Australian Banking Association

26 May 2021

Ms Kate O'Rourke
Recipient Position.
The Department of Treasury
By email: data@treasury.gov.au

Dear Kate

ABA submission to the CDR design paper

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on the 'Opt-out joint account data sharing model – CDR rules and standards design paper[1] (**the design paper**).

Our position

We thank the Department of Treasury (**the Treasury**) and the Data Standards Body (**DSB**) for the opportunity to comment on key CDR concepts at a design stage, and prior to draft rules and standards being issued for consultation.

This model of consultation allows the industry to consider the proposals conceptually and provide key feedback prior to detailed drafting work being undertaken. The ABA supports design stage consultation becoming a regular feature of the CDR development process going forward.

Key recommendations

The design paper seeks feedback on several key concepts related to joint accounts.

Proposed cross-sectoral definition of 'joint account'

Whilst the ABA supports the principle of a simple CDR, we question the ability to develop a 'one-size-fits-all-sectors' approach to joint accounts. The real economy has not evolved a single taxonomy for joint accounts because there are currently different legislative and practical requirements for sectors. It is unclear how the CDR can concurrently 'respect the rules of each sector' and develop an 'all-in-one' approach to joint accounts.

Proposed opt-out approach

The ABA supports retaining the current opt-in approach. The proposed opt-out approach is not supported on the basis that it undermines the foundational principle of the CDR, which is informed consent.

We consider the proposed opt-out approach is a lesser approach for the following reasons:

- It requires sharing another person's data (likely 'personal' and 'sensitive' data under the Privacy Act) where that other person will be incapable of reclaiming their data once shared.
- It may result in further downstream breaches of some of the Privacy Safeguards.
- It does not account for the fact that Australians rate very highly the protection of their privacy.
- It does not allow for other core principles such as control and transparency over one's data.
- It places pressure on consumers experiencing vulnerability.
- It does not consider banking sector specific settings, obligations, and risks.

[1] https://treasury.gov.au/sites/default/files/2021-04/c2021-168954-cdr_design_paper_joint_accounts.pdf

Complex joint-accounts

Notwithstanding the position articulated above, the ABA has considered the three options outlined under the proposed opt-out approach for in complex joint accounts.

We are of the view that it is not feasible to nominate an industry preferred option at this point. This is a particularly complex task given the principle to develop the ecosystem so that builds alignment to, or support for, the planned end-state (which is 'Action Initiation' and 'Payment Initiation'). The extent of rework (and therefore redundant build involved in this opt-out proposal) will vary for each option.

Other matters for consideration

Additional to the above the ABA raises the following matters of process:

- We question the need for further amendments to the CDR consent model so soon after the last rule change to consent was made. This is especially so given the lack of evidence that the opt-in model is a problematic friction point.
- Further, rules changes which appear to be counter to the future CDR roadmap are problematic because of the potential for confusion caused to consumers and therefore the risk that it will undermine potential trust in the CDR.
- Finally, the privacy concerns associated with this change are of a type which warrants a detailed review of the design by privacy experts and the OAIC in accordance with section 56BR of the *Competition and Consumer Act 2010* (Cth) (the Act). The ABA suggests that the lens of consumer privacy be applied at every stage of the policy development process, including the design stage.

The ABA has provided more detail on these themes in the Annexure. Please do contact me if you would like to discuss any aspect of this submission.

Kind regards,

Emma Penzo
Policy Director
Emma.Penzo@ausbanking.org.au

Australian Banking Association

Annexure

1. The need for further amendment

The express intent of the Government's Digital Economy Strategy is 'to deliver a roadmap for the economy-wide roll out of the Consumer Data Right'[2]. The ABA supports the development of a strategic roadmap for the CDR, on the basis that it will provide a pathway to ensure that any changes to policy and rules are made with consideration of and alignment to the intent of the project.

