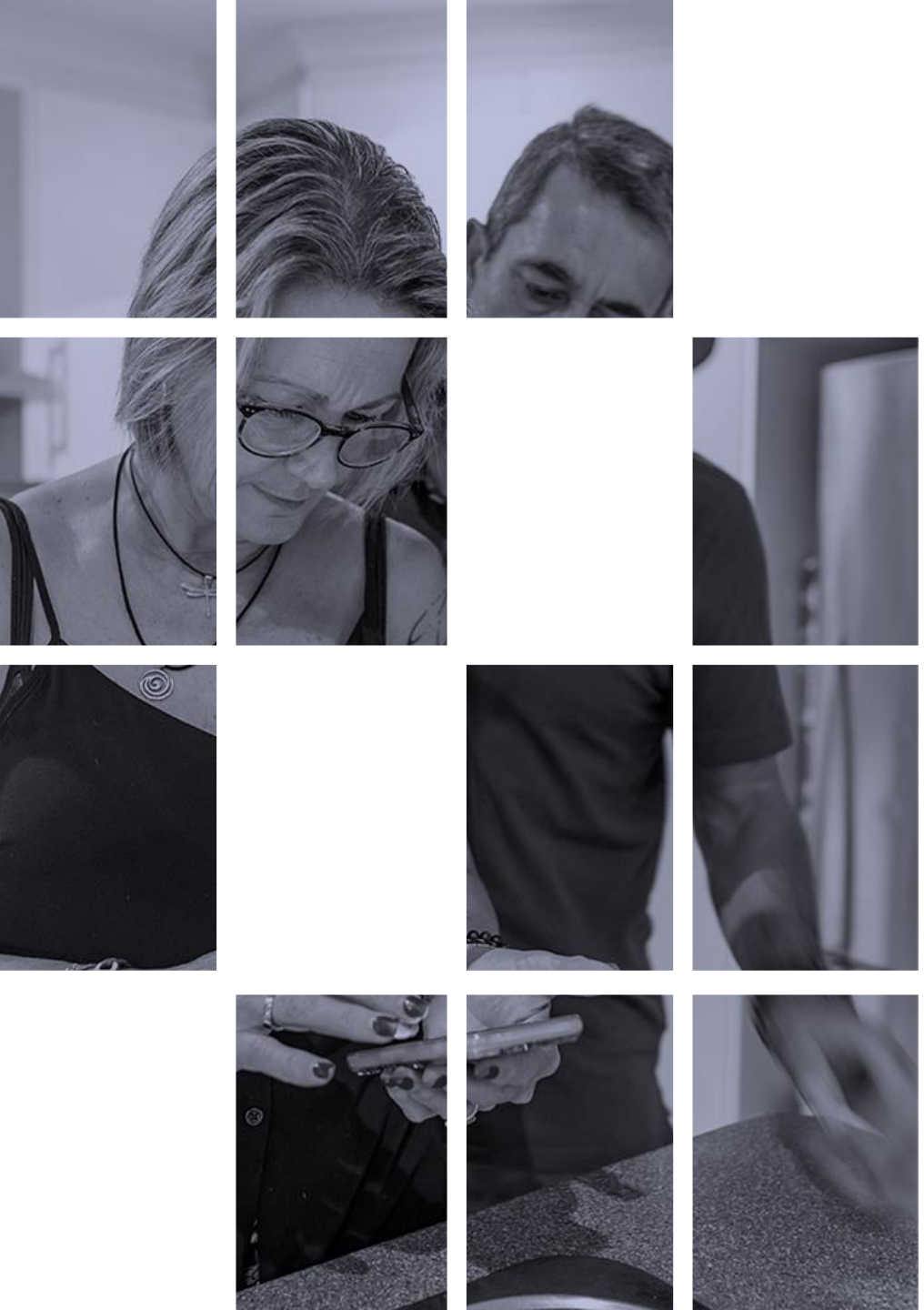


Joint accounts & the Consumer Data Right

PERSPECTIVES FROM COMMUNITY ORGANISATIONS & CONSUMER ADVOCACY

Report prepared by Nina Lewis, Consumer Policy Research Centre.

Consumer Policy Research Centre

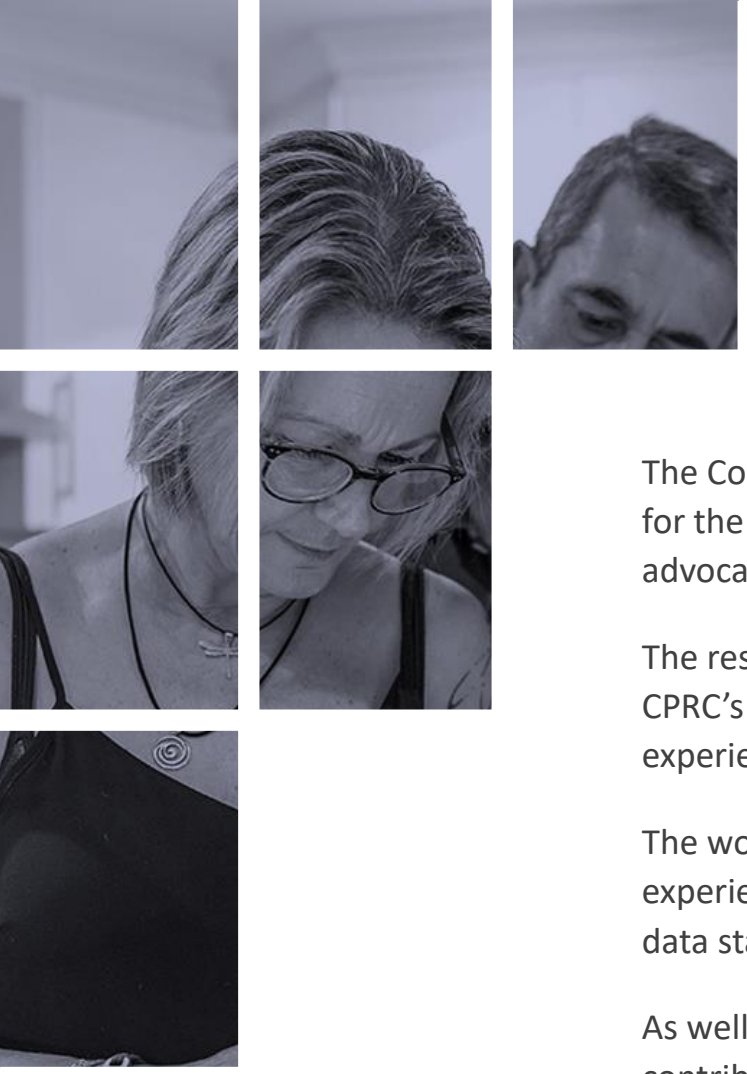
DATA STANDARDS CHAIR

Acknowledgement

This report is the product of many minds.

The Consumer Policy Research Centre thanks everyone who participated in the discussions that informed this document. We share our gratitude for your willingness to engage meaningfully on a complex subject at a time when COVID-19 has invoked new demands and challenges in the community sector.

In recognising the generosity of all involved, we further acknowledge this participation as a clear indication of the community sector's interest in contributing to the development of a Consumer Data Right that supports fair markets and positive outcomes for all consumers.



Background to the report

The Consumer Policy Research Centre (CPRC) has been engaged to prepare a series of consumer research reports for the Data Standards Body (DSB), on subjects identified as being priority topics by DSB, CPRC, consumer advocates and community groups.

The research derives findings through direct engagement with community sector stakeholders; reference to CPRC's broader consumer policy research activities; and analysis of existing material relating to consumer experiences of data markets, the CDR, and consumer data reforms in other jurisdictions.

The work has been initiated to bring more consumer-centric and practice-informed knowledge of consumer experiences, needs, and expectations for data sharing into the evidence base informing ongoing development of data standards for Australia's Consumer Data Right (CDR).

As well, the project aims to grow capability and seed opportunity for the community sector to be supported in contributing to CDR development in ways that will facilitate all Australian consumers having access to positive outcomes from the regime.

Executive Summary

Fair systems start from an understanding that not everyone comes to them with the same needs, capabilities, or advantages.

The Consumer Data Right (CDR) has been heavily shaped by engagement with data holders and potential data recipients regarding the technical and commercial use cases and problem spaces it invokes. Continuing opportunities for community and social services to share expertise in relation to whether consumer outcomes are similarly informing CDR development have been fewer in number. Our report acknowledges this gap and contributes a summary of qualitative findings and consumer experience inputs from discussions CPRC conducted with community sector organisations and consumer advocates during August and September 2020 on the topic of the Consumer Data Right and joint accounts.

Creating safe and useful CDR data sharing for joint accounts holders requires an understanding of who those consumers are, the contexts in which they are likely to encounter CDR, and what their capabilities might be when interacting with the scheme. Our report delves into consumer experiences and scenarios relating to joint accounts data that have not always been given prominence in industry-led CDR use cases to date. In sharing their stories and insights about how consumer data impacts on peoples lives, wellbeing, and access to essential services, participants have raised ambitions for a more inclusive and equitable data economy and a CDR capable of supporting the positive outcomes that all Australian consumers deserve.

Establishing trust in joint accounts data sharing through CDR processes can be addressed to some extent through the Data Standards, however positive consumer outcomes will also be contingent on the market conditions that the CDR regime and its rules encourage to flourish.

If consumers find themselves exploited, bamboozled, or locked out of accessing benefits; and if market stewards fail to maintain and uphold relevant consumer protections the credibility of the CDR will suffer. Driving market competition that does not improve consumer outcomes would be a poor return on investment for CDR. Alternatively, if CDR enables people to make meaningful choices about data sharing that will allow them to access better consumer outcomes without fear of their data being mishandled, misused, or brokered without prior knowledge or a means to redress; it could grow into a truly innovative reform.

The call from the community sector is for a CDR that is accessible and beneficial for consumers with diverse backgrounds and circumstances, and across changing life stages and events.

To fulfil its promise, CDR must acknowledge the depth of information asymmetries in data markets and consumer transactions, as well as the presence of power imbalances between joint account holders. Where multiple consumers have shared interests in consumer datasets, rights and repercussions for all account holders need to be reflected in CDR processes, and in the monitoring and measurement of outcomes.

For consumers transacting in data markets, quality of choice is often a more pressing need than quantity of choice; and downstream effects of data sharing are always of consequence. Transparency in how CDR data is transacted is a vital part of mitigating unauthorised consumer profiling and predatory marketing, risk of consent being manipulated, and the likelihood of CDR activity on joint accounts being weaponised in situations of coercive control.

In researching this report, we listened to stories about broken trust and existing failings in how consumer data is transacted. And we heard a desire for building trust through meaningful consent, genuine inclusion and robust accountability. Fundamental pillars for the entire CDR regime, these three themes impact directly on how CDR data sharing from joint accounts will be experienced by consumers.

