard 12 maintain the requirements of CPS 234. However, draft Rule 3.0 removes security standards to varying levels for banking data in respect to the proposed participation variations. Within seconds, under the draft Rules 3.0 a customer's data will travel from the most secure setting at the bank to no security in some circumstances (i.e., Trusted Advisers).

[4] https://www.themandarin.com.au/161713-whos-been-looking-at-your-check-in-data-we-asked-the-states-and-territories-to-fess-up/
[5] https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data

Australian Banking Association

Additionally, under CPS 234 banks have an obligation to '*assess the information security capability of [the third party] managing the information assets of the bank*' (paragraph 16). Also, banks '*must have information security controls to protect [their] information assets, included those management by ….third parties*' (paragraph 21). The proposed arrangements in draft Rules 3.0 (Affiliate-Sponsor, Principal-Representative, Trusted Adviser) creates a daisy-chaining of consumer banking data where once the data is shared beyond the accredited data recipient, banks will potentially by unable to fulfil prudential obligations.

The ABA notes the perspective that banks already permit their customers to download and share their data with third parties through CSV files and that Rules 3.0 is an extension of what banks already permit. It is our view that:

- this is a limited interpretation of these existing data sharing arrangements and the two cannot be equated. Draft Rules 3.0 is a government mandate for mass[6] bank data sharing under limited or no prescribed security requirements and introduces the potential for systemic misuse, including cyber risk, for banking data. On the other hand, bank's bespoke provision of data downloads for individual customers data is more akin to what CDR 'direct to consumer' was envisaged to be.
- as a government system, the CDR should be lifting the standards of data sharing to underpin a safe and secure digital economy.

We highlight the present reforms of the Department of Home Affairs to strengthen cyber security regulation of critical economic sectors, including the banking sector. This is part of the whole of government cybersecurity strategy 2020. As part of these reforms, the Department of Home Affairs has recognised the need to address cybersecurity of third-party service providers for these critical sectors – which would include entities that can access and use banking data. Data storage and processing has also been recognised as a critical sector in its own right, highlighting the importance of data and infosec in protecting Australian people's trust in critical sectors. It is possible the CDR participants which ingest banking data will be captured under these reforms.

Much effort has gone into establishing a CDR which consumers can trust. To avoid undermining this trust, the ***ABA's overarching strong recommendation is that that draft Rules 3.0 require further revision to ensure the minimum consumer protections represented by the foundational and supporting consumer protection measures are maintained in the CDR. Further, the ABA strongly suggests Treasury consider the cybersecurity requirements under development by the Department of Home Affairs***.

The remainder of this annexure will present more detailed recommendations.

2. Information security requirements

Appropriate information security standards, or the ecosystem trust framework is an important element of the digital economy. It is how people and businesses have confidence that their data (and eventually financial and non-financial actions) are travelling within secure parameters to people or entities, with the appropriate data transport and storage security protocols.

It is important that security risks are adequately managed. There is ample precedent for an entire ecosystem to align to one security management standard. For example, the Payment Card Industry Security Standards Council (PCI DSS)[7] sets information security standards for credit card numbers (called PANs or Primary Account Numbers) for the global cards industry. This ensures that all parties in that ecosystem know that cardholder data is protected globally. The ABA's view is that the CDR data should be no different. Entities that are unable to implement and maintain the information security

[6] Draft Rules 3.0 support mass bank data sharing on three levels (a) At the consumer level, the rules are a continuation of coarse-grained consent which means that select data sets cannot be sent by the consumer. Fine grained consent is required for consumers to control their data. (b) At an accredited data recipient level, where accredited data recipients support millions of customers (c) at the ecosystem level CDR is envisaged to be economy-wide multi-sectoral.

[7] https://www.pcisecuritystandards.org/

standards should consider participation in the CDR through aligning with an accredited data recipient who can provide data access without that data leaving the ecosystem.

For trust to prevail in the CDR, appropriately calibrated InfoSec requirements must be mandated. The InfoSec requirements should apply to all CDR participants, and interactions and data protection requirements.

Even if data protection controls are in place (e.g.: data encrypted in transit and at rest), we note that there is still a significant risk exposure without Infosec Standards for how CDR banking data is transferred and handed over (also referred to as 'integration'[8]) between accredited data recipients and other accredited data recipients, Affiliates, Representatives, unaccredited Outsourced Service Providers, or Trusted Advisers. This means that less secure mechanisms such as, email[9], batch feeds, and insecure APIs, are deemed by government to be acceptable mechanisms for accredited data recipients to share business and consumer banking data through the CDR. The ABA urges Treasury to ensure the security of banking data by incorporating principles-based standards for secure data transfer between all participants of the ecosystem.

