



26 May 2021

Kate O'Rourke
First Assistant Secretary
Consumer Data Right Division
Treasury
by email: Kate.ORourke@TREASURY.GOV.AU

Dear Ms O'Rourke,

'Opt-out' joint account data sharing model

Thank you for the opportunity to comment on Treasury's 'Opt-out' joint account data sharing model. This submission is from the Financial Rights Legal Centre (**Financial Rights**), Consumer Action Law Centre (**Consumer Action**), and the Australian Communications Consumer Action Network (**ACCAN**). This submission will address the one key question:

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

In short, no. We strongly oppose the proposal to establish an 'opt-out' model for joint accounts on the basis that an opt-out model:

- contradicts and undermines the consent model central to the Consumer Data Right (CDR);
- runs counter to current privacy principles;
- runs counter to recommended strengthened consent requirements and pro-consumer defaults in the Privacy Act;
- wrongly equates one's transaction preferences with their privacy preferences;
- prioritises the business interests of the FinTech sector over the interests of consumers to maintain privacy and security;
- will undermine consumer trust in CDR; and
- increases risks to those subject to financial abuse, elder abuse, or domestic or family violence.

We recommend Treasury:

- return to an opt-in approach for Joint Account Holders;
- require all CDR participants have internal processes in place to flag consumers who are subject to abuse, both for those who self-identification as subject to abuse and through the proactive identification of signs of abuse; and
- require all CDR participants to include clear communication channels for consumers to self-identify and seek assistance and that this be included as a requirement under the CX design standards.

We refer throughout this submission to Joint Account Holder A and Joint Account Holder B where:

- **Joint Account Holder A (JAH-A)** is a consumer who makes the initial decision to provide data to an Accredited Data Recipient (ADR) and
- **Joint Account Holder B (JAH-B)** is not the initiator of providing joint account data to an ADR.

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

Our organisations strongly opposes the proposal to establish an 'opt-out' model for joint accounts.

We do so on the following bases:

- **An opt-out model contradicts the consent model central to the CDR**

Currently an ADR is only be able to collect a consumer's data after the consumer has given consent for them to do so. That is an affirmative act of consent to opt-in to sharing one's financial data and must be, as required under the CDR rules:

- voluntary; and
- express; and
- informed; and
- specific as to purpose; and
- time limited; and
- easily withdrawn.

The elements of voluntary, express, informed, specific as to purpose that make up a positive act of consent to share one's data has been thrown out for joint account holders in the proposed opt out approach to joint accounts.

In the opt-out proposal an ADR will be able to collect a consumer's data without the consumer affirmative act of consent for them to do so. The Joint Account Holder's consent has been pre-empted and they are left to having to act to remove this assumed consent.

Treasury's consultation paper states that

The 'opt-out' setting largely leverages current regulatory and implementation requirements.

The use of the qualifying word largely is doing a lot of work here. What has not been “leveraged” is the current regulatory requirements regarding consent.

- **An opt-out model runs counter to current privacy principles and the recommended intention to strengthen consent requirements and pro-consumer defaults**

Chapter B of the APP Guidelines state that consent should have the following characteristics:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Under the proposal, Joint Account Holder B would neither be adequately informed before the giving of consent, nor will they have voluntarily given consent to have their data provided to a third party.

The ACCC Digital Platform Inquiry report has also recommended that consent requirements be *strengthened* from this base level. Recommendation 16(c) proposes that:

Valid consent should require a clear affirmative act that is freely given, specific; unambiguous and informed. This includes de-bundling consents and any settings for data practices relying on consent to be pre-selected to 'off'.

The current Joint Account Opt Out proposal again fundamentally runs counter to this recommendation.

No clear affirmative act would have been provided by Joint Account Holder B. Inaction cannot be deemed to be consent. Silence is not consent.

The consent has not been freely given since they were not either aware of the consent to begin with, if they have been made aware of it are unlikely to act due to status quo bias.