Consent

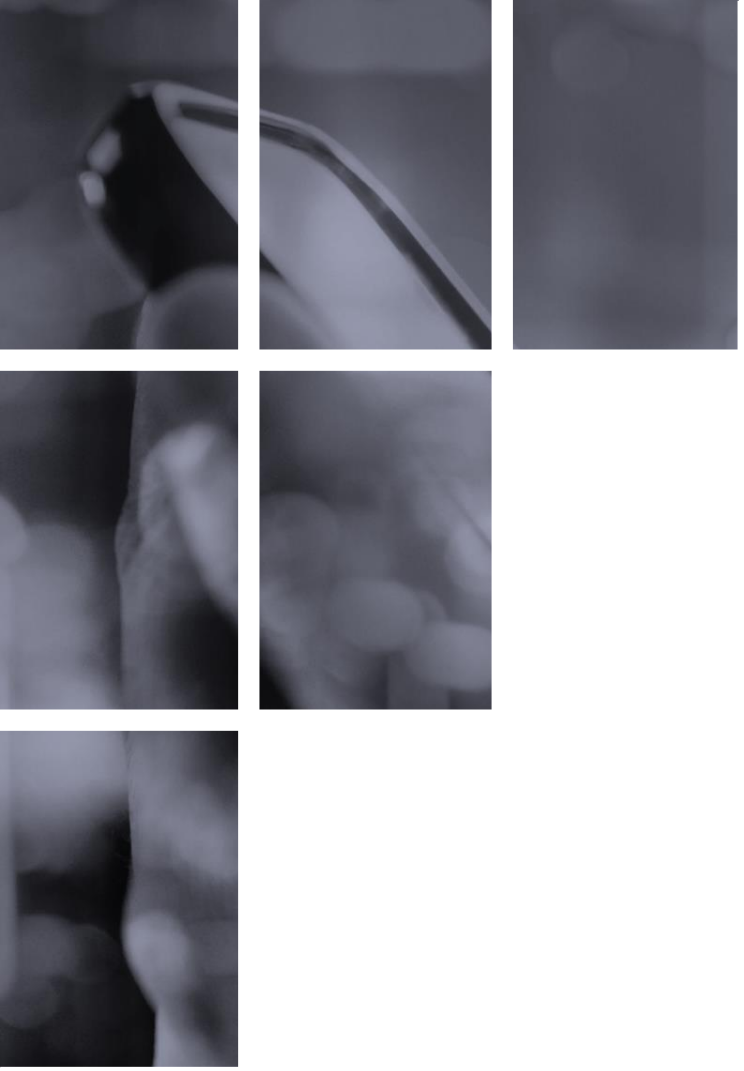
Issue: Joint account holders' consent may not be freely given or fully informed, but still functions as a technically valid CDR consent

Inclusion

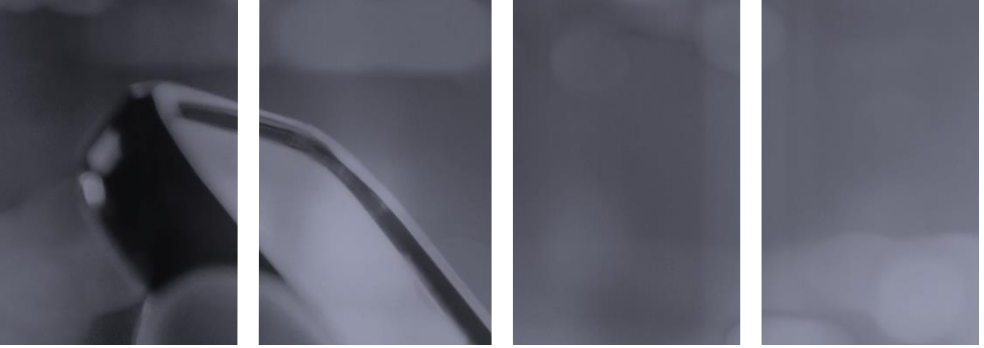
Issue: Joint account models for CDR may prioritise industry conventions over consumer realities of shared accounts

Accountability

Issue: Information necessary for safe and responsible conduct may be obscured from CDR consumers, participants, or regulators



Contents



A note on terminology:

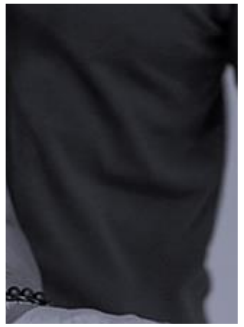
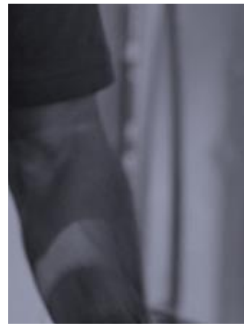
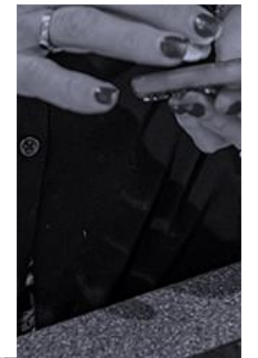
There are differences in how joint account holders are being defined in relation to CDR Rules for banking and energy (and, presumably, other sectors).

For the purposes of this report, "joint account" refers to an account with a data holder for which there are 2 or more joint account holders, each of whom holds full permissions and financial responsibility for the account and is an individual who, so far as the data holder is aware, is acting in their own capacity and not on behalf of another. However, with regard to conceptualising consumer issues with CDR data sharing from joint accounts more broadly, we also look beyond this definition of joint accounts to consider other scenarios where multiple consumer stakeholders are invested in CDR data, including where they may not be deemed to be CDR consumers for that data, and consider what this means for their consumer rights under CDR.

Glossary of abbreviations

ADR	Accredited Data Recipient
CDR	Consumer Data Right
CSO	Community Sector Organisation
CX	Consumer Experience
DH	Data Holder
DV	Domestic Violence (in this document, an interchangeable term with 'Family Violence')
DSB	Data Standards Body
JAH	Joint Account Holder (also, 'JAH1' and 'JAH2': where JAH1 is the joint account holder who is initiating a CDR consent and JAH2 is the other party to the joint account). For comparisons against the ACCC's October 2020 CDR Rules Expansion consultation paper, JAH1 and JAH2 correspond to Account Holders A and B, respectively.
JAMS	Joint Account Management Service



1. What did we do?

“It is a question of what you’re expecting the CDR to do and be able to mitigate versus the wider work that all those market sectors have to do…”

- INTERVIEW 6

We spoke with 20 individuals across 13 organisations, with expertise in areas including:

Note: see also Appendix 3 – interview matrix.

We extended the CDR consultation from technical infrastructure to societal impacts

Technology is not a neutral instrument, but the application of a particular culturally-specific set of knowledge to solve a (perceived) problem.

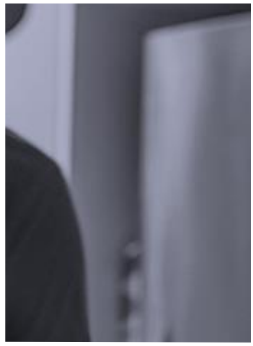
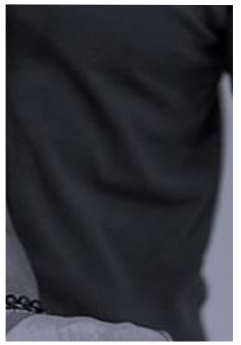
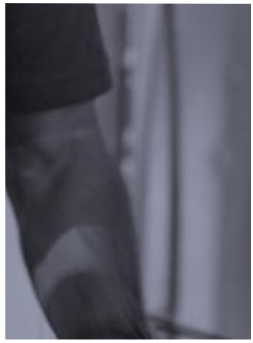
Technology is a cultural practice.[1]

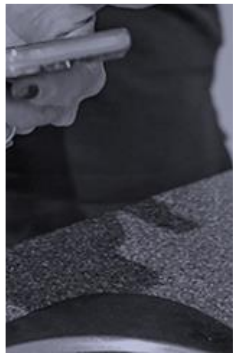
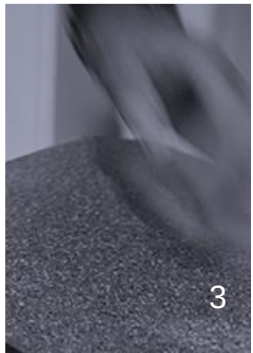
CPRC is translating technical consultations into relatable societal impacts, opportunities and risks to allow community sector expertise and consumer interests to be heard.

A technology-oriented approach, without similar focus on understanding and developing the social context and soft infrastructure within which CDR will operate, and which is equally important to its success, limits the potential for consumer needs to be adequately represented in the development of Australia's Consumer Data Right.

CDR's development and implementation roadmap has been heavily focused on the technical infrastructure necessary to implement a data pipeline and facilitate secure exchange of machine-readable data between Data Holders (DH) and Accredited Data Recipients (ADR). We suggest that shifting from a technical focus and centring consumer interests and outcomes will better support the task of building a CDR regime able to support an inclusive data economy with the positive consumer outcomes Australia can choose to aspire to.

Alongside the ongoing engagement with data holders and potential data recipients on matters relating to technical expertise and the practical capabilities of CDR participants, there have been fewer opportunities for the community sector to bring expertise regarding consumer capabilities, circumstances and outcomes to the CDR development table. Without comparable opportunities to test and challenge the assumptions being baked into CDR's design, a wealth of knowledge on the potential human and social impacts of CDR – both positive and negative – is sidelined. This consultation widens the channel for consumer perspectives to flow into CDR design.


We discussed:

"The consent prototypes were really great to show how the joint account situation would work: it really brought it alive.

But I was thinking, well – how would [consumers that I advocate for] – how would they do that? How would people navigate it? Many just couldn't."

- INTERVIEW 5

- Where data sharing under CDR might create new risks and opportunities for joint account holders in banking, energy and other sectors.
- How CDR might alter the prevalence or impact of existing consumer harms associated with joint accounts, and ways in which CDR could amplify or mitigate these dangers.
- What kinds of existing methods, tools, or best practices for facilitating consumer safety and equity in joint accounts products are transferable to CDR environments.
- Whether CDR processes, including standards, guidelines, and joint accounts protocols sufficiently support consumers to exercise meaningful consent and control over how their joint account data is shared, and to do this safely.
- The extent to which current prototypes for joint account consent flows (Appendix 1) are likely to be accessible to, and appropriate for obtaining meaningful consent from consumers.

We listened to what people wanted to tell us

There is a real generosity of knowledge and an appetite to understand and contribute to CDR in ways that recognise diversity in consumer needs and capabilities. All interviewees we spoke to want to see good consumer outcomes from CDR, but most believe such benefits will flow to already-advantaged consumers, with negative consequences largely borne by individuals experiencing vulnerability. This is seen to be especially (although not exclusively) true for consumers who have less access to digital services, who operate in a cash economy, or who may be dealing with a range of other barriers to data proficiency or market inclusion. In this context, CDR is perceived as representing the interests of a worldview that imagines consumer benchmarks of access, value, and capability that do not correspond to the lived realities of the people our interviewees support through experiences of financial and consumer harm.