In respect to data encryption at rest and in transit, these are important controls that do not cover integration requirements for Affiliate, Representative, unaccredited Outsourced Service Provider, or Trusted Adviser. The lack of information security profile for these participants' data sharing practices exposes CDR banking data to hackers and other cybersecurity risks. We note that even with the benefit of contractual arrangements between Affiliates, Representatives, unaccredited Outsourced Service Providers, Trusted Advisers, and accredited data recipients, this will be little comfort to a consumer whose data has been stolen. This situation is exaggerated by the lack of fine-grained consent: up to seven years' worth of data can be retrieved and stolen even if a consumer was consenting to a use case that requires only the transactions of the last 24 hours.

The Explanatory memorandum states:

> *The models are also designed to maintain trust and confidence in the CDR because any use or disclosure of CDR data by sponsored affiliates, CDR representatives or OSPs is subject to the same requirements and protections that apply to unrestricted accredited persons. (P4)*

The ABA does not agree with this statement; the analysis following will show that banking data (to the extent that it is transited and handled by Affiliates, Representatives, unaccredited Outsourced Service Providers, and Trusted advisers) is not subject to the same requirements as accredited data recipients and in some cases the data is subject to no requirements to protect consumer banking data.

This lack of information security is not commensurate with the risks associated with the banking data to be accessed by such entities.

Recommendation 2.1: All CDR which is transferred between accredited data recipients and other entities (e.g.: to other accredited data recipients, Affiliates, unaccredited Outsource Service Providers, Representatives, Trusted Advisers) be subject to integration requirements which will ensure CDR data is protected by the same level of API security throughout the 'daisy-chain' where that data is passed from accredited data recipients to other recipients.

The ABA understands that much of the impetus for the proposed changes is the result of feedback that it is too costly for participants to meet the InfoSec Standards of the CDR. There are two aspects to the costs: the build costs and the accreditation costs of the infosec standards.

In respect to the high build costs of the Infosec Standards, a key driving factor is the non-standard prescription of the CDR Infosec Standards:

[8] Integration is a technical term for giving or passing of data from one part to another.
[9] Refer to Table1 where a government agency exposed customer data held in emails to hackers.

- This leads to implementation complexity for both accredited data recipients and data holders.
- These require accredited data recipients to host APIs together with authentication and authorisation requirements

The non-standard prescription adds cost and complexity for the builds of data recipients because global vendors may not support custom Infosec Standards for what is presently a small ecosystem. Further, the current prescription is considered insecure by global infosec standards setting bodies which creates a negative feedback loop in respect to vendor support[10].

Whilst implementation costs of the information security standards will vary according to size and complexity of each entity, it is our understanding that accreditation with global technical standards bodies will cost circa $2,000-$3,000. This appears to be a modest amount to ensure uniform standards of information security implementation for consumers and participants of the ecosystem

Recommendation 2.2: The ABA recommends prescription of globally recognised Infosec Standards for the CDR. Further, we invite Treasury and Maddocks to review the ABA submission to GitHub Decision Proposal 182 which can be found on the GitHub Consumer Data Standards site here or the ABA website here as it discusses the significance of an appropriately designed and implemented InfoSec framework.

Draft Rules 3.0 seeks to achieve growth through the diminution of the security of consumer banking data. We question the proposal to enable entities which do not have capacity to maintain security levels appropriate for banking data being given relatively unrestricted access to that data.

Following is the ABA's analysis, position, and recommendations regarding the InfoSec Standards obligations for each of the accreditation and data sharing arrangements presented in draft Rules 3.0.

Affiliates

The ABA notes Division 8.4 Rules 8.11 does not specify InfoSec standards for Affiliates. Further Rule 2.2 table item 7 requires a 'third-party management framework' but does not specify InfoSec requirements for Affiliates. The Explanatory Memorandum states that 'an affiliate will not be required to provide an assurance report to establish that it meets the information security criterion once accredited'[11], and instead are required to self-assess and provide attestation statements every two years.

The prescribed self-assessment and self-validation, which involve no InfoSec requirements, and are required once every two years, is inadequate security for banking data, where InfoSec security standards require evolution to keep pace with cybercrime techniques.

On this basis, the ABA does not consider the security standards for Affiliates, set out in Rules 3.0, to be adequate.

Recommendation 2.3: The ABA strongly recommends that affiliates be subject to CDR Infosec Standards for the transmission and storage of CDR data.

Representatives

Disclosure of CDR data in a Principal-Representative arrangement is subject to contractual arrangements between the Principal and Representative under Rule 1.10AA(2)(c)(iii). The transmission of CDR data is not required to be undertaken in accordance with the InfoSec Standards of the CDR. Therefore, CDR data will exit the protection of the CDR for the period it is in transmission between the Principal and the Representative and when it is at rest with the Representative.

