23 July 2021

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

Dear Ms O'Rourke,

Consumer Data Right rules amendments (version 3)

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**), the Public Interest Advocacy Centre (**PIAC**), and the Australian Privacy Foundation (**APF**).

This submission will address our ongoing concerns with the intention to introduce rules with respect to:

- "trusted advisers"
- CDR insights; and
- joint accounts.

We are strongly opposed to these proposed rules amendments. Many of these concerns have been outlined in previous submissions on the matter[1] however we raise the following additional points:

[1] Financial Rights submission to ACCC re: Changes to Consumer Data Right rules, October 2020 https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf and Financial Rights Legal Centre, Consumer Action Law Centre and the Australian Communications Consumer Action Network on Australian Treasury's 'Opt-out' joint account data sharing model, May 2021, https://financialrights.org.au/wp-content/uploads/2021/05/210526_TreasuryCDROptoutModel_FINAL.pdf

- the proposed consumer protections/risk mitigations are entirely inadequate to address the real concerns raised by consumer representatives
- independent Privacy Impact Assessment processes are either incomplete or non-existent and have not been conducted early enough to influence the project design.

With specific reference to the proposed joint account rules we further note that :

- vulnerable consumers are unable to avail themselves of the minimal protections under the CDR Rules;
- the FinTech's sector's claim that an opt-out consent model is safer for victims of financial abuse is wrong and is self-interested;
- a right to transfer data is fundamentally different to the current bundle of rights to transact under a joint account;
- designing CDR Rules to merely reflect current unsafe and insecure data sharing capabilities does not fulfil the promise of the CDR to provide a safe and secure data environment for consumers;
- it is unclear whether all joint account holders will have the ability to delete or de-identify data shared after the fact.

With these three new proposals CDR now bears almost no relationship to the original promise. The effect of these recommendations is one of incremental privacy intrusion and scope creep such that it is becoming increasingly unsafe to use and consumer representatives may be in no other position but to advise consumers – particularly vulnerable consumers - to opt out of the CDR with respect to any interactions relating to joint accounts, "trusted advisers" and CDR insights.

We make the following recommendations:

1. Treasury must delay proceeding with the introduction of proposed new CDR rules re: "trusted advisers" until at least:
    a) an independent Privacy Impact Assessment has taken place,
    b) the proposed rules are reconsidered and redrafted in the light of the risks and recommendations identified and
    c) a new, strengthened *Privacy Act* is introduced as is currently being considered in the Attorney General Department's review of the *Privacy Act*.
2. As a part of this process, Treasury should also:
    a) require that "trusted advisers" meet minimum security standards of the CDR and the meet the Privacy Safeguards;
    b) alternatively, at a minimum, only allow CDR Data to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.
    c) alternatively, develop a data enclave structure for trusted advisers.

3. Treasury must delay proceeding with the introduction of proposed new CDR rules re: "CDR insights" until at least:

   a) a new independent Privacy Impact Assessment has taken place,

   b) the proposed rules are reconsidered and redrafted in the light of the risks and recommendations identified.

   c) a new, strengthened *Privacy Act* is introduced as is currently being considered in the Attorney General Department's review of the *Privacy Act*.

4. As a part of this process, Treasury should:

   a) require CDR participants to automatically provide consumers with the right to know what the insights are;

   b) require the Data Standards Body to consumer test and benchmark CDR insight standards to ensure consumers (including vulnerable consumers) genuinely understand what they are agreeing to;

   c) require the Data Standards Body to consumer test and benchmark CDR Insight standards to ensure consumers (including vulnerable consumers) are protected from pressure being placed on them to agree to sharing their CDR insights; or

   d) alternatively require ADRs to undertake this consumer testing and benchmarking on each CDR insight that they seek to rely upon.

5. The 'opt-out' model for joint accounts should be rejected and the current opt-in model be maintained

1. **"Trusted Advisers"**

Consumer representatives have previously raised our concerns with the proposal to allow so-called "trusted advisers" to gain access to sensitive financial data via the CDR.[2] In summary these concerns are:

- Disclosure to a "trusted adviser" is not just inherently risky but is contrary to the entire point of the CDR to provide a safe and secure data environment by not applying the same CDR privacy safeguards to the collection, holding and use of this data by the "trusted adviser";
- Referring to so-called "trusted" advisers is misleading since many will be unable to provide nor be required to provide a safe and secure data environment;
- Disclosure to "trusted advisers" facilitates and locks in the creation of two data protection regimes – one safe and secure environment, one with fewer, if any, consumer protections;
- Voluntary consent is undermined – insights from behavioral psychology suggest people who rightly (or wrongly) trust their adviser will simply do what the so-called "trusted" adviser will ask them to do;
- CDR consumers will genuinely not understand the privacy and security implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR;
- There are no additional restrictions placed on what non-accredited parties can subsequently do with CDR data once obtained;
- The high cost of accreditation should not outweigh the need for a safe and secure environment.