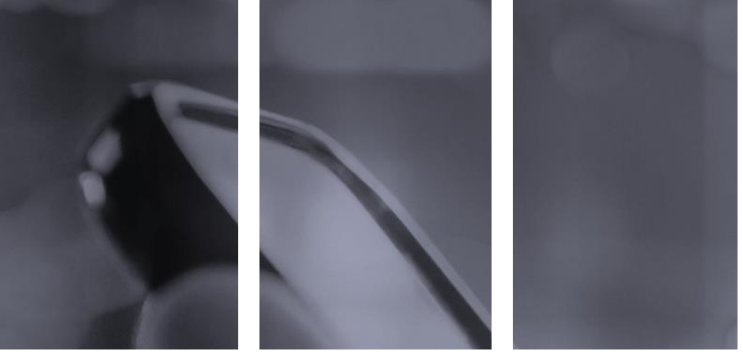
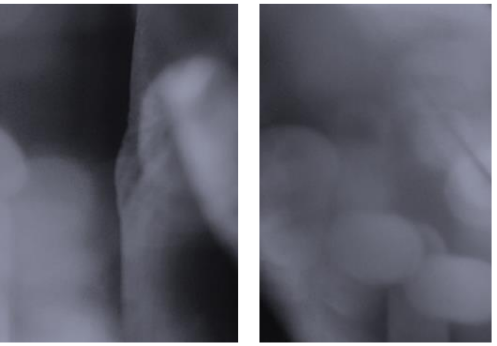
The primary concern is that people who are already facing hardship, vulnerability, or abuse will find themselves materially worse off as a result of CDR. This may be due to the regime affecting how markets perceive risk and price services (just as some consumers might be offered a better deal, others are likely to be offered a worse option based on what their data tells a service provider); as an outcome of manipulation or coercion of online consent; or simply because they are shut out from accessing CDR.

Most community organisations we spoke with can anticipate unintended consequences of CDR manifesting in adverse outcomes for clients of their services. They see their capacity to assist consumers in navigating the regime as constrained by an ongoing lack of clarity regarding how CDR will operate in practice and across different sectors, with data sharing propositions and consumer interfaces remaining to be iterated by market players who do not hold consumer interests as their primary concern.

"[CDR] might work for people who have good digital literacy, good skills, good access to devices and are of a certain socio-economic status; but its not actually going to be useful for people who don't have any of that.

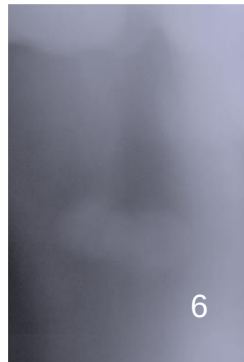
And ... those individuals will be further shut out of being able to navigate the market – it'll exacerbate and cement existing exclusion and disadvantage."

- INTERVIEW 5





2. What did we find?

“The thing that stands out the most is the consent question: what is consent?

And accessibility for vulnerable customers – for people without internet, for people who are not literate, people who speak English as a second language, all of those things – at the best of times they find it difficult to communicate and understand their rights - so when it’s something as complex as CDR I think that accessibility principle needs to be front and centre.”

- INTERVIEW 11

Contextual findings:

Not all issues raised by interviewees were specific to joint accounts.

Findings on this page contextualise what we learned about wider perceptions of CDR.

We intend to address these findings in more detail in subsequent reports.

- Proactive engagement with CDR stakeholders outside the DH/ADR community has been limited – most in the consumer/community sector do not feel well informed about how the regime will work in practice
- As a result, although interviewees had deep and wide ranging professional knowledge of people's experiences in relation to consumer data, few were comfortable claiming expertise in how, or how well, CDR will address these issues
- Benefits of CDR for already-advantaged consumers are understood
- Utility of CDR for consumers 'on the margins' or experiencing vulnerability is unclear: relevant use cases are not being well articulated; barriers to access are not being openly discussed; and risks for vulnerable consumers are not seen to be balanced by commensurate opportunity or protection
- CDR is expected to encourage competition in loosely regulated markets where poor consumer experiences are already known to be prevalent
- Credibility of the regime could be strengthened by clearer definition of how consumer outcomes/effects of CDR are intended to be measured
- ***Strong community concerns CDR will widen disparity in consumer outcomes***

Key messages:

Coercive control is a regular feature of abusive relationships. CDR safeguards that are dependent on data holders identifying risk of harm can offer only limited protection, as not all abuse will be known by (or be able to be disclosed to) data holders.

At the point of providing a CDR consent it needs to be clear to a joint account holder that, by default, the other party will be notified of their CDR activity. (*)
This is an important backstop protection for joint accounts where abuse has not been identified, and also (for sectors using JAMS, such as banking) where JAMS approval has been falsely provided by a single account holder who has access to both online accounts.

Consumer protections for joint account holders whose data is shared under CDR should not be contingent on consumers having high proficiency to engage with CDR markets and user interfaces.

"The biggest risk is that a victim-survivor [of an abusive relationship] is sharing their data because they're trying to re-establish themselves and is not really aware that the perpetrator will know [that they are taking these actions]."

- INTERVIEW 2

"Reducing friction comes with risks, both in economic abuse and also generally."

- INTERVIEW 10; PARTICIPANT 1

"With more data comes more responsibility."

- INTERVIEW 10; PARTICIPANT 2

"Consequences in a functioning relationship may be annoyance and inconvenience; consequences in a dysfunctional relationship can be incredibly detrimental.

We should be designing processes that can't inflict harm onto people."

- INTERVIEW 4; PARTICIPANT 1

"[CDR] is making changes determined essentially by the technology that's available.

We want to make sure that we're not being normative in our judgements of what people are capable of and what they want to do … and saying if they're not capable of dealing with that themselves then that's their problem."

- INTERVIEW 4; PARTICIPANT 2

(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.

Underlying issues

Consent

Joint account holders' consent may not be freely given or fully informed, but still functions as a technically valid CDR consent

What this means & why it matters:

In these circumstances, a 'valid' CDR consent might not reflect the true intent of the consumer and may contribute to fraud, economic abuse, or other consumer harms being perpetrated on one party to a joint account.

CDR is premised on enabling and evidencing consumer consent for data sharing. If it is seen to regularly operate in ways where that consent is not meaningful, the foundations of the regime are fundamentally undermined.

Inclusion

Joint account models for CDR may prioritise industry conventions over consumer realities of shared accounts

What this means & why it matters:

Data models in use by data holders may not recognise all individuals generating data on an account as joint account holders, meaning stakeholders on accounts may not be considered CDR consumers. In other cases, joint account models assume account holders to have equal opportunity to act on the account, whereas coercive or controlling behaviour may preclude this being a reality.

As a result, some consumers will be shut out from accessing their data through CDR. In other cases, there are repercussions for the validity of consent and the safety of consumers if abuse or coercion exists between joint account holders such that a consumer cannot act freely on their account but is assumed to be able to do so.

Accountability

Information necessary for safe and responsible conduct may be obscured from CDR consumers, participants, or regulators

What this means & why it matters:

Comprehension and effective regulation of CDR requires visibility of and for human actors in the system. Lacking this, protections are compromised. (See examples page 16).

If protocol for technical transfer of data between machines are established without sufficient attention being paid to co-existing requirements for how human relevant information is expressed and exchanged as part of the system, CDR will not have appropriate data structures in place to support necessary accountability to consumers.

Consent may not be free and informed

Why might this be the case?

Implicit or explicit coercion of one joint account holder by the other due to family violence, elder abuse, or other abuse of a power differential or dysfunctional relationship dynamic between joint account holders.

Cultural or learned bias whereby actions are agreed without question; or where one joint account holder defers to the other by default. Contributing factors could include acquiescence bias; gender stereotypes regarding financial authority or capabilities; or a habitual disengagement with financial decisions.

Comprehension is compromised so that a joint account holder does not fully understand what they are consenting to share, or the consequences of that sharing for themselves or the joint account holder. For example:

- the full parameters of data being shared from joint accounts is not made explicit to one or both JAH; for example, in relation to how CDR currently treats historical banking (discussed at page 23)
- the implications of joint account data sharing consent is not clearly explained; for example, in relation to the visibility of data sharing activity, and the loss of a right to deletion (discussed on page 23)
- a joint account holder experiencing cognitive difference, mental illness, or a learning disability is without independent support for financial (or other) decision making
- a joint account holder with a non-ongoing impairment to comprehension and decision making, such as sleep deprivation; or being under the influence of alcohol or other drugs is being prompted to give CDR consents (noting that the always-available nature of online CDR data sharing propositions may increase likelihood of consents being requested at such times).

COMMUNITY VIEWPOINTS

"Under coercion, asking someone to log into their online banking and tick a button [for JAMS election] would be easy to do in that situation – and one of the difficulties we have in economic abuse more generally is that where these things happen online there's no visibility."

- INTERVIEW 11

"The consent issue is massive. The majority of our clients - and this is so real - they will just say yes without having any understanding of what they have just agreed to."

- INTERVIEW 9

Consent may not be freely given or fully informed

(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.

Scenario	What happens in CDR?	What else happens?	What's missing?
Domestic violence **A joint account holder who is in a violent and controlling relationship is trying to escape the situation.** JAH1 is hoping to leave an abusive relationship and wants to use CDR to take steps towards financial independence, including sharing data from a joint banking accounts that already have JAMS election in place. JAH1 consents to an ADR requesting joint account data from the DH without realising this means JAH2 will see this activity on their DH consumer dashboard. *Note: a similar scenario exploring what might happen in a situation where JAMS election is not already in place is included in Appendix 2 (see: page 37).*	DH does not have to make the joint account consent visible on JAH2 dashboard if they consider this would result in physical or financial harm or abuse [*Rules; Schedule 3,* 4.6(b)]. Similarly, DH is not obliged to disclose eligible CDR data where they consider doing so would result in physical or financial harm or abuse. [*Rules* 4.7(1)a]. CDR Rules require a DH must inform the accredited person of such a refusal in accordance with the data standards [*Rules* 4.7(3)]. Relevant Standards have not yet been set, although proposed system responses in relation to a DV flag may involve returning a generic error message to the ADR in response. Interviewees supported this proposal in principle, noting that if a perpetrator perceives the other party as in any way responsible for the refusal this could invoke repercussions for the victim. Notably, the safeguards can only come into effect if the Data Holder knows about the DV situation, has flagged the account accordingly, and has put relevant technical protocol in place in relation to CDR requests.	JAH1 shares data and JAH2 is alerted to this activity, resulting in repercussions/harm **OR** JAH1 shares data and JAH2 is not alerted to the activity **OR** JAH1 is prevented from sharing data from the joint account - either because they do not want JAH2 to know about it; or because a DV flag has been applied to the account that refuses all CDR requests. Participants working in domestic and family violence emphasised the real and significant risk of harm if it is not completely clear to victim-survivors where their CDR actions may be visible to perpetrators of abuse. While the existing CDR provisions noted here are a necessary and important safeguard, many consumers who are at risk of harm will not be willing or able to self-identify, and may 'slip through the gaps'. It is important to consider where other protections can be added into the regime to support the safety of joint account holders in this situation.	a) In flow alert so that JAH1 knows JAH2 will see the activity by default (*) b) Notification that CDR safeguards can be activated to prevent this, and the ability for JAH1 to initiate that if they choose to c) Mechanisms for JAH1 to self-disclose abuse, safely, from both the DH and ADR side of a consent (noting that victim-survivors may not want to disclose this information) d) Referrals to support services integrated with CDR processes e) Information on data holders' website/JAMS/consumer dashboard to disclose their policies in this space f) Guidelines for how non-disclosure may apply and the granular effects of flagging an account for DV (ie, will it prevent data sharing by both parties; or for only certain types of data; how will dashboard non-disclosure to one JAH be managed in practice) g) Data Standards relating to notifications of refusal of CDR requests.