[10] The ABA recognises the time constraints under which the ACCC, Data Standards Body, and the major banks were under in standing up the ecosystem and this discussion is not intended as a critique of that effort. To the contrary, the ABA recognises the efforts of all involved in bringing to life the CDR.
[11] Exposure Draft Explanatory Materials, p24. Also see Rules Schedule 1, rule 2.1.

Representatives have no legislative or regulatory obligation under the CDR to protect the data of consumers. We note that the Principal is 'liable' for the Representative and therefore some protections will be afforded to the consumer. As this arrangement relies on supporting consumer protections and not foundational consumer protection measures to provide protection to consumer data, the ABA considers the InfoSec standards of this arrangement to be insufficient.

Recommendation 2.4: The ABA strongly recommends that Representatives be subject to CDR Infosec Standards for the transmission and storage of CDR data.

Outsourced service providers

Draft rules 3.0 is intended to 'allow ADRs to use the services of an unaccredited Outsourced Service Provider to collect data directly from a data holder on their behalf'.[12] Data holders will be obligated to provide consumer banking data to entities which have no legislative obligations to treat the data in a manner which is appropriate to the risk rating of banking data.

Further, the data holders have no way of knowing that the unaccredited Outsourced Service Provider will pass the data directly to an accredited data recipient. We consider this arrangement to be extremely high-risk as there are no Infosec Standards protecting the data as it leaves the data holder. For this reason, the ABA has assessed this arrangement to be inadequate.

Recommendation 2.5: The ABA strongly recommends that unaccredited Outsourced Service Providers be subject to CDR Infosec Standards for the transmission and storage of CDR data.

Trusted Adviser

Draft Rule 8.11(1)(iv) provides that Trusted Advisers are to receive CDR data in accordance with the consumer experience data standards. The ABA agrees that it is important for data to be presented in an accessible form, however, it is more important for that data to be received and held at rest with the appropriate Infosec Standards. As the draft rules 3.0 does not specify InfoSec obligations for Trusted Advisers the ABA considers this inadequate protection for consumers.

Recommendation 2.6: The ABA strongly recommends that Trusted Advisers be subject to CDR Infosec Standards for the transmission and storage of CDR data.

3. Privacy Safeguards

The Privacy Safeguards are important consumer data protection mechanisms of the CDR. The ABA considers that the Privacy Safeguards in whole or part ought to apply to all participants subject to the nature of their use of the CDR data.

Affiliates

The ABA supports the requirements in the draft rules for affiliates to be subject to all the Privacy Safeguards.

Representatives

The ABA supports the identified privacy safeguards for Representatives. However, Representatives may contract the services of overseas service providers and the privacy requirements under this scenario are unclear.

Recommendation 3.1: The ABA recommends that Representatives be required to comply with Privacy Safeguard 8, in addition to the safeguards proposed in the draft rules.

[12] Exposure Draft Explanatory Materials, https://treasury.gov.au/sites/default/files/2021-06/187223-cdr_rules_amendments_em.docx p12

Unaccredited Outsourced service providers

The ABA notes that unaccredited Outsourced Service Providers are not obligated to adhere to the Privacy Safeguards, a foundational consumer protection measure. Despite the unaccredited Outsourced Service Providers being under contractual obligation to the accredited person or accredited data recipient, such arrangements are supporting consumer protection measures and should not be relied upon as the primary mechanism for consumer protection. It is particularly concerning that unaccredited Outsource Service Providers will be able to access data from the data holder. Consumer protection should be strengthened so that unaccredited Outsourced Service Providers are also under regulatory obligation to protect CDR data.

Recommendation 3.2: The ABA recommends that, where relevant, unaccredited Outsourced Service Providers to be required to comply with Privacy Safeguards 4, 6, 7, 8, 12. In particular, unaccredited Outsourced Service Providers should be required to:

- ***take steps to protect the data (including Schedule 2 Minimum information security controls)***
- ***not disclose the service data other than in accordance with the contract with the accredited data recipient***
- ***delete service data when directed to by the accredited data recipient and provide records of the deletion***
- ***adopt and comply with the accredited data recipient's CDR policy in relation to the service data.***

Trusted adviser

Trusted advisers, under draft Rules 3.0, will have no legislated obligations to maintain the privacy of customer data beyond the Privacy Act 1988 (Cth). Treasury representatives explained that they believe that the existing obligations of being a professional and the requirements of the profession to keep their customer's data safe would be sufficient[13]. It is noteworthy that the Privacy Safeguards were developed because the Privacy Act 1988 (Cth) did not provide sufficient protections for consumers' data. We consider this to be a significant degradation of consumer data privacy rights.