In addition to these we wish to highlight the following concerns we have with the current proposal:

- ***The proposed consumer protections/risk mitigations are entirely inadequate to address the real concerns raised by consumer representatives***

The proposed risk mitigations or consumer protections fail to address all of the above concerns. The handful of "consumer protections" include:

> *"[A]n ADR cannot disclose CDR data to a trusted adviser unless it has taken reasonable steps to confirm the person to whom the data is to be disclosed is a member of a class of trusted advisers set out in the CDR Rules."*[3]

Reasonable steps is as yet undefined and simply has the practical effect of shifting liability away from the ADR on to the "trusted adviser." For example, the explanatory materials suggest that

---

[2] Financial Rights submission to ACCC re: Changes to Consumer Data Right rules, October 2020 https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf

[3] Page 15 Treasury, Exposure Draft Explanatory Materials.

reasonable steps might include 'seeking confirmation from the trusted adviser'. This does not bolster the safety and security standards applied to the holding and use of sensitive financial data.

Relying on fiduciary duties and best interests duties is a misdirection. Fiduciary rules *are not the same as* the strengthened CDR privacy safeguards, accreditation standards and consumer protections offered by the CDR regime. The consumer will not be able to rely on the strengthened CDR Privacy Safeguards if something were to go wrong, and, in a great number of cases, will not be able to rely on the privacy protections and rights provided under the current *Privacy Act* due to their lack of application to many of the "trusted advisers" identified. The promise of a safer data access regime is entirely undermined by the proposal.

> *The transfer of the CDR data from an ADR to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules, including the requirement to ensure that data is encrypted in transit.* [4]

While this addresses one of the concerns raised in the Privacy Impact Assessment[5] this does nothing to provide security controls to CDR data *once it leaves* the CDR regime.

> *disclosures are subject to CX standards to be made by the Data Standards Body (rule 8.11(1)).*[6]

We remain in agreement with the Maddocks PIA that CDR Consumers will not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR. It is highly likely that in the vast majority of cases consumers will not know what the risks and consequences of sharing their data outside of the protections of the CDR regimes.

> *When the ADR discloses the CDR data to a trusted adviser, the ADR must update each consumer dashboard that relates to the request to indicate what CDR data was disclosed, when it was disclosed and the name of the trusted adviser it was disclosed to (rule 7.9(3)).* [7]

This merely provides a post-facto paper trail to prevent ADRs being held liable and to identify how any harm may have taken place arising out of CDR data a customer consented to providing to a bad actor. It does nothing to prevent any harm.

- ***Incomplete Privacy Impact Assessment process***

We note that the 2020 independent Privacy Impact Assessment of the original ACCC consultation on trusted advisers (and CDR insights) recommended the following:

[4] Page 15 Treasury, Exposure Draft Explanatory Materials.

[5] Recommendation 18, Maddocks, Consumer Data Right Regime – Update 2 to Privacy Impact Assessment https://www.accc.gov.au/system/files/CDR%20v2%20Rules%20%E2%80%93%20Update%202%20to%20Privacy%20Impact%20Assessment.pdf

[6] Page 15 Treasury, Exposure Draft Explanatory Materials.

[7] Page 15 Treasury, Exposure Draft Explanatory Materials.

17 Disclose CDR Data and/or CDR Insights only to entities who comply with the APPs

We recommend that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.

In response, the ACCC stated that:

> *The final rules did not include the proposed rule amendments to permit the disclosure of CDR Data or CDR Insights to non-accredited persons.*[8]

However, the current new proposed set of rules put forward by Treasury *does* permit the disclosure of CDR Data or CDR Insights to non-accredited persons.

The new proposed rules essentially introduce a policy that is antithetical to the recommendation of the 2020 independent Privacy Impact Assessment and does not provide any response to this recommendation or reason why it has been rejected – in line with the OAIC's *Guide to undertaking privacy impact assessments* with respect to responding to Privacy Impact Assessment recommendations.[9]

Given this, we believe a new Privacy Impact Assessment should have taken place to consider the risks already identified and any new risks arising from the new rules.