Evidence for the need for Rule amendments

The ABA notes that concerns have been raised in respect to the operation the current rules or standards for joint accounts:

> *'In particular, concerns have been raised that the requirement for each joint account holder to 'opt-in' to sharing before joint account data can be shared will lead to poor consumer outcomes.'*[3]

The ABA makes three points in respect to paragraph 1 of the design paper.

First, the nature of these concerns is unclear in the design paper. In the DSB participant call (13 May 21), the Treasury representative noted that the concerns related to 'friction' in the consent process and that this 'friction' would result in 'poor consumer outcomes'. As a result, it was noted, entities were reticent to become accredited data recipients (ADR).

The extent of consumer engagement to understand the level of 'friction' pertaining to their banking data is unclear. It is important to engage with consumer groups in respect to their security needs and perceptions of trust for banking data and financial transaction security. The ABA notes that the design paper has drawn heavily on previous consumer experience testing (CX); it is doubtful that the output from the CX can validly be used to answer this question.

Consent requirements are a ***necessary safeguard*** in banking. Banking is unlike other sectors, such as online purchases of fast-moving consumer goods, where such safeguards may not be required for in-app purchases or real-time purchase decision making. The risk of misuse, and harm being caused by access to CDR data in banking relationships is greater than in other sectors, such as energy.

Second, it is the ABA's view that it is not appropriate to initiate changes to the rules without a solid body of metrics which supports a case for change. It is unclear to the ABA whether the 'opt-out model' is responding to hypothesised or projected concerns of participants or whether real issues have been identified and evidenced which have led to poor consumer and regime outcomes.

While the 'opt-out' model is stated to respond to the issue of 'friction' (paragraph 6 of the design paper) there is no evidence that consumers object to this additional step enough to lead to dropouts. In the DSB participant call (13 May 2021), the Treasury noted that feedback to date from consumer advocacy groups opposed an opt-out approach. It would be helpful if data were made available to demonstrate the validity of the concern. For example, is there a marked difference in the fulfilment rate for sole accounts versus joint accounts for the same offerings? What metrics have been analysed which compares the pre-enablement opt-in versus the in-line opt-in? Which customer complaints metrics show that the process is too onerous? Have consumer focus groups been asked about the opt-out arrangement versus the current opt-in process to ascertain the degree of security and control required by consumers in respect to their banking data?

[2] https://digitaleconomy.pmc.gov.au/fact-sheets/data-and-digital-economy
[3] Paragraph 1, design paper.

Third, the ABA notes the relative newness of the most recent changes to the rules relating to joint account authorisations. The amendments to the rules were introduced less than four months ago and have not been justified on a cost-benefit basis. For example, how many additional consumers will share data through the CDR under an opt-out model? Additionally, it will not be feasible, if the CDR roll-out is to achieve the Government's roll-out objectives, to revisit rules each time a concern (which is not evidence-based or consumer-centric) is raised.

Consideration of relevant factors

We note the elements considered by the Treasury in developing the proposed model (paragraph 10 of the design paper). The ABA suggests that additional matters be considered prior to the development of a draft design (per part B of the design paper):

- Consumer focus groups which test the concept at design stage.
- An impact assessment to demonstrate the degree of friction, which is the subject, and set a baseline for what the goal ought to be (e.g.: compared to individual sole accounts).
- An assessment of how any proposed change to the rules will apply in the context of:
    - The roadmap for the economy-wide rollout of the CDR
    - Vulnerable customers, and in particular the obligations to those customers, that are specific to the banking sector (and the specific risks of harm in that sector) and
    - Future directions for the CDR, regarding 'write access' and
- A statement of where, in the overall scheme of the roadmap for the CDR, does this requirement sit. Is this the highest priority issue to resolve about CDR take-up and what is the evidence to support this?
- Consideration of the subsequent regulatory or legal implications on data holders because of the proposed change.
- A risk assessment for an opt-out model which examines the consequences in any sector to which opt-out is proposed.