Recommendation 3.3: The ABA recommends that Trusted Advisers to be required to comply with the Privacy Safeguards, especially Privacy Safeguard 12.

4. Consumer dispute resolution

The ABA notes that from 5 October 2022 ASIC will withdraw Regulatory Guide 165 Licensing: Internal and external dispute resolution (**RG 165**) when Regulatory Guide 271 Internal dispute resolution (**RG 271**) will become effective. Unless updated, the CDR Rules will potentially be without an internal dispute resolution mechanism.

In respect to the current requirements under RG 165, it is the view of the ABA that the internal dispute resolution rules (Schedule 3 Part 5) will require amendment and possibly, reconsideration. The CDR Rules for complaints are based on RG165. RG 165 in turn mandates both internal and external complaints mechanisms. However, as many of the new entities (Trusted Advisers, Affiliates, Representatives, or unaccredited Outsourced Service Providers) which are to be in receipt of CDR data are not ASIC regulated nor within the remit of AFCA, it is unclear what arrangements will be in place for consumer complaints. Clarity will be required for participants and consumers.

Recommendation 4.1: The ABA recommends:

- ***Treasury update the CDR rules relating to consumer complaints to reflect the changes introduced by RG 271 and consult on those changes.***

[13] Treasury presentation during the Data Standards Body's weekly call on 22 July outline draft Rules 3.0

- ***All participants (including Trusted Advisers, Affiliates, Representatives, and unaccredited Outsourced Service Providers) be required to implement internal consumer complaints mechanisms which are compliant with RG165/RG 271***
- ***All participants (including Trusted Advisers, Affiliates, Representatives, and unaccredited Outsourced Service Providers) be required to be members of an appropriate external complaint resolution body.***

Recommendation 4.2: Consumers a given clarity in respect to which entity to hold accountable for losses experienced from the misuse of their CDR data.

5. Liability

Affiliate-Sponsor

The draft Rules 3.0 provides that it is possible for an affiliate to remain accredited for up to 4 months without a sponsorship agreement (Rule 5.1b). During this time, the affiliate is unable to access consumer data. However, the status of the consumer data already in the affiliate's possession and the affiliate's relationship to the customer is unclear. The ABA's view is that the liability structures for the Affiliate-Sponsor arrangement require further development.

Recommendation 5.1: The ABA recommends the Rules clarify the following:

- ***What is the responsibility and liability of the Affiliate and the former Sponsor during the period of the sponsorship gap?***
- ***What is the process for closing out a sponsorship agreement where (a) the Affiliate will close business (b) where the Affiliate will change Sponsors (c) under scenario (b) what is the ongoing liability of the first and subsequent Sponsors?***
- ***The Rules clearly state that data holders are not liable for the loss of data or loss to consumers resulting from the data sharing activities of Sponsors and Affiliates.***

Principal-Representative

We understand that under this arrangement, the Principal will be held responsible for the actions and any failures on the part of the Representative. This arrangement is simple for the consumer to understand; if the consumer is to suffer any losses due to the actions of the Representative, the consumer can seek recourse from the principal. The ABA supports the liability structure of the Principal-Representative arrangement.

Recommendation 5.2: The ABA strongly recommends that the Rules clearly state that data holders are not liable for the loss of data or loss to consumers resulting from the data sharing activities of Principals and Representatives.

Outsourced service provider

Although the Exposure Draft Explanatory Materials does not explicitly state the policy that the accredited recipient is fully liable for the actions (and inactions) of the unaccredited outsourced service provider, we assume this to be the case from the example with FinHealth (an accredited person) and iService (an unaccredited outsourced service provider)'[14]. The ABA supports the liability structure of the accredited recipient-unaccredited Outsourced Service Provider arrangement.

[14] Exposure Draft Explanatory Materials, p13

Recommendation 5.3: The ABA strongly recommends that the Rules clearly state that data Holders are not liable for the loss of data or loss to consumers resulting from the data sharing activities of accredited persons/accredited data recipients and outsourced service providers.

Trusted Adviser

The Trusted Adviser arrangement is discussed in detail in section 7, including the liability model.

6. Insurance

None of the new participants are obligated to hold insurance under draft Rules 3.0. business insurance is an important secondary consumer protection which consumers can rely on when things go wrong.

Recommendation 6.1: The ABA recommends that all participants (including Affiliates, Representatives, unaccredited Outsourced Service Providers, and Trusted Advisers) be required to hold cyber security insurance as a minimum.

7. Trusted Adviser

The ABA supports an ecosystem with multiple participant categories which are each subject to the foundational consumer protection measures and where supporting consumer protection measures are clearly specified. It is our view that the Trusted Adviser arrangement as specified in draft Rules 3.0 does not meet these minimum requirements.