It is important to reiterate the identified risk and gaps involved. The 2020 independent Privacy Impact Assessment identified that

> *Risk 23 - The proposed amendments will make it easier for CDR Data or CDR Insights to be disclosed outside of the CDR Regime, where the data will have less privacy protections (or potentially no privacy protections) than the same data will have when within the CDR Regime.*

The Assessment goes on to state:

> *We note that the proposed amendments will allow the disclosure of CDR Data and CDR Insights to recipients who are not Data Holders or Accredited Persons (and do not have any obligations under the CDR legislative framework). These recipients may not even have any obligations under other privacy legislation (i.e. the recipient does not need to be an APP entity for the purposes of the Privacy Act, or have otherwise agreed to comply with the APPs). It is important that CDR Consumers understand that if their CDR Data, or a CDR Insight, is disclosed to a Trusted Adviser or an Insight Recipient, that information will be disclosed outside the CDR regime. This means that the information, once disclosed, will not be afforded the protections offered by the CDR Rules (and, in particular, the Privacy Safeguards). Additionally, it is important that CDR Consumers understand that CDR Data and CDR Insights may be disclosed to recipients that do not have obligations under any privacy legislation.*
>
> *We recommend that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity*

---

[8] https://www.accc.gov.au/system/files/Attachment%20B%20-%20ACCC%20response%20to%20update%202%20to%20Privacy%20Impact%20Assessment.pdf

[9] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/#s10-respond-and-review

These risks and recommendations have been neither mitigated against nor responded to by Treasury.

- ***Data enclaves should be created to for advisers to access***

Data enclaves are the obvious solution to the issues outlined above with the current "trusted adviser" model. As Treasury would be aware, a data enclave is a secure CDR network through which sensitive financial data can be stored. Data enclaves are already foreseen with respect to ADRs working with third parties. This concept should be applied to the Trusted Adviser problem. Data enclaves should be created to service those "trusted advisers" who wish to access CDR data. That is, for example, an accountant should only be able to access, analyse and use CDR data via a data enclave or application that is created and controlled by an ADR that meets all the security standards and privacy safeguards. In this way:

- CDR data will remain within the CDR regime and not fall outside of it;
- consumers will still be able to rely on the protections and safeguards built into the CDR regime;
- "trusted advisers" can access CDR data and provide the same services as they currently do;
- sensitive CDR data will be held in a safe and secure way;
- "trusted advisers" will not have to maintain the security standards by receiving raw CDR data and holding it on their own servers or computers;
- ADRs can build and provide the necessary applications that provide a safer, faster and more convenient way for trusted advisers to provide necessary services
- the FinTech sector will build a market for their wares, leveraging off the safety and security that a CDR data enclave provides for consumers.

Recommendations

1. Treasury must delay proceeding with the introduction of proposed new CDR rules re: "trusted advisers" until at least:
   a) an independent Privacy Impact Assessment has taken place,
   b) the proposed rules reconsidered and redrafted in the light of the risks and recommendations identified and
   c) a new, strengthened *Privacy Act* is introduced as is currently being considered in the Attorney General Department's review of the *Privacy Act*.[10]
2. As a part of this process, Treasury should also

[10] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

a) require that “trusted advisers” meet minimum security standards of the CDR and the meet the Privacy Safeguards;

b) alternatively, at a minimum –only allow CDR Data to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.

c) Alternatively, develop a data enclave structure for trusted advisers.

2. CDR Insights

As with the issue of Trusted Advisers, consumer representatives have previously raised our concerns with these proposals.[11] In summary they are:

- Consumer Insights can be more sensitive than raw data;
- The Consumer Insights rules place all the responsibility on the consumer;
- Consumers will not have the automatic right to know what the insights are;
- Consent from vulnerable consumers is unlikely to be free or fully informed.

In addition to these, we wish to highlight the following concerns we have with the current proposal:

- ***The proposed consumer protections/risk mitigations are not enough to address the concerns raised by consumer representatives***

While we note that Rule 1.10A(3) limits an insight disclosure consent to four purposes, i.e:

(a) identifying the consumer;

(b) verifying the consumer's account balance;

(c) verifying the consumer's income;

(d) verifying the consumer's expenses

we do not think that this addresses all of the risks raised by the independent Privacy Impact Assessment. See further below.