In respect to the final point, the ABA reiterates our concern regarding the lateness of the Privacy Impact Assessment in this process[4]. Privacy and security considerations ought to be a foremost consideration in the ongoing design of the CDR and should be considered at every stage of the development. At the design phase, a thorough privacy and security assessment of a concept has the benefit of identifying issues very early and reducing work down the track. A published report by the OAIC or an independent reviewer at the concept or design phase would also give comfort to participants that these matters have been considered.

The ABA notes the Treasury's confirmation that a Privacy Impact Assessment will be undertaken should it take the decision to proceed with draft rules for an opt-out model.

Post implementation Review of Open Banking implementation

The ABA repeats prior requests for a timetabling of the Post Implementation Review per the Open Banking review report of 2017 which noted 'Open Banking should be formally evaluated 12 months after the Commencement Date'[5] . Any changes to the current rules or CDR policy should be dependent on the outcome of the Post Implementation Review of the current Open Banking regime to facilitate data-informed decision making.

[4] This concern was raised in the Treasury meeting with the Non-major banks on 18 May 2021.
[5] Farrell, December 2017, 'Open Banking, customers choice, convenience, confidence', p: xi

Australian Banking Association

2. Joint account definition

Question 1: Do you prefer the definition of joint accounts in the rules, or would you prefer a sector-wide definition, for example with a focus on financial responsibility? Are there other factors should we consider?

The ABA does not support a cross-sectoral definition of definition of joint accounts.

The ABA notes the intention of Treasury to 'develop a model that will be workable for data sharing on joint accounts across the economy' (paragraph 6 of the design paper).

The ABA supports a simple CDR however, we question the ability to develop a 'one-size-fits-all-sectors' joint account prescription. The real economy has not evolved a single taxonomy for joint accounts because there are different legislative and practical requirements for different sectors. It is unclear how the CDR can concurrently 'respect the rules of the sector' and develop an 'all-in-one' approach to joint accounts.

The banking sector[6] is nuanced in its approach to joint accounts in several ways:

First, the concept of a joint account involves two or more potentially independent transactors drawing on the same balance or credit facility for different transactions. In comparison, in the energy sector, the 'joint' will relate to a fixed transaction in the provision of energy to specific address(es), therefore the interests of the 2 customers are more closely aligned with each other.

Second, the harm possible from unauthorised sharing of banking data is higher than for some other forms of information, and the issues of family violence and coercive control are closely entangled with financial abuse.

Third, the sensitivity of financial data is fundamentally different to data in other sectors (e.g.: energy usage) as well as the high potential for fraud. Sensitive personal information can be derived from financial data, particularly transaction data (e.g.: by analysing where money is spent such as medical expenses, memberships of political organisations or donations to religious organisations) which would heighten bank customers' privacy concerns about sharing their financial data. Also, purchase history can be used for profiling. The ACCC digital platforms second interim report highlighted consumers strong desire not to be tracked or profiled[7]. By comparison, energy usage data does not give away details of (ie) the types of devices and appliances owned by the household, or what contributes to their energy usage.

Fourth, 'who' has 'financial responsibility' is not useful for banking. This concept refers to the person who is liable for repayments on debt, however, not all bank accounts are credit accounts. Further, the ability to transact on an account, that is to transfer or withdraw money, can change during the account's operation. Additional cardholders can be appointed or rescinded at will, as can other authorities such as powers of attorney. However, the ownership of the account will be consistent, even while the owners may be in dispute or for any reason require agreement to transact.

Fifth, for banking there is a common law duty of confidentiality[8], which while modified by consent, can be revoked in special circumstances (e.g., vulnerable customers). This duty is not always prevalent in other sectors. The opt-out model potentially overrides this duty of confidentiality.

[6] We assume other sectors have nuance relating to joint accounts that are specific to that sector.
[7] ACCC, 2021, Digital platforms services inquiry Interim report No 2.
https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202021%20interim%20report.pdf
[8] Which may not apply in other sectors.