Consumer privacy

The consumer's agency is not evident under this arrangement. Rule 1.10C states this arrangement will trigger when an 'accredited person … invite(s) a CDR consumer to nominate…trusted advisers.' It is unclear how this rule will operate in practice as the only way for this rule to operate is if an accredited person and a Trusted Adviser agree in advance that a customer should receive an invitation to engage with their Trusted Adviser. This arrangement raises a significant questions of consumer agency: On what terms would an accredited person have a detailed enough relationship with a CDR customer to understand the customer's needs so that the accredited person could then invite the customer to ask a Trusted Adviser to resolve their needs through the services of the accredited data recipient? It is unclear how this rule will apply without a impinging on the consumer's privacy.

Recommendation 7.1: ABA recommends Maddocks undertakes are review of the information flows assumed in Rule 1.10C and supporting rules.

Information security

In the normal course of events, when a consumer downloads their banking data from their internet banking and sends it to their 'trusted adviser', they do so on the basis that they have vetted that adviser. This is not the same relationship as the CDR Trusted Adviser where that entity is afforded legislated status as an entity that can be trusted.

As stated in section 2 of this paper, under the Trusted Adviser arrangement, CDR data travels from a state of security with banks (under APRA data security requirements) to no security (under a CDR legislated status that certain professions are to be trusted). The lack of security is apparent for both data in transit as well as data stored by the Trusted Adviser. The ABA does not support degradation in the level of InfoSec standards of banking data.

Refer to recommendation 2.6.

Privacy safeguards

It is unclear what obligations the Trusted Adviser will have in respect to the treatment and storage of CDR data once that data is outside the CDR. The Privacy Act 198 (Cth) was deemed insufficient for the protection of CDR data, leading to the development of the Privacy Safeguards. It is the ABA's view that Trusted Advisers should be accountable under all the CDR Privacy Safeguards.

Refer to recommendation 3.3.

Professions

If the term 'Trusted Adviser' is to be legislated and therefore receive government endorsement, it is the ABA's view that it should only be extended to those professions which fulfil the generally accepted elements of a profession: a professional body which registers members, members become accredited after extensive degree level or specialist training, members are required to undertake continuing professional training or education to maintain their membership, appropriate consumer complaints mechanism is in place, appropriate disciplinary mechanism exists for members who do not uphold the values and standards of the profession.

Further clarity is required regarding the scope and timing of obligations for an accredited data recipient to check a relevant person is a professional, i.e., meets the definition of Trusted Adviser. Accredited data recipients should be responsible for ensuring the continued registration and good standing of the Trusted Adviser.

Accredited data recipients have raised concerns about their ability to confirm whether the persons or entities they will share consumer data with are (and continue to be) registered in their professions. The ABA would be concerned if Treasury diminishes further the controls on Trusted Advisers by not mandating accredited data recipients take responsibility for the entities with which they share consumer data.

Recommendation 7.2: The ABA recommends for professions to be eligible for Trusted Adviser status, that they meet the generally accepted definition of a profession.

Recommendation 7.3: The ABA recommends accredited data recipients are to be responsible for undertaking on-going due diligence to ensure the eligibility of a professional to be deemed a CDR Trusted Adviser.

Liability

The ABA notes that Trusted Advisers carry no liability in the CDR. Draft Rules 3.0 make it the responsibility of the consumer to ascertain who is a 'Trusted Adviser'. However, this will likely not be the consumer's understanding as they will likely rely upon the government regulated status of 'trusted' in sending their data through the CDR to these entities. Consumers will have no way of knowing that they cannot rely on a breach of the CDR InfoSec standards, nor will they know that they do not have the privacy safeguards for remedy because Trusted Advisers are not obligated to adhere to these foundational consumer protection measures.

The ABA considers the liability framework for the Trusted Adviser to be inadequate.

Further, we note that Trusted Advisers are not typically independent businesses but rather have their business operations tightly coupled with accredited data recipients. In order for a Trusted Adviser to receive data from an accredited data recipient, it must have a pre-existing contractual relationship with the accredited recipient, it must also have pre-existing data links to the accredited data recipient. This relationship is the like that of Principal-Representative. There does not appear to be any distinguishing features to warrant a Trusted Adviser arrangement.

Recommendation 7 4: The ABA recommends that the Trusted Adviser arrangement be treated as special case of a Principal-Representative arrangement.

Recommendation 7.5: the ABA recommends that the liability structure of the Principal-Representative arrangement be applied to the Trusted Adviser arrangement.

Recommendation 7.6: The ABA strongly recommends that the Rules clearly state that data holders are not liable for the loss of data or loss to consumers resulting from the data sharing activities of accredited persons/accredited data recipients and Trusted Advisers.