The other consumer protections introduced by Treasury include:

> *Rule 4.11(3)(ca) requires an accredited person to give an explanation of the CDR insight to the CDR consumer when seeking the insight disclosure consent that will make it clear what the CDR insight would reveal or describe. The CDR Rules do not require a CDR insight to be shown to a consumer prior to it being disclosed.*

Being given an explanation of what the CDR insight would reveal is not the same as consumers having the automatic right to know *what the insights are* – just what they *would* reveal. For example, a consumer would be told that their account balance or total expenses will be provided to a third party but the ADR will not be required to tell the consumer what the account balance or expenses are – specific insights that may be important to know if it leads to negative consequences for the consumer. This is not in line with the core aim of the CDR to give consumer access to and control over their information.[12] It is also not clear what the problem is with informing the consumer what the insight actually is. Treasury then states:

---

[11] Financial Rights submission to ACCC re: Changes to Consumer Data Right rules, October 2020 https://financialrights.org.au/wp-content/uploads/2020/10/201029_ACCCCDRRulesexpansion_Sub_FINAL-1.pdf

[12] See Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019* https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6370_ems_ce513d68-7222-49f4-a2fe-67e1c2b32fed/upload_pdf/712911.pdf;fileType=application%2Fpdf

> *However, where practical, this step could be taken to assist the consumer's understanding of what the CDR insight would reveal or describe and help meet the accredited person's obligation under rule 4.11.*

But this is not a requirement – simply a suggestion.

> *Under rule 7.5A(5), even if an insight disclosure consent is given, the accredited person is not permitted to disclose the CDR insight if it includes or reveals* ***sensitive information*** *within the meaning of the Privacy Act 1988.*

This is a positive step but a consumer can only know if this has been breached if they are provided with the actual insight shared.

> *Rule 8.11(1)(c)(v) contains new requirements for data standards to be made about disclosure and security of CDR data that is disclosed in a CDR insight, and the processes by which insight disclosure consents are obtained, including ensuring the consumer understands their data will leave the CDR system and explaining the CDR insight in accordance with rule 4.11 (rule 8.11(1A).*

This too is a positive step – however placing the responsibility all on the consumer – particularly vulnerable consumers potentially pressured into providing consent - to understand the privacy and security implications of consenting to disclosure of CDR Data is wholly inadequate and unlikely to mitigate the risks of harm. No proposals have been put forward that demonstrate data standards can ensure consumer will understand these risks. It is also not 100% clear that there will be restrictions on the use of the insights including primary and secondary uses of this data, how it will be stored, and whether it will be deleted.

In fact, it has already been made clear by ASIC that disclosure should no longer be relied on a consumer protection.[13] As Deputy Chair Karen Chester said:

> *'It's time to 'call time' on disclosure as the default consumer protection. It's not the 'silver bullet' once thought, nor should it be relied upon as one. Disclosure can and has backfired in unexpected and harmful ways … 'Our report highlights the need to rebalance the onus from consumers to firms – to become a shared responsibility.*[14]

It is therefore disappointing that Treasury is perpetuating the myth that mere disclosure can act as the silver bullet to protect consumers in the Consumer Data Right.

If this proposal were to move forward, we would want to see thorough consumer testing that demonstrates that the standard does in fact empower vulnerable consumers. That is, it needs to be shown that they genuinely understand what they are agreeing to and there is no possibility of pressure to undermine the voluntariness of the decision.

---

[13] *REP 632 Disclosure: Why it shouldn't be the default*, https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/

[14] ASIC 19-279MR ASIC 'calls time' on disclosure reliance, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-279mr-asic-calls-time-on-disclosure-reliance/

- ***Incomplete Privacy Impact Assessment process***

We note that the 2020 independent Privacy Impact Assessment of the original ACCC consultation on trusted advisers (and CDR insights) recommended the following:

> *19 Consider appropriateness of CDR Insights in the CDR regime*
>
> *We recommend that the ACCC:*
>
> - *consider:*
> - *whether it is appropriate for CDR Insights to be part of the CDR Regime in circumstances where there is a significant risk that vulnerable CDR Consumers may be pressured into providing an Insight Disclosure Consent, or may otherwise not fully understand the potential negative consequences that their consent may have; or*
> - *if the ACCC determines that it is appropriate for CDR Insights to remain within the scope of the CDR Regime, implementing mechanisms to ensure that vulnerable CDR Consumers are giving free and fully-informed Insight Disclosure Consents; and*
> - *consider whether it is generally appropriate for CDR Insights to be generated and disclosed as part of the CDR Regime. This is because of the inherent risks associated with the disclosure of the results of the analysis of raw CDR Data.*

As with the "Trusted Adviser" recommendations, the ACCC responded with the following:

> *The final rules did not include the proposed rule amendments to permit the disclosure of CDR Data or CDR Insights to non-accredited persons.*[15]

However, the current new proposed set of rules put forward by Treasury does now permit the disclosure of CDR Data or CDR Insights to non-accredited persons. It therefore introduces a policy that goes against the recommendation of the 2020 independent Privacy Impact Assessment and does not provide any response to this recommendation.