Consent may not be freely given or fully informed

Scenario	What happens in CDR?	What else happens?	What's missing?
DV; elder abuse; other **A joint account holder who has been experiencing economic abuse is attempting financial recovery** An abusive joint account holder (JAH1) controls the online banking access and/or passwords through physical or psychological intimidation and coercion. Significant debts have been incurred by JAH1 on the joint facility. A financial counsellor is seeking to negotiate a reduction of the debt or waiver of liability on behalf of JAH2, on the grounds that JAH2 was not aware of, or was coerced into incurring the debt.	Write access paradigm does not yet exist, so joint account holders cannot use CDR to directly initiate an application (and incur associated debt), however they may be able to use CDR to more easily obtain offers (or, to obtain more offers) via ADR service propositions. With these offers, they might then coercively or fraudulently provide the consent of JAH1 as they would in a non-CDR context. A number of interviewees noted that if CDR extends to write access in future this may facilitate economic abuse in coercive relationships, even if such actions are two to authorise. As with the previous scenario, mitigation relies on the data holder being aware of abuse and having protocols in place to flag accounts and refuse CDR requests from ADR.	JAH2 maintains that they were unable to freely consent to data sharing, or to the resulting products and associated debts. Owner of the debt argues that the CDR consent is sufficient proof of JAH2's knowledge of and agreement with JAH1's actions.	a) Precedent…. Interviewees who provide legal or financial services hoped that arguments against victim liability currently used in non-CDR contexts would succeed in relation to coerced or fraudulent consent within CDR. However, this is untested; there is no precedent yet to support joint account holders who may suffer economic abuse effected using CDR. b) A simple way for consumers to enact rights under CDR Rules 9.5 (Requests from CDR consumers for copies of records) – ie, to easily request or generate a summary of all CDR consents (including expired consents, amended consents, and disclosure records) relating to a joint account – perhaps through the ability to download or export records of consent from a consumer dashboard. c) Support services being able to obtain a picture of their clients' financial situation, including visibility over CDR data requests to ascertain whether responsible lending practices were followed. The latter is distinct from proposed amendments to the CDR Rules to allow disclosure of data to trusted advisors[2], which were considered to add unwarranted risk for information that could be obtained through existing channels.

Joint account models for CDR may prioritise industry conventions over consumer realities of shared accounts

Why might this be the case?

Individuals generating data on an account are not recognised as account holders and/or are not considered to be CDR consumers.(*) This might occur where:

- multiple consumers are sharing a resource or service, such as the energy supply to a premises, but the account status of individuals is limited by parameters of the provider's data model (which may not allow for full status joint account holders)
- multiple services relating to different individuals are bundled on a single account, such as having several mobile phone plans on a single household account
- energy supply for a premises is part of an embedded network
- an individual credit card account has additional card holder/s
- a minor is living independently
- a financial counsellor, power of attorney, or other authorised representative is acting on behalf of a consumer.

Joint account holders are assumed to have equal rights to transact on the account, but coercive or controlling behaviour means this is not the case:

- a joint account has been obtained or is being managed through deceitful or coercive conduct
- one party is not aware of the account's existence
- one joint account holder is controlling access, or does not allow the other party access to the account.

(*) 'CDR consumer' has a broad meaning under the Act and is likely to include persons beyond those who are considered account holders. The energy rules framework limits the definition of eligible consumer to account holders and possibly to persons nominated on the account, all of whom must be 'known' to the retailer. In October 2020, the ACCC consulted on proposed rules that would allow sharing (if authorised by the account holder) by secondary card holders and persons with the ability to 'transact on an account' (see rule 1.15(5) and clauses 2.1 and 2.1A of schedule 3).

COMMUNITY VIEWPOINTS

"With telcos, there might be a single account holder but multiple individual and shared services on the one account, and that's very common."

- INTERVIEW 5

"Residential parks, aged care homes, some fully managed apartment developments that operate under grouped utilities fee ... There's an opportunity for CDR [in energy] to clean up some of those relationships, or at least recognise that they exist"

- INTERVIEW 4

Joint account models may not reflect consumer realities

Scenario	What happens in CDR?	What else happens?	What's missing?
Housemates are sharing energy usage. All pay an equal share of the utility bills, but only one tenant is identified as an account holder, as the energy retailer does not allow joint account holders. One of the housemates (an international student who is not on the lease and is not the energy account holder) is now experiencing financial hardship. They do not want to disclose to their housemates that they are undergoing financial stress over the energy bills because they worry this may affect how they are treated by others in the house, or even cause them to be evicted. Wanting to frame the discussion as a money saving opportunity for the entire household, they would like to share CDR data beforehand to a) understand any major appliance inefficiencies and b) explore different product offerings with a view to suggesting the household can switch retailers to reduce bills.	Rules for CDR in Energy not yet defined. Joint account holders with full permissions and authority to act on the account are in scope as eligible CDR consumers. JAMS election will not be required – data sharing proposed as one to authorise. As proposed in the July 2020 CDR *Energy Rules Framework Consultation Paper* some classes of 'nominated persons' (those who have been added to the account as a known person by the primary account holder, and who have been authorised, to some extent, to transact on behalf of the primary account holder) may be designated as being eligible to request data. In addition to persons consuming energy at the premises; nominated persons might include financial counsellors, family members other than those who occupy the premises, or employees (for business accounts).*[3]*	In this scenario, the energy user would not be considered an eligible CDR consumer and would be prevented from using CDR to share their household energy data in the way they want to do so. (*) (*) 'CDR consumer' has a broad meaning under the Act and is likely to include persons beyond those who are considered account holders. The energy rules framework limits the definition of eligible consumer to account holders and possibly to persons nominated on the account, all of whom must be 'known' to the retailer. In October 2020, the ACCC consulted on proposed rules that would allow sharing (if authorised by the account holder) by secondary card holders and persons with the ability to 'transact on an account' (see rule 1.15(5) and clauses 2.1 and 2.1A of schedule 3).	Where consumers of a product or service are generating data on the account but are not recognised as joint account holders, they will be prevented from sharing their consumer data to create the personalised offers and consumer benefits that CDR promises. Conversely, where JAH are assumed to have equal rights to transact on the account, but coercive or controlling behaviour means this is not the case, there is a significant power imbalance in the relationship that is not accurately reflected in the account structure. Communication of CDR use cases should be undertaken with an understanding of who will be excluded from using them and why. "Something encouraging energy retailers to have joint account holders would be great, because some households even now want to have more than one account holder and get told they can't, and I think that needs to change" -INTERVIEW 8

Joint account models may not reflect consumer realities

Scenario	What happens in CDR?	What else happens?	What's missing?
Data breach or misuse by an ADR, where a joint account holder has given a valid consent to share consumer data relating to multiple parties. An extended family of five living together in the same residence have a shared internet service and individual post-paid mobile phone services for each person bundled together on a single account. Two parents are named as joint account holders. Their two adult children (aged 18 and 19) as well as the elder daughter's partner (also aged 19) each pay a proportional share of the bill, but are not account holders.	Rules for CDR in Telecommunications not yet defined. Many of the CDR Privacy safeguards explicitly specify protection as being for the CDR consumer (see, for example, CDR Rules in relation to the direct marketing prohibition / Safeguard 7; and the notification of disclosure of CDR data / Safeguard 10). As joint account holders, both parents are CDR consumers. Their children, being associates according to the definition provided by section 318 of the *Income Tax Assessment Act 1936*, can also be considered CDR consumers. However, the elder daughter's partner is not a CDR consumer under the definition of CDR consumer given in the Act [Section 56AI(3)], and as such is not subject to the same level of protection as the other four individuals.	Only the parents, as joint account holders have a customer relationship with the DH. Only JAH1 has a customer relationship with the ADR. This may compromise the position of JAH2: CDR complaints must first be made to the relevant CDR provider before they can be lodged with the OAIC; but JAH2 will not have a customer account with the ADR in relation to which they can describe and lodge a complaint. Or, in the case that an ADR becomes aware of a data breach, JAH2 may not be advised at all – it is not clear what responsibility an ADR has to notify joint account holders or CDR consumers other than JAH1 in the event of such events. (Notably, the ADR won't have capacity to do so directly – are they required to notify DH; and does the DH then have an obligation to inform consumers, via the DH dashboard or other mechanisms). And, the three young people have even less standing to obtain information or make a complaint.	Clear information about the obligations of ADRs and DHs to coordinate and communicate data breaches to joint account customers, and other data subjects of CDR data. Clear information about recourse to complaint or redress for a person who may be a data subject and stakeholder in CDR data that has been disclosed under CDR and subsequently misused or mishandled, but who is not themselves considered to be a CDR consumer under the definition given in the Act. (*) Mechanisms to enact equivalent CDR protections for such persons.

(*) 'CDR consumer' has a broad meaning under the Act and is likely to include persons beyond those who are considered account holders. The energy rules framework limits the definition of eligible consumer to account holders and possibly to persons nominated on the account, all of whom must be 'known' to the retailer. In October 2020, the ACCC consulted on proposed rules that would allow sharing (if authorised by the account holder) by secondary card holders and persons with the ability to 'transact on an account' (see rule 1.15(5) and clauses 2.1 and 2.1A of schedule 3).

Lines of sight are masked – information needed for safe and responsible conduct may be hidden from CDR consumers, participants, or regulators

Why might this be the case?

Online environments, and individualised mobile devices, encourage consumers to feel they are acting in a 'walled garden' – belief in privacy, even if misplaced, can embolden people to behave in risky or harmful ways.

Divergence between how and what CDR value propositions are being made available to each joint account holder; and variation in the quality of information about consents (including disclosure or amendments) visible to account holders: JAH2 only has access to the more limited information conveyed on DH consumer dashboard.

Data holders and ADRs have less opportunity to observe relationship dynamics between joint account holders - signs of abuse between joint account holders may go unrecognised.

No obligation for ADR or DH to notify consumers or regulators of how decisions are informed by CDR data

- Consumers may be offered worse pricing/rates after sharing CDR data - data profiling allowable under CDR as part of a use case consented to by one joint account holder may have negative impacts for both. Without insight into how CDR data is used, consumers and advocates may struggle to interpret or contest grounds for decisions.
- Data holders made aware through CDR that joint account holders are looking at other providers or switching options may use that knowledge in an anti-competitive manner, or without the account holders realising CDR activity is affecting their existing offers.

Focus on short term benefits distracts from visibility of risks, accountability and longer term consequences

- Only one JAH has a direct relationship with ADR: JAH1 and JAH2 are not provided the same visibility over an ADR's full terms and conditions regarding data collection and use.
- A CDR logo indicating "safe" data sharing may distract consumers from distinctions in impact. For example, an offer to find a cheaper mobile phone plan (with an easily reversible decision attached) may be perceived no differently to an offer to find cheaper health insurance (with an unintended and irreversible consequence of losing coverage in relation to a chronic illness that is subsequently considered a pre-existing condition).

COMMUNITY VIEWPOINTS

"When we set up things that take the human out of the loop people see opportunities to do things that they might not attempt if they had to justify their actions to a human. Anytime we make things more anonymous and automatic it leads to some people feeling they can use that to their advantage."

- INTERVIEW 3

"The main thing is just to make [joint account] customers as aware as possible of who can see that their data has been shared and when."