8. CDR Insights

The ABA raises two matters in respect to CDR insights.

First, we query whether the specified person for CDR insights can be the accredited data recipient itself? We note this because the CDR insights rule might create an inconsistency in the rules between insights generated by accredited data recipients versus insights procured from accredited data recipients via an insight consent if this case isn't allowed.

Recommendation 8.1: The ABA recommends clarification in respect to whether the specified person for CDR insights can be the accredited data recipient.

Second, the definition of 'CDR Insight' (Rule 1.1(1)) permits raw CDR data to be shared with unaccredited persons without the protection of the Privacy Safeguards. The ABA does not support the passing of raw CDR data as a 'CDR Insight'. Further, the consumer's right in respect to the CDR insight is unclear if they disagree or dispute the insight.

Recommendation 8.2: To avoid risk of disclosure of sensitive information, that a CDR Insight be redefined as processed output of raw CDR data and that the definition incorporates the data minimisation principle to ensure that only the required amount of insight data is sent.

Recommendation 8.3: The rules should clarify consumer's right to challenge and request deletion of the insight.

9. Joint accounts

The ABA considers the draft Rules 3.0 joint account proposal will contribute to diminished consumer confidence in the CDR, which is contrary to the purpose of promoting competition based on consumer confidence in a secure sharing mechanism. It is our view that this proposal will:

- Diminish the core principle of the CDR, which is for consumers to be in control of their data. Automatic opt-in of a joint account diminishes the right of a person to provide positive consent to their data being shared.
- Cause confusion to customers with joint accounts. These customers have already received one set of rules on 1 November 2020, and they will now be told rules to the opposite effect in 2022). This confusion will likely be compounded to the extent that the joint account opt-in/opt-out rules are revisited for payment initiation in 2023.

The ABA considers the current requirements, with the addition of inflow elections, for Joint Accounts to be optimal.

Under the current requirements both parties consent to enable the account for sharing, and then sharing can take place by one party, or all parties (depending on their co-approval preferences). Further changes are not required to drive uptake, the CDR is a nascent ecosystem and it will take time for consumer uptake.

Recommendation 9.1: The current requirements for Joint Accounts with the Joint Account Management Service and the inflow election requirements be retained.

The remainder of this section discusses additional matters of concern in relation to the Joint Accounts prescription of draft Rules 3.0. Appendix 1 seeks clarity on detailed matters.

9.1 Consumer Privacy

The ABA has identified a number of consumer privacy issues with the opt-out model proposed in draft Rules 3.0. The following are based on a scenario where there are two joint account holders. Account Holder A provides to consent to share the data of the joint account; Account Holder B has not consented to the data share.

Issue 1: In the situation where under the proposed opt-out model, Account Holder A shares joint account transaction information with an Accredited Data Recipient who then on-shares the data with another accredited data recipient, or a Representative, Affiliate, or Trusted Adviser, Account Holder B will have no visibility of the on-sharing arrangements to entities beyond the accredited data recipient and the consequences of the use of their data by those entities.

Issue 2: It is not possible for the accredited data recipient to know which transaction data belongs to Account Holder A and Account Holder B. For example, if Account Holder A is sharing data to apply for an individual credit card, what data will be used in the assessment of the application? The consequences Account Holder B are unclear.

Issue 3: There is no mechanism for a joint Account Holder B to request the deletion of their data from the accredited data recipient and from the entities to which the accredited data recipient shared Account Holder B's data.

We refer to the ABA submission to the 'Opt-out joint account data sharing model – CDR rules and standards design paper[15] for a detailed discussion on the issues of the opt-out model.

The ABA considers that whilst controls can be implemented for these issues, that those controls will result in greater complexity to all participants and confusion for consumers.

Recommendation 9.2: The ABA refers Maddocks to the ABA submission to the 'Opt-Out joint account data sharing model' for consideration in the Privacy Impact Assessment for draft Rules 3.0.

9.2 Changing approval settings

The ABA seeks confirmation that the following interpretations are as intended and correct:

Situation A: An account for which all account holders have agreed to be set to 'pre-approval'; later one account holder wishes to change to co-approval[16], but the remaining account holder(s) do not wish to change the account's status. The ABA's interpretation is that the account should revert to co-approval.

Situation B: An account for which all account holders have agreed to be set to 'non-disclosure' but later one account holder wishes to change the status of the account to 'pre-approval'.

Recommendation 9.3: Confirm the ABA's interpretation of Situation A that the account should revert to the co-approval setting, and of Situation B that the account should remain in the non-disclosure status.