The consent is not unambiguous because again it could be because the Joint Account Holder B may be supportive of sharing their data but they may also be disengaged, apathetic, subject to pressure or acting (or not acting as the case may be) according to a status quo bias.

The Joint Account Holder is only informed after the fact and must act against the express interests of Joint Account Holder A if they were to act to deny or prevent the data from being provided.

This final point could lead to significant problems re: domestic or family violence. See further below.

- **An opt-out model wrongly equates one’s transaction preferences with their privacy preferences**

Having a preference for sharing the control of transactions on a joint bank account is not the same as expressing a preference for your partner/joint account holder to do whatever they like with the data in that account. It does not follow that if you agree to sharing your money with someone, you naturally agree to sharing your data. Your finances and your personal financial

data are two distinct forms and it is not the case that ones transaction preferences are the same as one's privacy preferences.

- **An opt-out model places the business interests of the FinTech sector over the interests of consumers**

Opt-in and opt-out approaches determine a consumer's *default* consent status in relation to data collection. Under an opt-in regime, consumers are opted out by default and must take action to opt-in prior to data collection. Under an opt-out regime, consumer are opted in to data collection by default and must take action to stop data collection.

The choice of one over the other has profound implications for the values a jurisdiction forces upon consumers and businesses. Opt-in and opt out models vary across the world – the EU's GDPR has established an opt-in model, while the US has generally adopted an opt-out regime where there is no requirement to obtain affirmative consent prior to data collection.

Generally speaking though, jurisdictions that culturally value privacy over economic interests typically operate under opt-in regimes, and those that value business interests over privacy operate an opt-out model.¹

This is because of what is known as the status quo bias where consumers tend to stick with a default option even if a different option is relatively easy.² A jurisdiction that values privacy applies an opt-in regime because no data collection is the default, and will tend to remain that way given consumer's status quo bias. A jurisdiction that values business interests applies an opt-out.

However, an opt-out model assumes a positive state of consent to the collection of data, a state that would otherwise be a required unambiguous and affirmative act of consent. An opt-in model gives the consumer the choice to act and positively consent to the collection of their data.

The opt-out model being put forward undermines the concept of consent by allowing the sharing of their data without their prior knowledge – and afterwards particularly if they are disengaged from the process.

The interests for business in seeking out an opt-out regime are:

- *friction is removed for consumers to access FinTech offerings*

The consultation paper states that under the current opt-in approach:

¹ Lauren Kaufman, *To Opt-In or Opt-Out? How data privacy regimes influence economics, user experience & consumer choice*, 7 March 2020. <https://lolokaufman.medium.com/to-opt-in-or-opt-out-5f14a10bae24#:~:text=Opt%2Din%20vs.&text=Under%20an%20opt%2Din%20regime,under%20an%20opt%2Din%20regime>.

² See Kahneman, Knetsch Thaler, *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 1991, *The Journal of Economic Perspectives*, 5(1), pp. 193-206, Winter 1991

“data holders must not share data on a joint account unless both account holders have proactively consented to data sharing on the account. While this provides a high level of oversight and control, it may create an undue level of friction and lead to consumers abandoning the data sharing process.

Further the paper indicates:

... the data sharing process will not require re-direction or timely delays while awaiting a response from the other account holder(s).”

Firstly, the consultation paper presents no evidence to demonstrate that this friction is a problem, nor that this friction is the reason why people drop out of the sharing process over any number of other reasons including simply not being interested in what is being offered.

Secondly, friction is not a social ill that needs to be removed in all situations at all costs. Some friction or pause is needed in a process that may lead to significant financial consequences – especially in a read/write access world. Frictionless transactions are already causing significant consumer harm, for example the ease of accessing payday loans via mobile applications. Some friction is desirable to enable better consumer decision making, particularly for potentially harmful products.

Thirdly, an opt out approach shifts the “burden” of friction away from the business interest and places it upon the Joint Account Holder B. That is: the friction that the FinTech sector is complaining - Joint Account Holder A having to wait for Joint Account Holder B to initiate consent - is borne by Joint Account Holder B who now needs to engage with, understand and act. It undermines consumer control and oversight³ since the status quo bias is likely to mean that most consumers are unlikely to act to oversee and control when given a notification for sharing data. A positive, voluntary, express and informed act of consent under an opt-in regime is a more meaningful and effective act of control and oversight in this way.