- INTERVIEW 6

Lines of sight are masked

Scenario	What happens in CDR?	What else happens?	What's missing?
DV; elder abuse; other. Joint account holder(s) are seeking information about products and services online, including exploring new credit or loan facilities offered using CDR-enabled services. DH loses opportunity to observe power dynamic between JAHs and misses signs of abuse that may be evident in their interpersonal interactions.	Valid consents are assumed to have been given without coercion. No flag is placed on account. CDR safeguards are not enacted. CDR provisions intended to protect account holders who may face harm through CDR data sharing rely on the existing processes of Data Holders to identify such risk.	Existing banking guidelines for identifying abuse have dependencies on self-disclosure by a victim-survivor, or being able to assess in-person interactions[4]. By increasing the extent to which consumer interaction and the provision of information takes place online, CDR may be detrimental to the ability of Data Holders to recognise, flag, and take action to mitigate abuse.	a) Lens for DH to "see" abuse where one JAH is responding to CDR data requests in ways that are controlling or harmful to the other JAH. b) Data on CDR complaints relating to joint accounts to identify transaction types or use cases that are more frequently implicated in abuse; application of this data to develop algorithms that can detect patterns in CDR requests being made on a joint account, to indicate where human intervention may be needed.
Defacto couple living together in a relationship that is not abusive. JAH1 and JAH2 each maintain independent bank accounts, and share a joint credit card account for household expenses and a mortgage account for their home loan. They have an active JAMS election on their shared accounts. JAH2 is apprehensive about the number of consents JAH1 is making and is concerned about what might happen to the data over time. JAH2 asks JAH1 what choices they have made in relation to expired data being deleted or deidentified.	Many of the ADRs JAH1 is transacting with do not have a policy of deletion by default. In some cases JAH1 has expressed a choice that the ADR delete the CDR data when consent expires, in other cases they have chosen de-identification. Consents made by JAH1 are visible on JAH2's DH dashboard, however CDR Rules do not explicitly require DH dashboards to indicate (to either party) whether CDR data in relation to a consent will be deleted or deidentified [*Rules* 1.13(3)]. Currently no requirement for ADRs to inform DH of a redundant data handling policy, so DH do not have visibility over this and cannot convey it on DH consumer dashboards.	JAH2 asks JAH1 to select data deletion rather than deidentification on existing and future CDR consents. JAH1 says they'll do this but subsequently forgets **OR** JAH1 says JAH2 is overreacting and it's not important **OR** JAH1 can't remember what they nominated and doesn't want to go through each ADR dashboard and consent individually Consent expires (or, is revoked by JAH2). The CDR data disclosed to the ADR is deidentified, against JAH2's preference for deletion.	a) Line of sight enabling consumers to see their choice of deletion or deidentification as part of DH consent dashboard. Without this, JAH2 has no visibility on how their data is going to be treated. b) Rules/Standards to require ADR policy (and consumer elections) in relation to handling redundant data be conveyed between DH and ADR, to facilitate visibility for both JAH. Centralised dashboards that 'pool' consent data held by both ADR/DH. c) Mechanism for JAH2 to exercise agency to apply their preference for deletion of their CDR data where consent for data sharing has been provided by JAH1.

How does CDR change the nature risk in relation to joint accounts?

- Increases ease or opportunity for joint account holders to exert control or abuse.
- Promotes growth in markets that target vulnerable consumers.
- Increases likelihood of consumers inadvertently sharing data or information that they may not want disclosed.

“Is this establishing the system for a Royal Commission in 20 years time?”

- INTERVIEW 1

Where does CDR increase ease or opportunity for joint account holders to exert control or abuse?

CDR may give perpetrators of abuse new insights that facilitate their ability to exploit joint account holders. For example, although CDR does not allow a perpetrator of domestic violence to directly access any additional information about their partner's spending which they could not already obtain through online banking on a joint account product, CDR value propositions (such as budgeting tools designed to identify and highlight patterns in spending) may inadvertently make it easier for them to derive insights about their partner's financial behaviour that could be used to refine how financially controlling behaviour or economic abuse is perpetrated.

CDR adds a new tool into an arsenal of abuse. A joint account holder who is a perpetrator of abuse is given a new way of exerting control over the other party. For example, they can veto data sharing authorisations or revoke JAMs election from the joint account for a sole purpose of demonstrating to the other account holder that they can control that person's capacity to share data.

Where does CDR increase ease or opportunity for businesses to target vulnerable consumers?

CDR is likely to stimulate competition in markets that are operating on regulatory fringes (including fintechs and credit disruptors with service offerings in areas such as payday advances and Buy Now Pay Later platforms). Legal centres and financial counsellors advised us in this consultation that these kinds of products currently give rise to a high proportion of the consumer complaints and hardship matters they deal with in relation to financial services. Accordingly, growth in these markets through CDR is likely to see an increase in poor consumer outcomes if the system is not well regulated.

Personalised services increase pressure on joint account holders to give consent without seeking advice. We heard that pressure on a joint account holder to consent to something they are not comfortable with or do not understand (whether from the other JAH, or by targeted messaging from an ADR) is more easily applied where there are no witnesses; and that online market delivery exacerbates this risk. It is anticipated that the business models of CDR data recipients will utilise behavioural marketing techniques to obtain customers, such as personalised advertising of value propositions based on existing data profiles and online activity. Patterns of late night activity on betting platforms or shopping channels (for example) may lead to vulnerable consumers being targeted for credit products they don't require or can't afford, with CDR making it seamless for them to act on that offer at a point in time when they are potentially not making an informed consent.

Note – this section of the report seeks to identify where CDR may alter particular risks associated with joint accounts. It does not propose that such risks only exist when data is shared using CDR, and we emphasise that many underlying risks also arise (and may be more pronounced) through other data sharing processes, such as screen scraping.

Where does CDR increase likelihood of joint account holders inadvertently sharing consumer data or related information that they may not want disclosed?

Information about use of CDR. Interviewees identified significant risk of joint account holders in abusive relationships sharing CDR data without realising that the other account holder will, by default, be notified of the fact of their data sharing activity and substance of the consent. This was deemed to pose a real and substantial risk of repercussions for victim-survivors, likely to occur where a data holder is not aware of abuse. (*)

Loss of right to deletion of redundant data. Interviewees held that the right to elect that CDR data be deleted by ADRs once it becomes redundant (as opposed to deidentification of the CDR data) was an important aspect in enabling consumers to exert agency over the full lifecycle of consent. Concerns were noted that while CDR nominally offers this protection, the act of providing a JAMS election would effectively result in a joint account holder relinquishing their rights in this regard for any consents made by the other party. Further, in the case of CDR data relating to energy accounts, where no JAMS is proposed, this potentially means that the effective removal of a right to deletion extends to all energy joint account holders by default. This is a significant loss of consumer rights and safeguards for holders of joint accounts.

Historical data. In the case of CDR banking data there is no requirement for an ADR requesting CDR data to inform consumers of the date range of data that they are seeking under a consent; and no right for consumers to limit the extent of data they might be comfortable disclosing as part of a consent. Currently, DHs will by default release historical account data to ADRs to the maximum extent that it is designated CDR data – up to seven years in the case of banking transaction data.

In other words, a CDR consumer seeking to share transaction data from their savings and credit card accounts for the purpose of an ADR providing a budget tool for the coming 12 months (and giving express consent for that data use and duration) would not be explicitly informed by the ADR that this consent to share means they are also consenting for the ADR to collect and use up to 7 years of historical transaction data on the nominated accounts (or, in the case of direct debit authorisations two years of historical data). It was noted by participants that, for this use case, a consumer might reasonably expect that the data they are giving permission to share will relate only to the 12 months for which their consent is valid, and that there should be an onus on data recipients to make clear that they will be collecting, and have consent to make use of, a significantly more extensive dataset. For joint account holders, this effect may be compounded if one consumer (JAH1) unintentionally misinforms another (JAH2) in a corresponding manner, for example when explaining why they are seeking a JAMS election from a shared account.

The responsibility to notify the consumers of "the period of time to which the CDR data that was the subject of the request relates" is a requirement for the DH as part of authorisation, under Rules 4.23(b). Concerns were raised by our interviewees that this is liable to be easily missed at the authorisation stage, based on CX prototypes (Appendix 1). It would be preferable for ADRs to be required to state upfront the historical range of data being released by default, and for the ADR – and, by extension, the consumer – to be able to specify a particular historical range. This would prevent unnecessary collection of CDR data and ensure better conformance to CDRs data minimisation principle. We understand technical standards would be required to implement this.

(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.

Where are there opportunities against the risks?

- Enable more granular consent options
- Require joint account holders to be provided the option to nominate two to authorise for all CDR consent requests
- Use system decision points as triggers to provide relevant information about effects and safeguards to consumers
- Use data about CDR to make a better CDR

“There’s two parts – one is designing the products to be safe – the other is increasing customers awareness of the implications, which is … putting all the onus back on that person to manage the risk. So it is better to design a good product!”

- INTERVIEW 6

Enable more granular consent options

CDR consent models could be evolved to provide consumers with greater control and choice over data sharing by enabling granular consent for specific accounts, data clusters, or data types. This would allow a consumer to elect to share data payloads differently in relation to a single ADR consent. For example, allowing a consumer to elect consent to share (in relation to a single ADR request):

- 7 years of historical savings account transaction data
- 2 years of historical personal credit card account transaction data
- joint credit card account data only from the date of the consent forward through the duration of consent

As well, and in addition to the existing right to revoke authorisations relating to data requests/consents made by a co-JAH [Rules, Schedule 3, 4.2(1)(iii)], CDR should also provide all joint account holders with the agency to compel ADRs to delete redundant CDR data relating to a joint account on which they are an account holder, regardless of whether or not they are the party who provided consent to that ADR. If a person has reservations about sharing data with an entity, there is a strong likelihood that they will also want any of their CDR data that may have been shared with said entity up to that point to be deleted. Providing greater control and protection over the end state of their data where another party wishes to share the data may also increase the propensity of consumers to allow data sharing from joint accounts. If this kind of granularity is, after investigation judged too difficult to implement (in light of there being no direct relationship between JAH2 and the ADR), we advise that deletion should be required for all redundant CDR data that has been disclosed from joint accounts.

Require joint account holders to be provided the option to nominate two to authorise for all CDR consent requests

Interviewees were divided as to whether two-to-authorise was necessary for read access to CDR data, and if so whether certain sectors should be exempt. It was noted that two-to-authorise requirement at request level could potentially result in CDR being used for ‘nuisance’ value by a perpetrator seeking to harass a victim-survivor by bombarding them with requests; or as a means of exercising control by refusing all requests and thereby denying a victim-survivor agency over their data.

However, there was consensus that two-to-authorise consent on each data request would be a requisite consumer protection in any future write-access CDR paradigm that sought to include CDR data from joint accounts.

It was also emphasised that two-to-authorise requirements within CDR will not in themselves offer a complete protection for joint account holders or provide accurate representations of consent in all cases: interviewees repeatedly highlighted the relative ease with which it is believed coercive or abusive joint account holders will be able to manipulate CDR processes to secure a JAMS election or ‘valid’ CDR consent from the other account holder.

Use system decision points as triggers to provide relevant information about effects and safeguards to consumers

In theory, CDR will offer opportunities for victim-survivors of domestic violence or economic abuse to seek financial recovery by providing avenues to share data and access new products or services in preparation for, or after, leaving an abusive relationship. In many cases, however, acting on such opportunities is itself likely to incur risk of repercussions which would outweigh any benefit and, if understood, would likely deter CDR participation on safety grounds.