Australian Banking Association

3. 'Opt-out' approach

Question 7. Do you agree that an 'opt-out' approach is preferred over the current 'opt-in' approach?

The ABA does not support the 'opt-out' approach; the current opt-in approach is preferred.

The proposed opt-out approach will facilitate the following hypothetical situation:

> **Example 1: A 'typical' joint account**
>
> In the scenario of Joint Account Holder 1 (John) & Joint Account Holder 2 (Mary) where John grants consents to the ADR and Mary has a pre-approved default – Mary has no relationship with the ADR. Mary can revoke the consent granted by John via her relationship with the data holder, however, Mary has no recourse with the ADR to get the data deleted (unlike John who has the relationship with the ADR).
>
> Transactions relating to Mary include descriptors such as 'Cancer Biopsy', 'Communist Party', 'Franciscan Monks'.

Informed consent

The 'opt-out' approach does not meet the standard of express, informed, and purpose specific consent (per Rule 4.9) – as is the case with Mary in the example above. The OAIC's guidance states that an 'accredited person may only collect and use consumer data right data with the consent of the consumer' and 'an accredit person must ask for a consumer's consent in accordance with the consumer data rules which see to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited an easily withdrawn.'[9]

Opt-out goes against the letter and spirit of the CDR regime which is underpinned by the notion of informed consent. Consumer trust in the regime is based on this fundamental principle.

Sharing customer data of another person

The ABA supports the prohibition on sharing customer data of another person (paragraph 12 of the design paper). This prohibition only works through an opt-in model (the current model). Under the proposed opt-out model, inevitably some customer information (such as the name of the other account holder where this forms part of the account name and transactions as noted in the example which are identifiable to one party which contains details about merchant/location/time etc.) will be disclosed as part of the joint account consumer data. Example 1 demonstrates how sensitive information which implicitly relates to Mary can be shared without her consent. Messages and transaction details will commonly identify an individual.

The ABA notes the alternate position that because statements are available to each account holder, and transaction history is available through digital banking channels there is no difference with, in this case, John sharing Mary's data without her consent through the CDR.

However, the ABA also notes that the CDR poses new risks of mass data sharing, in a way which PDFs and Excel spreadsheets do not. The CDR will enable the potential for more misuse on a greater scale because it enables the transfer of machine-readable data into services driven by algorithms capable of analysis at scale. The data points which can be derived from banking data by the algorithms will add further depth of analysis which is not achievable as easily under current data transfer methods.

[9] OAIC, Chapter C Consent -The basis for collecting and Using CDR data (link)

Additionally, banks may present the information differently in statements or online banking which reduces the risk from the existing processes. Also, certain manual options are possible in extreme cases of customer safety needs, which are not feasible to be replicated in the CDR.

Finally, if no consent is required from the person who made those transactions (Mary), then 'information that identifies or is about the person'[10] would be shared without their consent in breach of rule 3.2(3)(b) in Schedule 3.

Information contained can be 'sensitive information'

Under the 'opt-out' model, the transaction data of customers will be sent to the ADRs without explicit consent. As identified in example 1, such data will inevitably include sensitive information under the Privacy Act, such as doctors' details, religious affiliations, and political affiliations.

The Australian Privacy Principles continue to apply to a data holder of CDR data as set out in section 56EC(5) of the *Competition and Consumer Act 2010* (Cth) (the **Act**). A data holder disclosing transaction information that reveals sensitive information about a joint account holder who has not consented to their information being disclosed is potentially in breach of Australian Privacy Principle 6.

If the opt-out model is adopted the Act would require amendment to confirm that such a disclosure is permissible.

A move to an opt out model of consent warrants review under section 56BR of the Act including review of the likely regulatory impact of allowing the rules to impose disclosure based on this model.