- *transaction costs increase for data collectors*

The consultation paper also states that an opt in regime:

also introduces technical implementation complexity for CDR participants, and may ultimately lead to longer implementation timeframes as the CDR expands across sectors.

Here in lies one of the key reasons an opt-out approach places business interests over consumer interest in privacy and express consent. It may be more costly to do so and therefore prevent businesses from joining the CDR framework.

However, lowering transaction costs should not be implemented at the cost of safety and security of Australians. This is particularly the case for people’s sensitive financial data.

Authorising safe and secure access to this data is the key goal for the CDR regime. Lowering safety and security around the handling of financial data for the sake of developing a new market for FinTechs is not.

³ listed as a factor at para 10

- **An opt-out model will undermine consumer trust in CDR**

There is still very little evidence supporting consumer interest in Open Banking and other potential use cases for the Consumer Data Right. There has so far been minimal take-up in offers available since July 2020 and UK experience is such that their consumer uptake for Open Banking services is limited.⁴ Whatever interest there is in expanding the CDR is purely supply driven in the hope that a market can be created to support a fledgling sector. In other words, the FinTech sector is seeking the loosening of consent, and privacy interests to help build a viable FinTech sector. This is short-sighted thinking as it will ultimately undermine trust in the CDR.

There is in fact very strong evidence that consumers want a safe and secure data environment. The majority of Australians do not want companies sharing their information for secondary purposes. According to OAIC's 2020 Community Attitudes to Privacy survey the vast majority of Australians indicated they were uncomfortable with most types of information being shared with third parties:

Australians are increasingly questioning data practices where the purpose for collecting personal information is unclear, with 81% of Australians considering 'an organisation asking for information that doesn't seem relevant to the purpose of the transaction' as a misuse (up 7% since 2017).⁵

The OAIC survey also found overwhelming consumer demand for stronger action from government with respect to privacy protections:

Eighty-three percent of Australians would like the government to do more to protect the privacy of their data.⁶

Any moves to do undermine consent and strong privacy standards will inevitably undermine any potential success of the CDR by undermining trust in the system. This deeply flawed proposal sets the FinTech sector and the CDR regime up for failure. This is because any potential for trust or confidence in the CDR regime will be damaged from the very start and be given a mortal blow with the first breach of data privacy.

- **The proposed risk mitigations do not remove the risks.**

The Treasury Consultation Paper proposes the following 'risk mitigations' proposes the following approaches that act somewhat to ameliorate the obvious problems that arise from the proposal to opt out.

⁴ Finextra, Open Banking year two: Insights from the CMA9
<https://www.finextra.com/newsarticle/35054/open-banking-year-two-insights-from-the-cma9>

⁵ OAIC Australian Community Attitudes to Privacy Survey 2020, Page 7
<https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-CommunityAttitudes-to-Privacy-Survey-2020.pdf>

⁶ OAIC Privacy Survey, Page 8

1. Either joint account holder would be able to override this default setting at any time and change data sharing to 'off' if desired
2. Joint account holders would continue, as per the current rules, to have knowledge of other account holders' sharing and would receive notifications of new sharing arrangements and the ability to stop particular sharing arrangements
3. Data holders should be encouraged (but should not be required) to notify consumers of default CDR data sharing settings on their joint account. This could allow data holders to leverage notifications in their internet banking apps or emails informing joint account holders of default CDR data sharing settings.

With respect to the first point, this requires joint account holders who will be otherwise unaware of the default setting or even the existence of the consumer data right, to be actively engaged. As behavioural economics, the status quo bias, and the lack of extant consumer interest in the CDR shows – it is highly unlikely most people will engage with the settings unless forced to so.