Interviewees emphasised the importance of clearly notifying consumers at the point of making consent that their data sharing activity from joint accounts will be visible to the other account holder by default. (*)

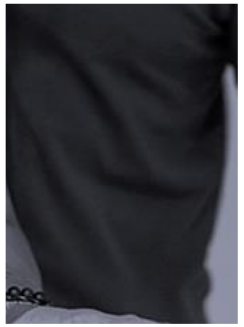
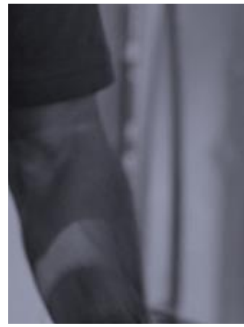
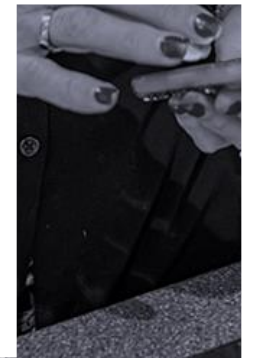
Use data about CDR to make a better CDR

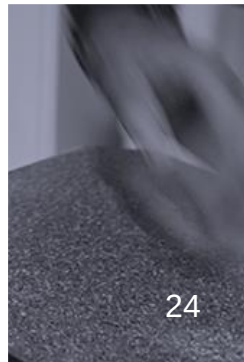
Analysis of CDR requests being made by ADRs may enable banks and other data holders to detect unusual patterns of behaviour on joint accounts that can help identify abuse or fraud. A number of interviewees raised the example of CBA's recent work in developing an algorithm capable of detecting patterns where frequent low value Pay Anyone transactions are being used to send abusive messages in the descriptive text, and were keen to understand how CDR usage data might be harnessed to recognise circumstances where it is used by joint account holders as a tool for perpetrating abuse; or to identify patterns of risky behaviour that could support early intervention with vulnerable consumers at risk of hardship.

Within the CDR framework itself, CDR complaints data could be a rich source of quantitative data about consumer outcomes if available powers are used to set Data Standards to require standardised classification for reporting of complaints data by CDR participants across the regime.

(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.





3. What next?

"…something like CDR, if it works, is going to unlock all these extra possibilities and then those possibilities will become things that people have access to - but if people are locked out from accessing those possibilities then they're going to miss out on growth in the market…"

- INTERVIEW 8

Priority questions

Many questions arise from the scenarios, ideas, and insights that interviewees from the community sector put to us in the preparation of this report. The following should be of particularly high priority for further consideration from consumer and regulatory perspectives:

1. **How can the occurrence (and associated risks) of technically valid CDR consents that do not reflect consumer intent be mitigated, both in relation to joint accounts and across the regime more broadly?**

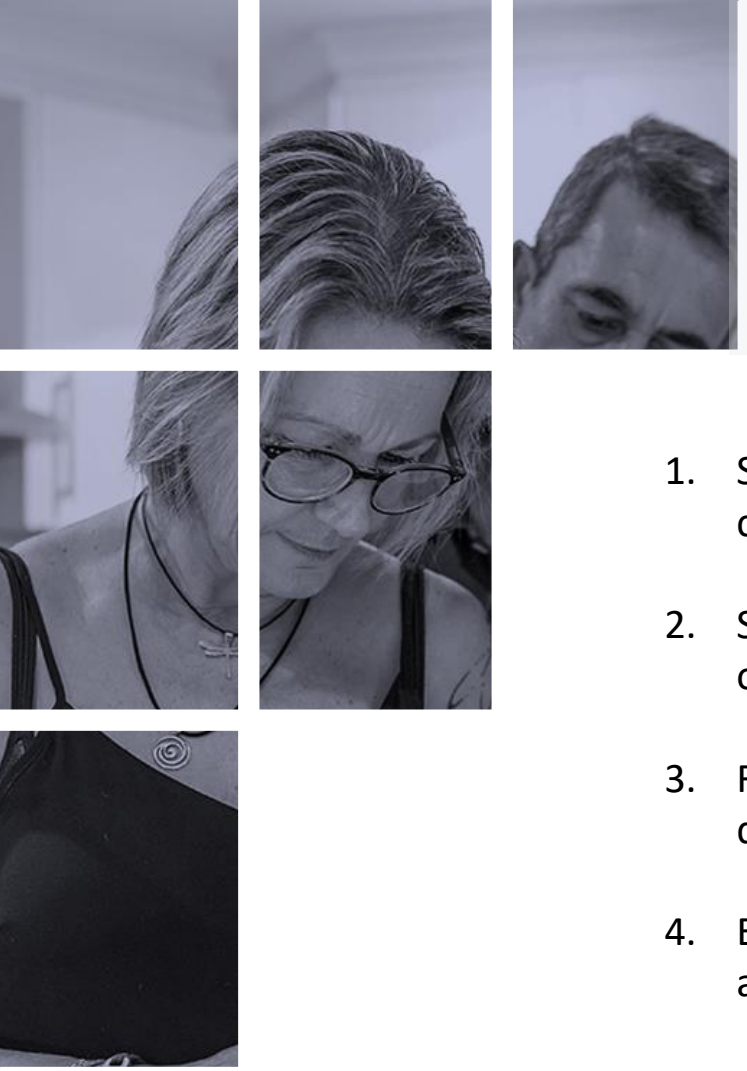
2. **How will CDR deal with anomalies (and associated risks) arising where a data subject responsible for generating CDR data on an account is not considered under the Rules to be a CDR consumer, particularly where CDR is also enabling disclosure of that data to be controlled by another person without allowing the data subject coverage under CDR Privacy Safeguards?**

3. **How can CDR work to provide better visibility and oversight of data sharing for human actors in the regime?**

4. **How will CDR reforms seek to establish a system that is inclusive, accessible, and accountable to vulnerable consumers?**

In voicing these questions, we note that it is beyond the capacity of Data Standards alone to remedy the issues that the community sector is identifying in relation to joint accounts, and CDR more broadly. We refer to our earlier findings (page 11) that these issues of consent, inclusion and accountability affecting joint accounts scenarios also scale to the wider CDR framework. While it is possible – and necessary, in the first instance - to treat matters as they arise specific to joint accounts, the underlying concerns from a consumer perspective are more fundamentally integrated with the entire CDR regime and should be heard in that context.

Our attention was also drawn to some specific opportunities to strengthen elements of the CDR's Data Standards in ways that might contribute to consumer comprehension and bolster both the agency and safety of joint account holders. Six actionable suggestions in relation to the Data Standards are outlined on the following pages.



Action opportunities for the Data Standards Body

1. Set CX Data Standards requiring DHs to explicitly inform consumers, during authorisation of CDR consent requests, that other joint account holders will by default be notified of this CDR activity

2. Set Data Standards in relation to the requirement for data holders to inform the accredited person of a refusal in accordance with the Rules

3. Require sensitive data to be identified as part of the Data Language Standards for designated CDR data

4. Express the Data Language Standards in a way that can be of greater utility for CDR consumers and advocates

5. Set Data Standards to specify complaint types required for reporting by CDR participants (data holders and accredited data recipients)

6. Set Data Standards for how ADRs are to convey the extent of historical CDR data that may be disclosed as part of a CDR request, including CX standards requiring this to be made clear to consumers

Joint accounts & CDR – action opportunities for the Data Standards Body

1. Set CX Data Standards requiring DHs to explicitly inform consumers, during authorisation of CDR consent requests, that other joint account holders will by default be notified of this CDR activity

This is a necessary friction point that can be implemented through the Data Standards to help consumers use CDR safely. It can and should be addressed independently of other important questions regarding how consent for joint accounts operates at Rules-level and how that may vary between sectors (ie, 1 to authorise vs. 2/all to authorise; and whether consent is required at account level to make it available for CDR data requests).

Domestic violence services emphasised the importance of victim-survivors of family violence (and other joint account holders experiencing abuse or exploitation) to be made aware *at the point in time of providing CDR consent* that the other joint account holder will be notified of their data sharing activity.*

We strongly recommend that CDR's CX standards require this as mandatory, to ensure that this default outcome of consent is clear to consumers. We understand that this would need to occur DH side (during selection and authorisation of accounts for sharing data from), as ADRs will not generally have visibility over whether a consumer consent is including data sources that are held as joint accounts.

Although there is a technical reason for this to be a DH responsibility, we heard strong messages that ADRs should also be bearing responsibility for informing consumers of implications of CDR consent (and being clear about the outcomes CDR use cases are intended to achieve for consumers across both short- and longer-term timeframes).

(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.

2. Set Data Standards in relation to the requirement for data holders to inform the accredited person of a refusal in accordance with the Rules

In order for community services to understand and advise victim-survivors on how they are protected under the CDR scheme, it is necessary to be certain what information will be shared back to ADRs in the event that a domestic violence flag on a joint account is the trigger for a CDR refusal. Legal and domestic violence services told us that in the event of a known abusive relationship between JAH where a flag has been placed on the account by the DH (so that CDR data is not disclosed to an ADR under an otherwise valid CDR request), it would be important for the safety of the victim of abuse that information is not inadvertently disclosed that might indicate to a perpetrator that the other account holder is in any way responsible for them not being able to complete the desired transaction.

3. Require sensitive data to be identified as part of the Data Language Standards for designated CDR data

Data Language Standards are a key instrument not only for the mechanics of data request and transfer, but also for assisting consumers to have clarity over the specific data types and/or data clusters that are being requested for sharing. They also provide a mechanism for facilitating consumers to provide express and granular consent in assigning their agreement for CDR data sharing. We suggest this utility could expand to flagging sensitivity of data types, which may otherwise be overlooked by consumers.

This would have additional value for joint accounts where, even within a functional relationship between account holders, individuals may have different tolerances for the types of information they are willing to share with commercial entities (ADRs).

4. Express the Data Language Standards in a way that can be of greater utility for CDR consumers and advocates

There is scope here for Data Language Standards to support the consumer node in CDR transactions, as well as the ADR and DH nodes. We suggest that in addition to defining the Data Language Standards for machine transfer of data, these should also be mapped in plain-language forms: a consumer facing “dictionary of data types” to serve as a guide for consumers and community services seeking to better understand the scope of CDR and the full range of data that may be requested.

We note that this will be of benefit to joint account holders who were not the party making a consent and are seeking to interpret consents appearing on their dashboard that were made by the other party; as well as enabling all consumers to access this interpretative information outside the point-in-time moment of giving consent.

5. Set Data Standards to specify complaint types required for reporting by CDR participants (data holders and accredited data recipients)

Standardising complaint type at a high level will provide a valuable source of data for regulators seeking to evaluate the CDR regime in terms of consumer outcomes; including providing opportunity to measure and monitor the number of CDR complaints involving joint accounts (and how these might be spread across different sectors).

We share concerns heard during this consultation that leaving the required reporting of complaint types open to unstandardised classification (set by each individual ADR/DH)[5] may obfuscate the nature or prevalence of consumer issues arising from the scheme. We propose that Data Standards for complaints need not create unreasonable burden for CDR participants; and that guidance could be provided on mapping data from existing complaints handling processes to required CDR complaint types.