Potential breaches of the Privacy Safeguards

The opt-out model will potentially cause contraventions to several the Privacy Safeguards by ADRs and data holders:

> Privacy Safeguard 1 is foundational in setting the requirement of an 'open and transparent management of CDR data'. The mandating of opt-out contravenes this safeguard, as the customer will not know that their data is sharable until after it has been shared – this is not open and transparent. Additionally, OAIC's guidance notes that 'Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges'[11]. It is unclear what proactive steps are being contemplated by ADRs when they are in possession of data for which they have not had explicit consent to hold, use, and act on.
>
> Privacy Safeguard 4 may be inadvertently contravened when an ADR receives CDR data that is collected other than as a result of the accredited person seeking to collect it under the CDR Rules12. The non-authorising recipient could object to the data being collected by the ADR on the basis that they did not provide informed consent for the data to be shared.
>
> Privacy Safeguard 6 required that the use and disclosure of CDR data be done only with a valid request from a consumer. The OAIC notes that this is an important safeguard because 'consumer consent for uses of their CDR data, including subsequent disclosure, is at the heart of the CDR regime'[13]. Further, 'by adhering to Privacy Safeguard 6 an accredited data recipient…will ensure consumers have control over what their CDR data is being used for and who it is disclosed to. This is an essential part of the CDR regime'[14]. The opt-out model is inconsistent with this safeguard.

[10] Schedule 3 Rule 1.3
[11] OAIC Para 1.42 https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-1-privacy-safeguard-1-open-and-transparent-management-of-cdr-data/
[12] OAIC Para 4.16 https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-4-privacy-safeguard-4-dealing-with-unsolicited-cdr-data-from-cdr-participants/
[13] OAIC Para 6.8 https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-6-privacy-safeguard-6-use-or-disclosure-of-cdr-data-by-accredited-data-recipients-or-designated-gateways/
[14] OAIC Para 6.9 https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-6-privacy-safeguard-6-use-or-disclosure-of-cdr-data-by-accredited-data-recipients-or-designated-gateways/

Privacy Safeguard 7 prohibits 'accredited data recipients and designated gateways from using or disclosing CDR data for direct marketing unless the consumer consents and such use of disclosure is required or authorised under the consumer data rules'[15]. Recalling example 1, not only is the potential for contravention a possibility but with it comes potentially serious consequences for Mary who may become the focus of marketing materials from 'aligned' services gleaned from analysis of her transaction history. Depending on the nature of the marketing, this may also contravene other laws such as the Spam Act and APP 7.

Australians value security of their banking data

Australians take the security and privacy of their banking data seriously. Our submission to the Inquiry into Future Directions for the Consumer Data Right[16], referenced independent research which supports the conclusion that Australians consider the security of their data to be a priority. Notably, the Deloitte 2019 report on Australians' trust levels and open banking found:

> *'Trusting organisations to keep your money safe is one thing. But for open banking to be successful, people need to trust organisations to keep information about them and their transactions secure. At its epicentre people need to believe that the organisation they select will treat their privacy seriously'*[17]

To the ABA's knowledge, this opt-out proposition has not been explicitly tested with consumer groups or with actual potential consumers of the CDR. The CX testing is not sufficient because it does not test explicitly the proposition of consumer expectations for banking data security for trust in the CDR to prevail. The focus of the CX is on consent flows.

Additionally, to the ABA's knowledge, it is unclear whether consumer groups have had a significant opportunity in designing the CDR, including the opt-out design. If the CDR is intended for the benefit of consumers, the ABA is interested to know the extent of involvement of consumer groups in the design of the opt-out model.

Control and Transparency

The paper appears to assume that 'transparency' is a form of control because if a customer is aware that they have been automatically opted-in to data sharing that that they have control (paragraph 5 of the design paper). The ABA proposes this assumption does not follow and that opt-out is a non-customer-centric proposition where customers lose control over their data because they have been opted-into the CDR without their prior consent. Further, stopping the sharing arrangement retrospectively does not put the joint account holder back in their original position – the data has already been shared.