Again, it is important to reiterate the risk and gaps with CDR Insights. In addition to Risk 23 described above, the 2020 independent Privacy Impact Assessment identified that

> *Risk 24. Consent from vulnerable CDR Consumers*
>
> *There is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully informed.*
>
> *We note that there is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully-informed, particularly in circumstances where the CDR Consumer:*
>
> - *may not understand the negative consequences that may flow from giving their Insight Disclosure Consent (i.e. that the disclosure of the CDR Insight to another person may result in the CDR Consumer being refused access to goods or services); or*

[15] ACCC response to final Privacy Impact Assessment - version 2 of the CDR rules https://www.accc.gov.au/system/files/Attachment%20B%20-%20ACCC%20response%20to%20update%202%20to%20Privacy%20Impact%20Assessment.pdf

- *may be pressured into providing their Insight Disclosure Consent by a potential provider of goods or services.*

25. CDR Insights may be more invasive than sharing raw CDR Data

There is a risk that sharing a CDR Insight about a CDR Consumer may be as, or more, invasive than sharing a CDR Consumer's raw CDR Data.

We note that CDR Insights contain the results of the analysis of raw CDR Data. Therefore, CDR Insights contain information that is more sensitive than raw CDR Data alone.

It is our view that these risks have yet to be adequately mitigated and there is no direct response from Treasury with respect to these risks.

Recommendations

3. Treasury must delay proceeding with the introduction of proposed new CDR rules re: "CDR insights" until at least:
   a) a new independent Privacy Impact Assessment has taken place,
   b) the proposed rules are reconsidered and redrafted in the light of the risks and recommendations identified.
   c) a new, strengthened *Privacy Act* is introduced as is currently being considered in the Attorney General Department's review of the *Privacy Act*.[16]
4. As a part of this process, Treasury should also:
   a) require CDR participants to automatically provide consumers with the right to know *what the insights are*;
   b) require the Data Standards Body to consumer test and benchmark CDR insight standards to ensure consumers (including vulnerable consumers) genuinely understand what they are agreeing to;
   c) require the Data Standards Body to consumer test and benchmark CDR Insight standards to ensure consumers (including vulnerable consumers) are protected from pressure being placed on them to agree to sharing their CDR insights. or
   d) alternatively require ADRs to undertake this consumer testing and benchmarking on each CDR insight that they seek to rely upon.

[16] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

3. Joint Accounts

We remain strongly opposed to the proposal to establish an 'opt-out' model for joint accounts by setting the pre-approval disclosure option at Rule 4A.4 as the default.

We do so on the same bases as outlined in our previous submission on the matter[17], that is:

- Default pre-approval fundamentally contradicts the consent model central to the CDR – that is, consumer's consent should be voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn.
- Default pre-approval runs counter to current privacy principles and the ACCC's recommended intention to strengthen consent requirements and pro-consumer defaults
- Default pre-approval wrongly equates one's transaction preferences with their privacy preferences
- Default pre-approval places the business interests of the FinTech sector over the interests of consumers
- Default pre-approval will undermine consumer trust in CDR
- There are no risk mitigations that will remove the risks.
- Default pre-approval will increase risks to those subject to financial abuse, elder abuse, or domestic or family violence.

We note that Treasury have not acted to adequately mitigate any of the risks and concerns raised by consumer representatives. On this we wish to raise the following further points/concerns.

- ***Treasury has initiated a late Privacy Impact Assessment on the opt-out model counter to OAIC guidance and good public policy development***

To date there has yet to be a public and independent privacy impact assessment for the proposals being put forward with respect to the opt-out model. We note that Treasury's May 2021 proposals for an opt-out consent model for joint accounts – now being implemented with these new draft rules – are substantially different to the proposals consulted on by the ACCC in late 2020. We note that the ACCC produced and consulted on an independent privacy impact assessment at the same time as they released the consultation paper.