6. Set Data Standards for how ADRs are to convey the extent of historical CDR data that may be disclosed as part of a CDR request, including CX Standards requiring this information to be shown in consumer interfaces for consent

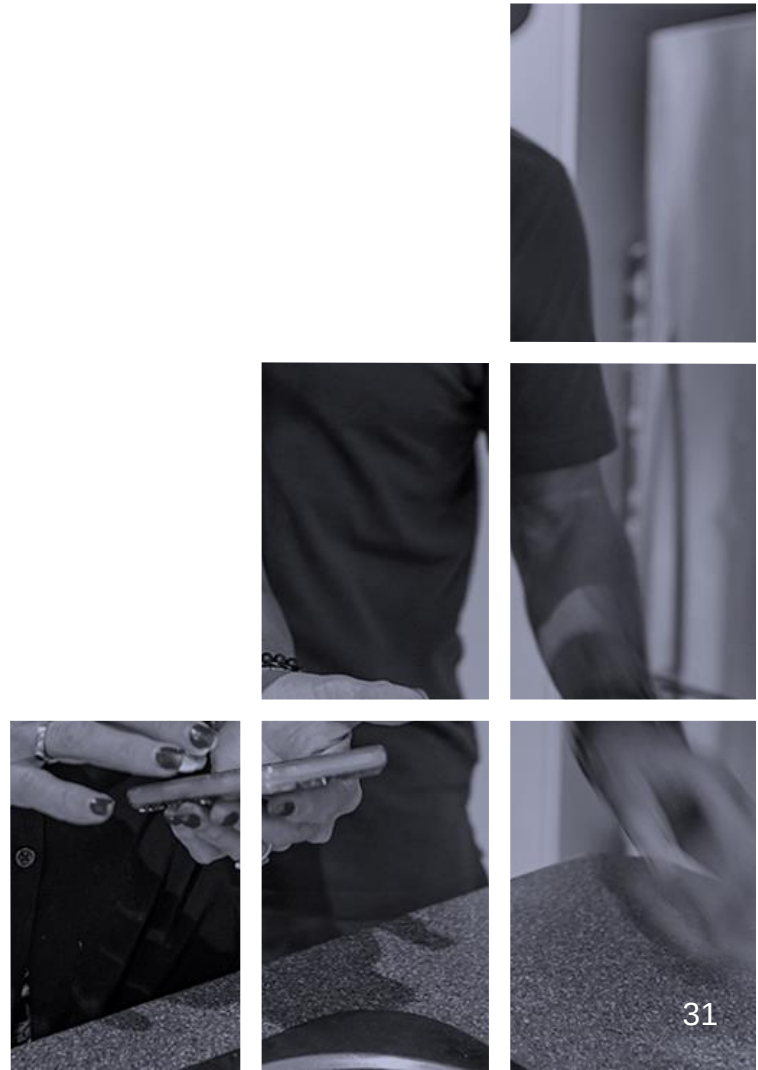
There is currently no requirement for consumers to be informed by ADRs how much historical data is subject to collection and use by that ADR under a CDR consent request (although there is an obligation for DHs to notify this as part of authorising consent). We consider this is counter to both the CDR's Data Minimisation Principle [*Rules,* 1.8(a)(ii)] and the requirement under CDR for consent to be expressly given by consumer [*Rules,* 4.9(b)]. We acknowledge that a transaction date may not be an attribute of all data elements subject to CDR requests, but where it is consumers should be able to exercise agency over how they provide consent for disclosure and use. At the least, it should be made clear to consumers the extent of historical data they agreeing to share.

This was identified as an issue with the consent prototypes shared with interviewees. There was a wide agreement that, in the absence of information to the contrary, the duration of consent has a high likelihood of being misunderstood by consumers as also being the period to which the data being shared relates. We have confirmed with DSB that under a valid CDR request the maximum range of historical data allowable under legislation will be disclosed to an ADR. Should a lesser range be requested, it would be up to the ADR to de-identify/delete the excess. There is currently no technical mechanism for an ADR to request a specific historical range to the DH.

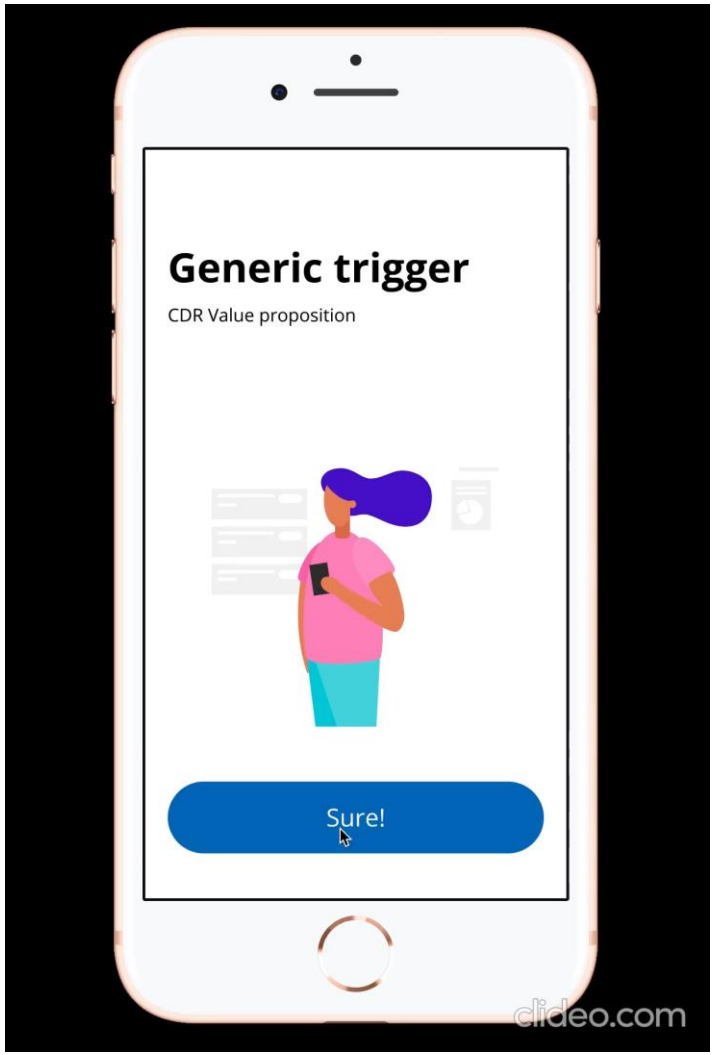
We suggest (1) ADRs be required to state the historical range of data covered by a consent request, and to reduce that range according to the Data Minimisation Principle, and (2) CDR data standards should provide a mechanism that allows ADRs to request a DH to disclose data within a specified date range, resulting in the DH only disclosing data within that required (and minimal) historical range.

Appendix 1:

Consumer experience prototypes representative of consent flow for CDR data sharing, as supplied by the Data Standards Body.

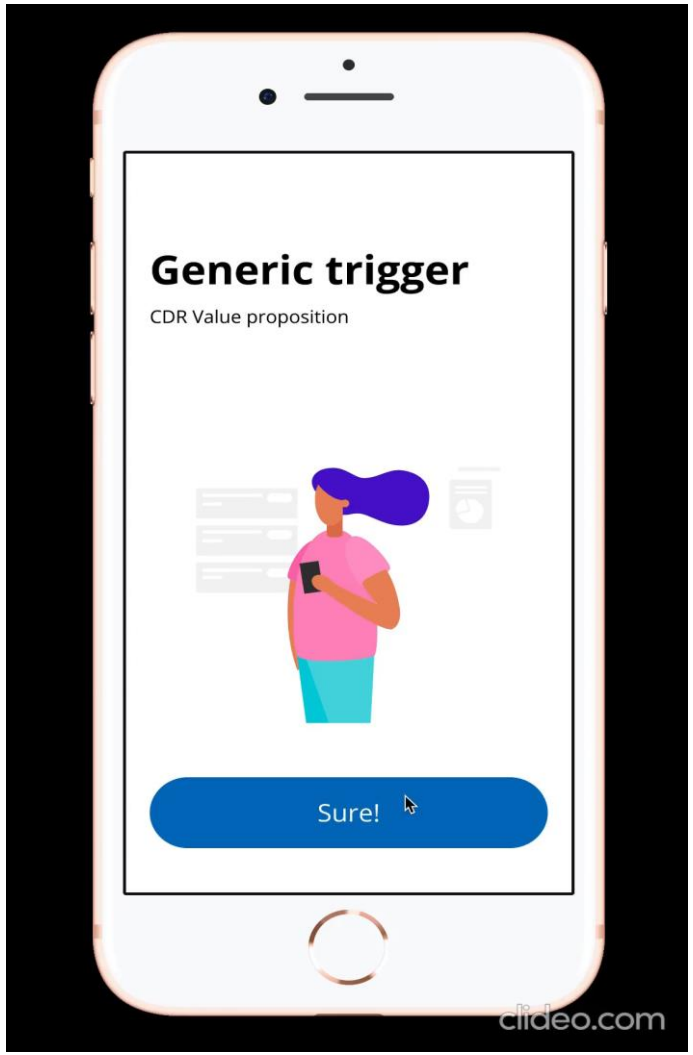


a) JOINT ACCOUNT has been elected for data sharing



Interactive click through version

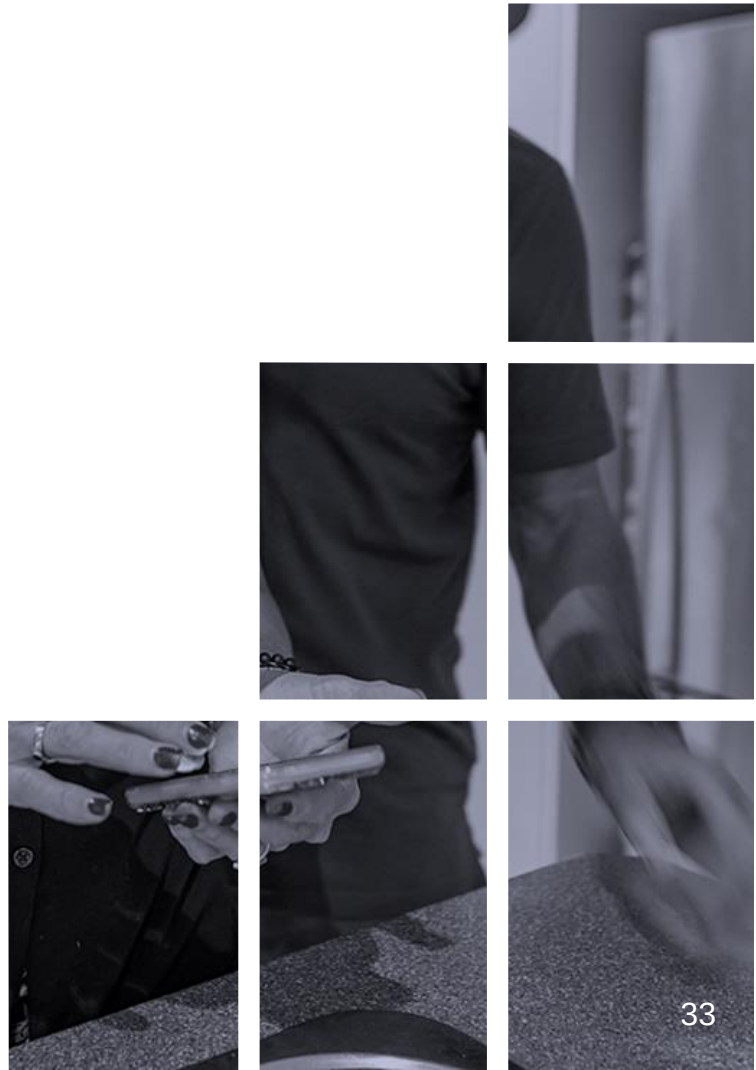
b) JOINT ACCOUNT has not been elected for data sharing



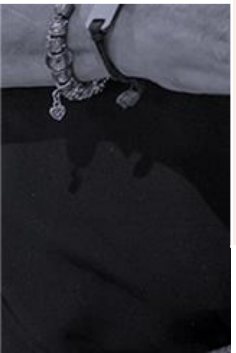
Interactive click through version

Appendix 2:

Additional scenarios.