Customer protections

It is unclear to which existing protections for consumers paragraph 11 of the design paper refers. The ABA understands that the consumer protections which have been built into the CDR follow the principle of not sharing another person's data without their consent.

The 'opt-out' proposal is a reversal of the current well-considered and discussed CDR requirements. Therefore, the ABA suggests a rules/standards analysis to identify the protections and how they will be unchanged by the proposed opt-out design. If this analysis has already been completed, it would be helpful for the Treasury to make it public for review.

[15] OAIC, PS 7, Key Points, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-7-privacy-safeguard-7-use-or-disclosure-of-cdr-data-for-direct-marketing-by-accredited-data-recipients-or-designated-gateways/
[16] https://www.ausbanking.org.au/wp-content/uploads/2020/05/200521-ABA-Submission-Inquiry-future-of-CDR-FINAL.pdf
[17] Deloitte,2019, p17 https://www.financialcapability.gov.au/files/open-banking-switch-or-stick-insights-into-customer-switching-behaviour-and-trust.pdf

Customers experiencing vulnerability

The design paper notes that one of the protections for vulnerable customers in a joint account arrangement is to 'treat joint accounts as if there were held in the name of one person alone where a data holder considers it necessary to prevent physical or financial harm or abuse' (paragraph 11 of the design paper).

It is unclear how treating the account as though it were in the name of one person alone would support the vulnerable customer. Banks have specific ways that they can assist customers who are at risk and often the solutions are context specific. Further, customers can enter and exit situations of vulnerability. Therefore, a status of vulnerability is not always permanent.

The advantage of the 'opt-in' model over 'opt-out' is that it minimises the risk of provoking potential violence or abuse. The vulnerable joint account holder takes no active step to *prevent* the other joint account holder from sharing the joint account information with a third party. For example, the vulnerable party may wish to prevent a data sharing arrangement that could negatively affect them, to the advantage of the other account holder. The opt-out model (1) does not enable a notified transaction to be blocked and (2) requires the vulnerable joint account holder to actively stop future data shares potentially provoking violence or abuse.

Example 2: Joint accounts involving vulnerability

Joint Account Holder 1 (Julie) is experiencing vulnerability, and Joint Account Holder 2 (Peter) is not experiencing vulnerability. The joint account that they have operated for the last 10 years has a transacting authority of either one to sign.

After being informed of Julie's situation of vulnerability, the bank determines that changing the authorities to two-to-sign is not appropriate. This is because restricting accounts to two-to-sign where the account default is one-to-sign is often very difficult to apply and provocative in abusive situations. Further, when an account is made two-to-sign, in cases such as family violence, transaction details may need to be manually redacted, and statements manually generated. This is like treating the account as two individual accounts who are drawing on the same funds. This is a very manual process. In no case is an account held by Person A (Julie) and Person B (Peter) treated as a sole account of A, nor would doing so adequately address the risk of harm from Peter.

Therefore, rather than change the account authority, other mechanisms are invoked to support the people in the vulnerable situation. These mechanisms are specific to bank and situation.

In this example Julie has shared data on their joint transaction account to an ADR. Peter has not given consent, nor has he been informed that his data in the joint account has been shared (per Wireframe 1.3).

Scenario 1: Julie is in a situation of domestic violence. Julie's data sharing action where Peter is not informed will potentially worsen Julie's situation should Peter discover the share at a future point.

Scenario 2: Julie is seeking help for a gambling addiction and Peter has temporarily assumed the financial responsibilities of the family as Julie fully recovers. Julie's data sharing action would undermine Peter's temporary role of overseer of the family's finances.

Example 2 demonstrates that banks will not usually know of a vulnerability until notified, or until some interaction raises a suspicion (for example during a loan application process where under paragraph 54 of the ABA Banking Code of Practice banks are required to be satisfied that there is no abuse)[18].