With respect to being notified of new sharing arrangements – this too will require uninterested parties to take active steps to read, understand, decide and act. This occurs in an opt in model as well but in an opt out model, the tendency of people to again not engage with such notifications will mean more people will not take the sufficient steps to engage to overturn their assumed consent. It may also lead to a higher likelihood of financial abuse. See further below.

Finally, with respect to merely encouraging data holders to notify consumers of default CDR data sharing – this further undermines the need for a consumer to provide *informed* consent. This suggests that it is not even a requirement to proactively inform the consumer.

- **The opt out approach increases risks to those subject to financial abuse, elder abuse, or domestic or family violence.**

Financial abuse, be it in the form of elder abuse, domestic or family violence or any other abuse is a serious issue for a significant number of Australians. And it is inevitable that financial abuse perpetrators will engage with the CDR that either initiate or perpetuate such abuse.

There are a number of scenarios that need to be considered under the CDR since perpetrators can be in the position of initiating engagement with the CDR (ie as a JAH-A) or in the position of the non-initiating joint account holder (ie as a JAH-B), and vice-versa, with an abuse victims⁷ in the position of initiating engagement of in the position of non-initiating party.

In summary:

- A perpetrator can act as JAH-A and initiate engagement with the CDR and data sharing for potentially abusive purposes (such as seeking out more loans, different services that may cost a lot and be of no benefit to the victim). A victim JAH-B subject to potential

⁷ We use the word “victim” for brevity’s sake through this section but this should be read to encapsulate victims, survivors and people experiencing abuse.

abuse who has not been flagged, or self-identified by a Data Holder (**DH**) can be alerted to the sharing and then decide to act or not act as the case may be. A victim JAH-B subject to potential abuse who *has* been flagged, or self-identified by a DH can prevent the data sharing from occurring in the first place, and may or may suffer consequences as a result.

- Similarly a victim can act as a JAH-A and initiate engagement with the CDR and data sharing to potentially look for options to escape abuse, or manage or administer their situation after leaving an abusive situation. A victim JAH-A either has or has not been flagged, which will may lead to the perpetrator JAH-B being alerted or not alerted, as the case may be.

Both of these scenarios can empower or disempower a victim/perpetrator in varying ways but these are dependent upon whether there is an Opt Out or Opt In regime.

In an opt-out regime, as proposed:

- A victim JAH-B will by default be opted in to sharing data
- A perpetrator JAH-A will therefore be able to seek out further financial services to potentially perpetrate financial abuse, without needing to obtain the consent of the victim JAH-B.
- This abuse could be prevented if JAH-B has been flagged or self-identified prior to the perpetrator engaging with the CDR.
- A victim JAH-B who has not been flagged or self-identified to the DH will be alerted to the CDR engagement but no consent or action is required for the sharing to take place. They may or may not take steps to reject, inquire or self-identify to the DH at this point.
- The perpetrator JAH-A therefore does not have to pressure a victim JAH-B, and the friction or hurdle of obtaining consent from the victim JAH-B is lost. This essentially makes it easier for perpetrator JAH-A to potentially initiate abuse.
- A victim JAH-B needs to engage and understand what is happening in order to act to reject the data sharing. They could do so merely as a reaction against the perpetrator's act but it requires an affirmative act to reverse the initiation.
- A victim acting as a JAH-A could potentially use a CDR app to seek out financial service options to assist in escaping financial abuse or supporting the process after escaping. A victim JAH-A would still need to alert the DH or ADR that she is subject to abuse in order to not alert the perpetrator JAH-B. A victim JAH-A may make a mistake and initiate engagement in the CDR, alerting the perpetrator JAH-B because they have not flagged themselves.

In an opt-in regime:

- A victim JAH-B will by default be opted out of sharing data
- A perpetrator JAH-A will therefore be unable to seek out further financial services to potentially perpetrate financial abuse, without needing to obtain the consent of the victim JAH-B.