No such Privacy Impact Assessment has been released by Treasury on the opt-out approach or the new draft rules. We understand that there is a "privacy roundtable" being held by Treasury which will feed into a still to be drafted Privacy Impact Assessment but there is no clarity on this and the Assessment's ability to influence the outcome of the process. Stakeholders have also previously been given the opportunity to provide input into a Privacy Impact Assessment

[17] Financial Rights Legal Centre, Consumer Action Law Centre and the Australian Communications Consumer Action Network on Australian Treasury's 'Opt-out' joint account data sharing model, May 2021, https://financialrights.org.au/wp-content/uploads/2021/05/210526_TreasuryCDROptoutModel_FINAL.pdf

directly to the independent assessor separate to any meetings with Treasury. This does not seem to be the case this time.

Conducting an independent Privacy Impact Assessment after a decision has been made to move forward with a policy proposal and releasing and consulting on it *after* the release of draft new rules and draft explanatory materials is counter to the expected Privacy Impact Assessment process and counter to good public policy development. The OAIC's *Guide to undertaking privacy impact assessments*[18] process state:

> *To be effective, a PIA should be an integral part of the project planning process, not an afterthought. It should be undertaken* ***early enough in the development of a project that it is still possible to influence the project design*** *or, if there are significant negative privacy impacts, reconsider proceeding with the project. A PIA works most effectively when it evolves with and helps to shape the project's development, ensuring that privacy is considered throughout the planning process.*
>
> *Making a PIA an integral part of a project from the beginning means that you can identify any privacy risks early in the project and consider alternative, less privacy-intrusive practices during development, instead of retrospectively. Also, consistent and early use of a PIA ensures that all relevant staff consider privacy issues from the early stages of a project.*

The current policy development process is reminiscent of the inadequate privacy impact assessment process Treasury first conducted in 2018 – the last time Treasury had carriage of the Consumer Data Rights.[19] In this first Privacy Impact Assessment, Treasury decided not to outsource the development of the PIA to external consultants and conducted the Privacy Impact Assessment themselves. This was not in keeping with the recommendations of the OAIC in its Privacy Impact Assessment guidelines. Treasury at the time relented to criticism of this flawed process and engaged an independent Privacy Impact Assessment to take place – one that was far superior to the one Treasury conducted.[20]

It is therefore unfortunate that Treasury have chosen not to undertake an independent Privacy Assessment at a time early enough "to influence the project design." This should have occurred at the same time as the May 2021 consultation on the opt-out approach proposal and released with responses at the time any new draft rules were released – as occurred with Version 2 of the CDR Rules under the ACCC.

Given the critical importance of the joint account issue and the decision to move forward with an opt-out consent model in direct contradiction of the consent principles, it is incumbent upon Treasury to pause and delay any introduction of new rules, conduct an appropriately independent Privacy Impact Assessment with input from all stakeholders including consumer representatives, and develop a joint account policy that fully addresses the privacy risks of sharing joint accounts. We believe that the privacy risks of the opt-out approach and the

[18] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

[19] See Draft Treasury Privacy Impact Assessment Consumer Data Right December 2018 https://cdn.treasury.gov.au/uploads/sites/1/2018/12/CDR-PIA.pdf

[20] See Consumer Data Right: Maddocks, Privacy Impact Assessment (December 2019) https://treasury.gov.au/publication/p2019-41016

undermining of consent in the proposal cannot be fully mitigated for all the reasons we have outlined in this (and our previous) submission, and that this will be borne out in an independent Privacy Impact Assessment.

- ***In practice, vulnerable consumers are unable to avail themselves of the minimal protections under the CDR Rules***

We have previously raised the issue that there remains no requirement for DHs or ADRs to have physical or financial harm or abuse flag systems in place. Nor is there a requirement for DH or ADR to provide a simple mechanism for consumers to self-identify as vulnerable to potential 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 to do so. Consumers already 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. When such details are provided they are often difficult to find, or infrequently monitored resulting in delayed responses.

The question that we posed in our previous submission was:

> *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?*

The answer is in reality there is no way for consumers to be able to invoke the CDR rules re: the threat of physical or financial harm or abuse. This has been confirmed with us in discussion with Regional Australia Bank – the only non-big four bank and non-Australian Banking Association member to have been accredited under the CDR.

Regional Australia Bank has confirmed that they *do not* have a way to flag customers who may be subject to abuse. And they do not have a way for the customer to tell them except in a face to face meeting. Further, it is our understanding that they *don't* keep a record of the fact that a customer is subject to abuse and they do not flag them in their system as requiring protection even if they are told.