The minimum protections, as currently envisaged involve the at-risk customer being able to disable data sharing which prevents their data on a joint account being shared, and to 'pause' existing data sharing on the joint account which is more valuable than a termination of an arrangement (since

[18] https://www.ausbanking.org.au/wp-content/uploads/2021/02/2021-Code-A4-Booklet-with-COVID-19-Special-Note-Web.pdf

circumstances can change in risk situations and personal safety may require “un-pausing” such arrangements).

The proposed notification requirements compromise the protections for vulnerable customers to achieve transparency. A notice of termination of sharing arrangement may put a vulnerable customer at more risk than a less confronting action such as ‘disable data sharing’ at the joint account level.

There is a need for deeper consideration for how a bank would respond to a customer alerting their bank to their safety being at risk of their CDR data is made available to the joint account holder. Not all situations of vulnerability involve separately located joint account holders where simply terminating an arrangement is a solution, nor will that prevent the data already shared being used by the ADR.

Banks need to be able to manage these cases in such a way that escalating conflict is avoided, and arrangements reflect customers’ needs (including those driven by their safety concerns). CDR rules must be flexible about how banks protect customers in different situations.

If the Treasury were to pursue a default setting for an opt-out approach, customer education campaign by the Government will be required to ensure people are aware how to protect themselves from their joint account holder sharing their joint CDR data. This approach will involve difficulties for vulnerable customers to understand their rights and position, but it will also have the effect of educating abusers that they can utilise the opt-out default.

Banking specific considerations

Joint accounts have definition and operation which is specific to the banking sector. These must be reflected in the CDR.

First, the concept of a joint account involves two potentially independent transactors drawing on the same balance or credit facility for different transactions. In the energy sector where the “joint” will relate to a fixed transaction in the provision of energy to particular address(es) so the interests of the 2 customers are more consistently closely aligned with each other, the two types of joint account cannot be redefined into a one-size-fits-all.

Second, there is no equivalent in other sectors of the banker duty of confidentiality, which is owed to each of the joint account holders. Further, the harm which is possible in unauthorised sharing of banking data is higher than for some other forms of information, and the issues of family violence and coercive control are closely entangled with financial abuse.

Third, preliminary legal advice is that the CDR cannot rely on the authorities for customers that have signed banking transaction authorisations for the purposes of enabling data sharing. The Treasury will need to develop a mechanism for the Government to gain data sharing authority from Australian consumers under the opt-out model.

Australian Banking Association

4. Complex Joint accounts

The ABA firmly considers that opt-in should be retained as the default setting for all joint accounts whether simple or complex.

Given the ABA's support for the current opt-in model, we have briefly considered the three options proposed for complex joint accounts.

If the Treasury elects to change to an opt-out approach, that approach should be consistent across all joint accounts. For clarity, the ABA considers the Treasury's proposal where an opt-out approach is adopted for (simple) joint accounts (one-to-authorise) and an opt-in approach is adopted for complex joint accounts to be overly burdensome and confusing for consumers and it not aligned with the principle of a simple CDR.

The following provides considerations for each option:

> ***Option 1 'Mirror current authorities to transact on complex joint accounts'*** may appear to support Action initiation and Payment Initiation because these features will require equivalent approval by consumers. We note that each payment or action will require a positive authority from the consumer (in accordance with the account authorities) for the transaction to be undertaken. However, without a roadmap, and agreed design for how Action Initiation and Payment Initiation will operate, Option 1 may be premature and likely to require rework within 12 months of implementation (and therefore resetting of those accounts and re-education of customers).
>
> ***Option 2 'Require opt-in for complex joint accounts'*** would introduce complexity to the CDR where one group of joint accounts are treated differently to another group of joint accounts due to their signing authorities (which are subject to change at any time at the discretion of the account owners).
>
> ***Option 3 'Apply the opt-out setting to complex joint accounts'*** may achieve the ability to direct data flows differently to the account's right to transact, however, it is unclear how this option fits with the future roadmap of the CDR, and may lead to further rework of the model for future use cases. Such a development will be particularly unhelpful for Action Initiation (for account opening) and Payment Initiation as these functions will likely require some alignment between the right to transaction and the right to share data.