9.3 JAMS no-action opt outs

The major banks' Joint Account Management Services (**JAMS**) have now been live for nine months. The current specification for JAMS is that customers are opted out unless they, with informed positive action, opt in the joint account for data sharing. Therefore, it is likely that many customers have reviewed their JAMs service and made the decision to remain opted out of the CDR simply by not

[15] https://www.ausbanking.org.au/submission/opt-out-joint-account-data-sharing-model/

[16] If this option is provided by the data holder, the ABA supports the position that co-approval be an optional aspect of the service.

taking any action. It is not possible to identify those customers who have made this choice and with the prescribed 'pre-approval' option it is likely that customers who chose not to participate in the CDR for the joint account will be registered for CDR, contrary to settings, which they may well have 'selected' by omission.

For some of these customers there may be real harm from a default setting, especially an unexpected setting, allowing their joint account CDR data to be shared by their joint account holder without their active consent.

Recommendation 9.4: Additional to recommendation 9.1, the ABA recommends finalising development of the joint account in-flow election.

9.4 1 April 2022 compliance date

Members do not expect to be able to implement the joint account changes by 1 April 2022. The ABA refers Treasury to its submission on the 'Opt-Out Joint Account Data Sharing model' and encourages Treasury to carefully consider the suggested timeframes and issues raised in that submission[17].

The safe build and transition to the new model involves significant technical complexity (as set out in the Appendix) and proper testing and migration planning for existing live customer sharing scenarios.

Banks will also be required to undertake a review of all product terms and conditions as well as internet banking channel terms and conditions to ascertain whether the proposed default 'pre-approval' option will require an update of those terms and conditions. Where update is required, in accordance with robust corporate governance processes, banks will need to engage legal, business, compliance, risk, IT, and product review and sign-off, as well as update, design and distribute updated terms and conditions to all customers with affected products or services. Based on recent experience with the implementation of Design and Distribution Obligations, which involved the same undertaking, this will be a minimum 8-month process (depending on the complexity of the entity's operations)

The ABA submission to the 'Opt-Out Joint Account Data Sharing Model' noted an obligation date of no earlier than 1 July 2022. However, given the additional requirement to review product and internet banking Terms and Conditions, as well as to design, built, test, and implementation of the technical solution, the ABA considers 1 September 2022 to be more appropriate for the major banks. Furthermore, banks key technical resources are currently dedicated to preparing for the 1 November compliance release and will not have capacity to commence work on Rules 3.0 until after the annual December 2021 shut-down period.

Recommendation 9.5: The ABA recommends, a compliance date of no earlier than 1 September 2022 for major banks and for non-major banks to be given optionality to comply with this requirement by opting into joint account provision up to 1 December 2022.

9.5 Notification requirements

Notification requirements are complex to design and execute. The ABA highlights several matters in respect to notification requirements:

Rule 4A,16(2) refers to notification by the 'ordinary means of contacting the joint account holders.'

Recommendation 9.6: The ABA recommends data holders to be left with flexibility in terms of the method that they will use to notify customers of a new pre-election. Different data holders will have different capabilities and customer expectations.

[17] https://www.ausbanking.org.au/submission/opt-out-joint-account-data-sharing-model/

Data holders may refuse to disclose data when a non-disclosure option exists as described in Rule 4A.11

Recommendation 9.7: The ABA recommends Treasury consider (either directly or through the data standards) how customers might be informed as to the reason why the data sharing request was denied.

The ABA considers the 7-day notice period to be inadequate time for consumers to access their communications, give consideration and act (Rule 4A.6(2)).

Recommendation 9.8: The ABA recommends data holders be permitted to send notifications to existing joint holders prior to commencement in a timeframe that is in keeping with their standard practices for notifying customers. Therefore, the 7-day requirement should be deleted.

"Rule 4A.16 requires data holders to allow joint account holders to set certain notification preferences. If data standards are in place, this must be done in line with those standards. This would allow consumers to set preferences such that they would not receive certain notifications that data holders would otherwise be required to provide. The ability to set preferences does not affect dashboard requirements or the requirement for data holders to obtain agreement from joint account holders to change the disclosure option or approve a disclosure of CDR data."

Notification preferences introduce substantial complexity, and we would suggest that they be optional at this stage. More consideration is required regarding the nature and granularity of these notifications. Further, some existing notifications may be deemed necessary for transparency and privacy reasons and should not be subject to preferences. There are also questions as to the intersection of such preferences with existing notification preferences which exist outside of the CDR.

Recommendation 9.9: The ABA recommends notification preference should be made an optional implementation and Data Holders respective approach allowed to align with their existing policy and procedures.