What this means is that there is *no way* for a vulnerable customer of Regional Australia Bank to avail themselves of the protections in the CDR rules (Rule 4.6) for the data holder to:

> *"consider it necessary, in order to prevent physical or financial harm or abuse, not to update the consumer dashboard of the other joint account holder to indicate the matters referred to in paragraphs 7.9(a), (b) and (c)."*

This is a serious concern that the only non-big 4 bank to be involved in the CDR so far *cannot* provide the minimal protection available to vulnerable consumers under the CDR as it stands. We appreciate that the big four banks have greater resources and have progressed further along the path of identifying and protecting vulnerable consumers than other smaller players. This clearly demonstrates, however, that relying on the flagging of vulnerable consumers as the cornerstone measure for mitigating this risk is set up for failure.

We note recommendation 16 of the independent Privacy Impact Assessment was that the ACCC:

- *consider ensuring that the CDR Rules prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure option process in JAMS is to apply (or that a notification need not be given); and*
- *continue to monitor the appropriateness of the measures in place in the CDR Rules to protect vulnerable CDR Consumers, including to investigate any additional measures that could be implemented to afford further protections.*

In its response stated that

> *The ACCC considered that the CDR Rules should not prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure options process in JAMS is to apply (or that a notification need not be given). The ACCC is aware that data holders currently have systems and procedures in place to identify vulnerable consumers. Prescribing a level of evidence that a data holder must be satisfied of before relying on an exception may:*
>
> - *undermine the procedures currently in place by data holders; and*
> - *introduce conditions that do not consider the individual circumstances of vulnerable consumers.*

It seems from the above information that the ACCC only considered the procedures of the four banks currently required to be a part of the CDR. These four banks are members of the ABA where they have committed to family violence policies under their Code of Practice and do have some systems and procedures in place.

No such commitments exist with other Data Holders – nor with FinTech ADRs who ultimately may become DHs under the regime.

We recommend that Treasury reconsider this recommendation and the ACCC response, taking into account the likely absence of adequate systems and procedures in place with other Data Holders to give effect to the mitigation measure.

- ***The FinTech's sector's claim that an opt-out consent model is safer for victims of financial abuse is misguided and self-interested***

In discussions with FinTech industry representatives it has been asserted to consumer representatives that an opt-out model is actually safer for potential victims of financial abuse. The argument – as we understand it - is as follows:

Under an opt-in regime (where affirmative consent is required by a joint account holder) a perpetrator may attempt to undertake financial abuse via the CDR. If this occurs the process alerts the victim and the victim can either consent or not consent. It is asserted by the FinTech sector that this is dangerous for the victim because the perpetrator will be angry if the victim does not consent or does not act, and will subsequently take it out on the victim, physically or otherwise.

However, again according to the FinTech sector, under an opt-out regime (where joint account holders are automatically opted-in to sharing data) if a perpetrator attempts to undertake financial abuse via the CDR, the process simply alerts the victim that the data is shared with no consent required. The victim is therefore less likely to enrage the perpetrator and be physically abusive.

The FinTech sector claim that there is now a paper trail of the abuse under the opt-out scenario.

What is wrong with this analysis?

Firstly, under the opt-in scenario - there will be perpetrators who see the need to obtain consent as a hurdle to undertaking the abuse and will be less likely to do so if they know they need to obtain consent. The FinTech sector has already acknowledged that requiring consent is a hurdle/friction.

The threat of physical abuse in the scenario put by the FinTech Sector can similarly arise under an opt-out regime where a victim seeks to actively deny the consent: see the examples of Bob and Erin in the Draft Explanatory Materials.[21] The difference is the harm is taking place automatically under an opt-out regime (i.e. data is automatically shared without the need for affirmative consent from the victim) while the victim has a potential to prevent the harm taking place in an opt-in scenario.

Defaulting pre-existing consent removes the agency from the victim from the beginning and forces them to act to reign in harm taking place – the opt-in empowers the victim to prevent the harm from taking place.

In every scenario there will always be a perpetrator who will explicitly and physically take action to force a victim to consent no matter what. For example, in situations of abuse where the victim still lives with the perpetrator and is under his thumb he will just force her to consent or take her phone and opt-in without even asking. This potential arises under either scenario.

In situations where a victim has escaped violence and is trying to piece her financial life back together the opt-in regime can give her some actual power to prevent further abuse and seek advice. This could be the trigger for her to close a joint account all together.