The ABA reiterates its concern that the foundational element of the CDR, informed consent, continues to be subject to change involving reversals of long-standing principles. The changes envisaged by this design document will require further changes in the coming months as new functionality is added to the CDR. Revolving consent requirements will undermine consumer's ability to keep pace with the changes and will result in a potential failure of the CDR to gain the trust of consumers. A more comprehensive consideration of the requirements of the next phases of CDR should be undertaken to inform the immediate consultation to avoid multiple points of change.

The consent model needs to be simple and consistent to support consumer understanding as to how their data will be managed.

Australian Banking Association

5. Implementation considerations

The opt-out model raises several implementation issues and considerations:

Authority for 'opting-out'

The opt-out model requires all Australians to be informed of the default position of the CDR for all joint accounts across sectors. Treasury would need to consider the Government undertaking an education campaign equivalent to that of the 'My Health Record' where Australians were educated and given the opportunity to opt-out well in-advance of the system going live.

Ensuring transparency and control for consumers

The ABA continues to advocate for a government issued broad and sustained education program of the Australian public and for greater clarity of the liability framework of the CDR. If the opt-out model is adopted, customers may perceive that data holders are sharing their data without their permission, undermining their trust in the regime, and causing an increase in consumer complaints.

Significant rebuild

The ABA notes that data holders are going to need to undertake significant rebuild of the current implementation to enable fine grained consent in the coming year. Fine grained consent is a foundational change to the consent model which will support future Open Banking functionality. It is unclear how this opt-out proposal strategically fits into the development of Open Banking.

Revised timeframes

The ABA notes the proposed extension of obligation for joint accounts to Quarter 1 2022. However, given the expected size of IT change required to enable the opt-out arrangements, Quarter 1 2022 is insufficient time to undertake this change, or to deliver the current obligation of in-flow election (also noting the banks technical change lock down period in December-January to ensure continuity of system stability and payment processing during this higher volume period).

This timing would also need to accommodate appropriate consumer reviews which specifically seek to understand views regarding their banking data privacy and security requirements to place trust in the CDR. For accuracy and as noted previously in this submission, these reviews cannot be blended with CX as in these tests, consumers are more focussed on their understanding of the transaction flow than they are with their views on privacy. Additionally, the extent of consumer education and communication which will be required should be a consideration in the review of timing.

Noting that the ABA considers that opt-in should be retained as the default setting, a simple summary of the implementation considerations has been provided by some members of the ABA (Note: an industry consensus view would require more time for consideration).

Option	Implementation considerations[19]

Option 1	• Complexity **high**.
	  ○ Requires tight linking of transaction authority and data sharing authority which is not a current data sharing system entitlement check
	  ○ Requires build of a co-approval solution into the consent authorisation flow.
	  ○ Rework to reset customers who have already set their election to 'Pre-Approval'
	• Implementation as a result would likely require circa 12 months + from the point of rules and standards being defined

Option 2	• Complexity **high**. Also requires tight linking of transaction authority and data sharing authority which is not a current data sharing system entitlement check • Whilst positioned as simpler than option 1, in that the co approval flow would not be required, the need to transition from opt in to opt out states when transaction authorities change will create additional system complexity • Implementation as a result would likely require circa 12 months + from the point of rules and standards being defined

Option 3	• Complexity **medium**. The simplest of the 3 options. However, whilst on face value the change appears simple it is more complex than the consultation paper presumes as would require
	  i. complete reworking of the system logic from positive to negative
	  ii. ensuring this change flows to customer dashboard and banker service tools in addition to the consent itself
	  iii. any change to the system security flow requires extensive testing.
	• As a result, would require approximately 9 months from the point of rules and standards being defined

[19] It is very challenging to provide an estimate on the implementation effort as external factors (such as other concurrent CDR requirements) also affect delivery timeframes.