- A victim JAH-B will be alerted to the CDR engagement if they have not been flagged and will have to provide consent. They may or may not accept, they may make their own inquiries inquire or even self-identify to the DH at this point if that is available. However by not acting, their data is not shared.
- A perpetrator JAH-A could pressure a victim JAH-B into consenting but it is at least one hurdle that they would need to leap in order to initiate any abuse.
- Just as in the opt-out scenario, a JAH-B could prevent data sharing by having been flagged or self-identified prior to the perpetrator engaging with the CDR.
- Just as in the opt-out scenario, a victim JAH-A could potentially use a CDR app to seek out financial service options to assist in escaping financial abuse or supporting the process after escaping. The JAH-A will still have to be flagged or self-identify in order for the perpetrator to not be alerted, just as in the opt-out scenario.

Under both scenarios there are varying outcomes for the victim JAH-A when initiating engagement with the CDR but these are generally the same and require similar flagging or self-identification rules to prevent poor outcomes for the victim survivor.

However the key difference between the two scenarios is that under the opt-in scenario there exists a hurdle (or “friction”) for a perpetrator JAH-A to lead to initiate engagement with the CDR by needing the consent of the partner and any potential subsequent financial abuse. The opt-out scenario removes the hurdle to abuse, merely alerting the victim. Similarly, the opt-in scenario requires inaction from the victim to delay or prevent data-sharing, the opt out scenario requires the victim to act after the fact.

It should also be noted that a perpetrator (or potential perpetrator) is in our view more likely to initiate financial abuse through initiating changes to a couple’s finances, than a person subject to abuse is likely to use the CDR to seek out assistance, since the victim is more likely to seek assistance from social services including financial counsellors.

The former supports the very real potential for a perpetrator to search for, instigate or continue the abuse, the latter seeks to undo abuse or escape. In other words, an opt-in model can act as a measure to help prevent the harm from happening in the first place. An opt out approach, places the burden on the person subject to abuse to act to prevent the abuse.

The final key difference between the opt in and opt out approaches is that in an opt-in regime, a victim maintains their autonomy and power by holding their right to express, informed consent to initiating data sharing in the first place. An opt-out regime takes this away from them and requires them to act in response.

Weak risk mitigants

The “range of existing protections in the CDR rules to protect vulnerable consumers” currently is inadequate and would need to be bolstered considerably under either an opt in or opt out regime.

There remains no requirement for DHs or ADRs to have physical or financial harm or abuse flags system in place.

Nor is there a requirement that a simple way to communicate to a DH or ADR that a consumer may flag themselves as potentially subject to abuse. While some banks do have processes in place – not all do, and there is little evidence of the FinTech sector introducing such processes unless required. Consumers already regularly find it difficult to get in contact with the makers of Apps, digital services and other software – with no phone numbers and in some cases no emails – or if they are they may be difficult to find or not answered quickly.

How are data holders going to be able to invoke the CDR rules re: the threat of physical or financial harm or abuse, if they don't know about it and how will they know about it if there isn't a requirement for a contact form to enable one joint holder to inform them or a requirement to proactively identify an issue.

We recommend that the CDR rules require all CDR participants to have internal processes in place to flag consumers who are subject to abuse, both for those who self-identification as subject to abuse and through the proactive identification of signs of abuse.

We also recommend that the CDR rules require all CDR participants to include clear communication channels for consumers to self-identify and seek assistance and that this be included under the CX design standards.

While acting to require contact forms, flagging processes or proactive identification of abuse may assist, it is clear that these mitigation strategies cannot be the full solution. Preventing the harms occurring in the first place is preferable, and an opt in approach is more effective than an opt out approach.

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Drew MacRae, Senior Policy Officer, Financial Rights on (02) 8204 1386 or at drew.macrae@financialrights.org.au

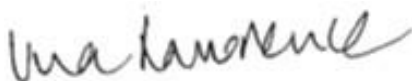
Kind Regards,



Karen Cox
Chief Executive Officer
Financial Rights Legal Centre



Katherine Temple
Director Policy & Campaigns
Consumer Action Law Centre



Una Lawrence
Director of Policy
Australian Communications Consumer Action
Network