There is also a paper trail of abuse under both the opt-out and opt-in scenario – the paper trail in opt-out is longer since it involves the actual sharing of the data (and its potential harm) while the trail stops at the point of consent being required. (This is similar to the difference between fraud and attempted fraud).

Opt out fundamentally overturns the notion of voluntary express and active consent disempowering victims. It removes important rights from people who may be in abusive relationships on the basis of a misguided argument that this is for their own safety.

Ultimately the argument being put forward by the FinTech sector seems to primarily serve the interests of the sector to create a market for the sharing of data without the full consent of consumers, rather than any genuine accounting for the needs of vulnerable consumers who may be harmed by having their consent rights taken away from them.

[21] Page 20, Treasury, Exposure Draft Materials, https://treasury.gov.au/consultation/c2021-187223

- ***A right to transfer data is fundamentally different to the current bundle of rights to transact under a joint account***

The Productivity Commission's 2016 Data Availability and Use report argued for the need to introduce a *new* "right to transfer data" because there is "no such right to request the transfer of data to third parties."[22] This is the entire reason behind the need to introduce the Consumer Data Right in the first place – it is a right to transfer data or as we have repeatedly stated it is a "right to portability" in line with Article 20 of the EU's General Data Protection Right.

No such right currently exists with respect to one's financial data held with a bank – a joint account or otherwise. Yes there is the manual capability of exporting financial data via a pdf or CSV files to be shared but this is significantly different to the capabilities embedded in a right to transfer data or a right to portability. The differences are of substance, functionality, quality and quantity. The right to transfer involves data transfers that are:

- faster,
- easier,
- more reliable,
- machine readable,
- at higher volume transfers
- more consistent data standards, and
- able to be automatically analysed using a panoply of algorithmic tools for old and new purposes and thus with a higher value to the consumer and the industry.[23]

Consumers – including those with joint accounts - will rightly have different expectations about the ability to transfer or port their data in this way. These rights are currently not present under privacy law nor at contract under the terms and conditions of bank accounts.

These differences in expectation between a right to transfer and current manual sharing capabilities are only further exacerbated once the Consumer Data Right shifts from a portability right and capability to a portability and action initiation right and capability. Consumers will once again have different expectations with respect to consenting to such action.

Given the creation of this new right - we strongly believe that consumers with joint accounts will expect to - and should always be able to - consent to the transfer of the data under the Consumer Data Right.

[22] Page 202 Productivity Commission, Data Availability and Use, 2016 https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

[23] Further differences in the use of APIs over current methods are outlined in the Productivity Commission report see Page 564 https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

- ***Designing CDR Rules to merely reflect current unsafe and insecure data sharing capabilities does not fulfil the promise of the CDR to provide a safe and secure data environment for consumers.***

Treasury notes in the Exposure Draft Explanatory Materials that:

> *The Rules reflect current data sharing capabilities on joint accounts for PDF and CSV files. Currently joint account holders may independently share their joint account data in CSV or PDF format, or via screen scraping, without consent from or notification to the other account holders.*

The Consumer Data Right has been developed to provide a safer and more secure way of accessing and using one's own data. The Consumer Data Right Explanatory Memorandum states, that "strong privacy and information security provisions are a fundamental element of the CDR." However, the new proposed rules re: joint accounts, trusted advisers (without privacy safeguards) and CDR insights implement processes that for all intents and purposes maintain an insecure and unsafe status quo. In other words, the Government has spent over 5 years and many millions of taxpayer funds to introduce a system that is essentially no safer, no more secure and provides no further consumer protections than is currently the case in sending a PDF or CSV file.

- ***It is unclear whether all joint account holders will have the ability to delete or de-identify data shared after the fact***

It is unclear to us whether a joint account holder who has chosen to not consent to the continued sharing of data can have this data deleted after it has been provided. It is unclear how a joint account holder - who has been notified of the other joint account holder sharing the data – will be able to enforce their right to ask the ADR to de-identify or delete their data after the fact of sharing. This is particularly the case since they do not have the relationship with the ADR.

Recommendations

5. The 'opt-out' model for joint accounts should be rejected and the current opt-in model be maintained

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

Gerard Brody
Chief Executive Officer
Consumer Action Law Centre

Roger Clarke
Secretary
Austrlaian Privacy Foundation

Jonathon Hunyor
Chief Executive Officer
Pubic Interest Advocacy Centre