9.6 Retrieval of data

Draft Rules 3.0 do not address the right of retrieval or deletion of a joint account holder's data where their data has been shared without their express consent by the accredited data recipient, unaccredited Outsourced Service Provider, Affiliate, Representative, or Trusted Adviser. In this situation, it is not sufficient for these participants to de-identify the joint account holder's data as they can continue to make use of that data against the wishes of the joint account holder.

Recommendation 9.10: The ABA recommends the rules include a mechanism for the joint account holder, who did not give their consent for their data to be shared, to request their data to be deleted by the Accredited Data Recipient, unaccredited Outsourced Service Provider, Affiliate, Representative, or Trusted Adviser and for those participants to send a confirmation to the joint account holder that they have acted on the request.

9.7 The Rules create variation in implementation

In light of recent matters raised by Treasury regarding perceived non-conformance of implementations by data holders, we note the questions raised in Appendix 1 to be an example of where the Rules provide insufficient detail from which to develop a standardised solution across all data holders. This leads to a situation where data holders request further detail and clarification from Treasury. We note that Treasury, unlike the ACCC, has indicated that it will not issue further guidances. Without such

clarification, data holders will be required to build according to their own interpretations leading to lack of standardisation at the policy level (as well as potentially, the standards level).

Recommendation 9.11: The Treasury issue all required Rules and associated guidances before data holder development commences.

Appendix 1: Joint account detailed questions

The following joint account related items included in the draft Explanatory Materials require clarity for implementation. Broadly the shift from no-disclosure to pre-approval (or co-approval) raises several substantial implementation issues which collectively, make an April 2022 obligation date high risk.

Page reference	Rule extract	Clarification required
p19 - Schedule 4 -Joint accounts: Disclosure Options	*"The default is the pre-approval option (rule 4A.4(1)(a))."*	We assume that current customers who have yet to make a disclosure will be automatically switched to pre-approval under proposed rules?
p20- Schedule 4 -Joint accounts: Disclosure Options	*"Joint account holders will be able to:* *• change the default sharing setting to the non-disclosure option, including ahead of joint account data being in-scope and available for sharing. Choosing this setting would ensure no future data sharing from the joint account via the CDR is possible and any on-going data sharing arrangements are ceased;*	We request further clarity with respect to the cutover approach to DOMS. Drafting suggests that both JAMS and DOMS will operate in parallel for the week prior to implementation. This will increase the technical solution complexity and will be difficult to communicate to consumers.
p20- Schedule 4 -Joint accounts: Disclosure Options	*"Joint account holders will be able to:* *• stop data sharing arrangements with a specific accredited person, whether this was initiated by themselves or another joint account holder. This will allow consumers to have granular control of data sharing arrangements."*	The wording suggests that ADR-specific, fine-grained controls are to be implemented by DHs, rather than authorisation specific controls (as per current design). Is that the intent? ADR specific control is a substantial deviation from the current design.
p21- Schedule 4 -Joint accounts: Oversight and changing disclosure options	*"Rule 4A.7 provides that a change from the non-disclosure option to another option requires the agreement of all the joint account holders."* *"Rule 4A.8 provides that if a joint account holder wants to change the disclosure option on the joint account from non-disclosure to*	Draft wording suggesting that the disclosure is recorded only at the account level and not at the individual consumer level (as is the case today with JAMS). Is that intentional or is the CX behaviour expected to be the same as JAMS today? Or doesn't it

Page reference	Rule extract	Clarification required
	either pre-approval or co-approval (if offered), that account holder may propose the change using the DOMS."	matter as long as the outcome is apparent to the consumer? We assume that where one joint account holder chooses to change from either pre-approval or co-approval (if offered) to non-disclosure then this does not require agreement from all parties.
p22 Schedule 4 -Joint accounts: Notification requirements	*"Rule 4A.6 requires data holders to notify joint account holders of the following matters in relation to the account (for new accounts, when the account is opened, or for existing accounts, at least 7 days prior to joint accounts being in scope for sharing under the Rules)."*	Our assumption is that this rule only applies to eligible CDR consumers with eligible CDR products.
p23 Schedule 4 -Joint accounts: Other matters	*"Set 1 April 2022 as the new compliance date for joint account data sharing in the banking sector.* *The Rules also include transitional provisions that:* • *require relevant data holders to continue to comply with the former joint account transitional provisions until 1 April 2022, when they must begin to comply with Part 4A of the CDR Rules;* • *require data holders to notify consumers with joint accounts of the change to the default setting to share at least a week before the commencement date; and* • *provide that joint accounts that are currently set to the 'no disclosure option' are not switched to the pre-approval option on the commencement date"*	As per earlier comment, it isn't clear whether this is a "hard cutover" at implementation date or if the expectation is that consumers have opportunity to change their preferences using DOMS before the implementation date. The approach will significantly impact the change management impacts for data holders.