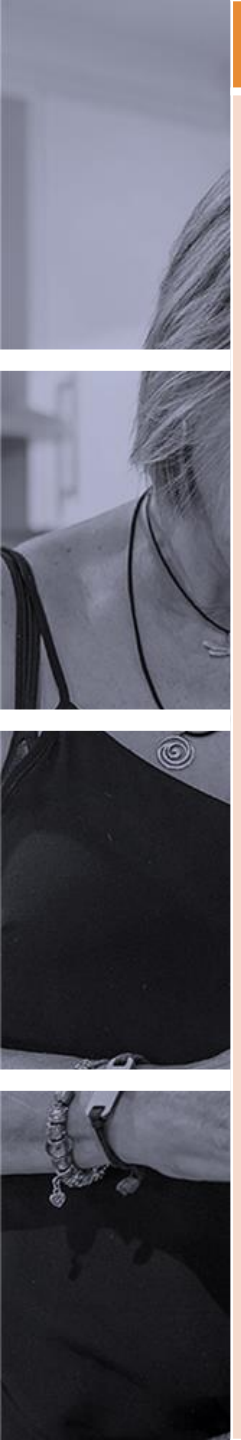


Scenario	What happens in CDR?	What else can happen?	What's missing?
Mental illness / vulnerability JAH1 has a diagnosis of bipolar disorder and, in the past, has acted in financially irresponsible ways during the manic cycles of an episode of their illness. Both JAH1 and JAH2 are aware of this and are trying to manage it. They have not informed the bank of the situation as JAH1 is worried that sharing the information may negatively affect their ability to obtain credit in the future should they need it.	CDR Rules make provision for a Data Holder not to disclose required CDR data where the DH considers this to be necessary to prevent physical or financial harm or abuse [*Rules* 4.7(1)a]. Data Holders can implement 2 to authorise consents, but this is not mandatory. As the bank is not aware of JAH1's condition there are no active safeguards.	JAH1 makes valid CDR consents when they are not in full control of their ability to make rational and informed decisions, due to mental illness. In a future write access CDR paradigm, this could result in JAH1 incurring financial harm for themselves and for JAH2.	a) Simple mechanisms for JAH to self-disclose their experience of and/or potential for causing financial harm, if they choose to do so. Ideally, this should be integrated with system decision points, such as (for banking) the process of JAMS election b) A requirement for DH to proactively offer 2-to-authorise consents where a joint account customer discloses vulnerability. c) Mechanisms that allow JAH to nominate higher visibility of consents – for example to receive an email notification as well as a dashboard notification.
Domestic violence JAH1 has recently left a violent relationship and moved interstate. The joint account remains open and has an active JAMS election. JAH2 does not know her current whereabouts but is trying to locate her. There is no DV flag on the account.	JAH1 shares data from a joint account through CDR to demonstrate her credit history to a new provider. JAH2 still has online banking with the same DH and sees details of the CDR data sharing authorisation as it relates to the joint account on their DH consumer dashboard. This gives JAH2 information including what data is being shared, and which ADR has requested it.	The ADR only has a presence in one state. JAH2 now has a solid clue to where JAH1 has gone.	a) An alert to JAH1 at the point of giving consent for data sharing that JAH2 will see this activity by default. (*) This might occur at the point of authorisation, enabling: b) Mechanisms for JAH1 to notify the DH of abuse and enact CDR safeguards (noting that even with such a mechanism not all victim-survivors of abuse will feel comfortable or supported to make the disclosure).

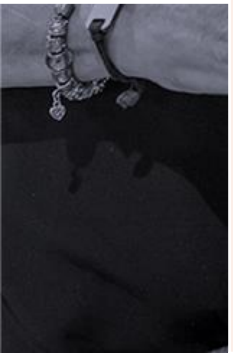
(*) In October 2020, the ACCC consulted on proposed rules that would require all joint account holders (JAHs) to be notified when another joint account holder gives an authorisation (see proposed clause 4.16 of schedule 3); and which would require JAHs, in electing a disclosure option, to be notified that under such an election all JAHs receive consumer dashboards which, where CDR data is shared under such an election, would make authorisations made by all JAHs visible (see proposed clause 4.6(7)(a) and (d) of schedule 3). These rules are distinct from the recommendation in this report that consumers be notified that the other joint account holder will be alerted to sharing before authorizing – ie, as part of providing informed consent.

Scenario	What happens in CDR?	What else can happen?	What's missing?
Domestic violence JAH1 and JAH2 have separated following an abusive relationship. JAH1 is living in the family home with the children and is seeking to refinance the mortgage. She wants to share data from a joint loan account that does not have a JAMS election in place.	JAMS election is required. Depending on the DH, there may be a notification sent to JAH2; or it may be up to JAH1 to broker that contact. JAH2 is contacted (by either JAH1 or the bank) but chooses not to elect the account in JAMS [Data sharing does not proceed] **OR** JAH2 provides their account election and JAH1 can nominate the account for data sharing. **[**Data sharing proceeds]	JAH1 does not feel safe contacting JAH2 (or is no longer on speaking terms with JAH2) and abandons the process [Data sharing does not proceed] "Both account holders having to give permission for the account to be sharable potentially could be a problem if she's left and she now wants to look at price comparisons and move on with her life but because he and she never gave [JAMS] approval for that account previously then she can't do that without his knowledge, and she can't [share her CDR data]. So that's maybe one problem that after she's left and she's trying to separate out all the joint accounts she's not able to do that." –INTERVIEW 6	The *CDR rules expansion amendments Consultation Paper* published 30 September 2020 describes proposed additions to the Rules to: "enable vulnerable consumers to share CDR data on a joint account as if the account was held in their name alone, where the data holder is satisfied that to do so is necessary in order to prevent physical or financial harm or abuse."[6] An addition of this kind could remedy this scenario in circumstances where JAH1 is, as well, being supported to disclose the abuse to the DH, and the DH has robust and effective protocol in place to enact the Rule.
Domestic violence JAH2 wants to continue exerting control over JAH1 after she's left. The joint account they shared is closed, but had an active JAMS election in place at the time it was closed. The DH was not aware of abuse within the relationship, so there is no flag on the account. JAH1 has consented to share data with an ADR.	JAH2 still has online banking with the same DH and sees details of the CDR data sharing authorisation as it relates to the joint account on their DH consumer dashboard, including duration of the consent	JAH2 revokes authorisation for the data sharing via notification on their DH dashboard. **OR** JAH2 withdraws JAMS election **OR** JAH2 allows data collection to proceed initially but then revokes authorisation after a period of weeks or months so that her ADR product unexpectedly stops working as intended	As above.



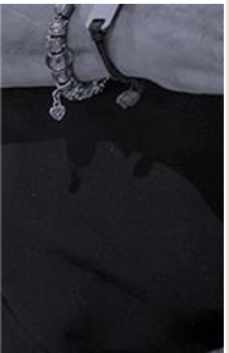
Scenario	What happens in CDR?	What else can happen?	What's missing?
Future paradigm: CDR includes insurance sector JAH1 is not very data literate, but has agreed to JAMS election after a conversation with JAH2 in which JAH2 explained why they want to use CDR. JAH1 has no issues with JAH2's CDR activity. JAH1 subsequently receives an email from their airline loyalty program including a CDR value proposition from an ADR to "get a better deal on your insurance and boost your points". JAH1 clicks on the link. JAH1 is taken to the ADR's pre-consent page. Reading this page, JAH1 doesn't really understand the proposition, but they do trust the referring airline loyalty program, having been a member for more than twenty years- and the bonus points on offer will be enough for flights to visit the grandkids interstate; so they continue.	The ADR consent flow prompts JAH1 to authorise data sharing from both individual and joint accounts with their data holder; JAH1 provides this consent, because they remember JAH2 was very enthusiastic about CDR. As the JAMS elections are already in place, consent proceeds and data sharing commences.	JAH1 has "consented" to share data but is not really sure what they have shared or why. They start receiving related insurance offers from the ADR and are feeling increasingly stressed because they don't understand the context and are worried that they may have done something that will affect their insurance policies. Embarrassed, they ignore it in the hope it will go away, and avoid further CDR activity. **OR** They accept one of the offers for a cheaper insurance premium, not realising that the policy does not include a particular clause specific to their needs. When they seek to make a claim they find they are not covered. **OR** After sharing data, they are not provided with a better offer. When it comes time for renewal of their existing policy, they see their premium has also increased more than usual.	Consumer awareness and capability of what CDR is and how it works. CDR standards or guidelines to cover pre-consent processes relating to how use cases and services are explained to consumers. "There's potential for harm in that someone ends up losing control not only of their own data, but by losing that data losing [control over] the decisions that get made using that data." – INTERVIEW 4



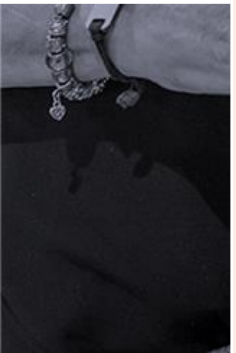
Scenario	What happens in CDR?	What else can happen?	What's missing?
Minor living independently, seeking to get a better retail energy deal. JAH1 is 17 years old and living independently after having left the family home due to escalation of a range of longstanding and intersectional vulnerabilities.	Banking: Minors are not eligible CDR consumers. Energy: Rules not defined, but likely to exclude minors from being eligible consumers. Telco: Rules not defined, but likely to exclude minors from being eligible CDR consumers	Concerns raised by some participants echo those highlighted in the CDR Energy Rules consultation regarding the risk of CDR participation putting minors at risk of predatory and exploitative behaviour. Others noted such risk does not vanish on an individual's 18th birthday, and prohibiting minors who are living independently, often due to family breakdown, from accessing CDR places another layer of exclusion on an already vulnerable cohort.	"I think if a minor is an energy account holder they absolutely should be [eligible CDR consumers] – otherwise they just have a disadvantage, they have a barrier to understanding their usage, and making good choices – for an arbitrary reason." - INTERVIEW 8
A joint account holder with limited English language skills JAH2 does not speak English fluently and relies on their daughter (JAH1) to attend to financial matters. JAH1 tries to explain all activities and processes to JAH2, but sometimes this proves too difficult and she takes an action without explaining it. JAH1 wants to use CDR to find better energy and telco deals to minimise the household bills, but is struggling to explain the implications of CDR data sharing in a way that JAH2 can understand.		"It reminds me of My Health Record: you've got to be incredibly technologically savvy and involved in your own health management to understand how to navigate that platform and how to get the best out of it. Most of these types of technological platforms are built with a quite highly educated white person in mind, to be frank, so it will benefit a segment of society more than it will benefit others … you start to think how does that intersect with a CALD community, or a victim-survivor whose partner may be far more savvy or literate in these things than she is, or she's been prevented from learning English, or having access to any of those sorts of [digital] resources." - INTERVIEW 6	Culturally and linguistically diverse approaches to CDR awareness, education, and interface design. Research into cultural difference in relation to understandings of consent and data privacy. Complaints and dispute processes that are understandable and usable by CALD communities and others with barriers to literacies (financial, digital, data, or English language).



Scenario	What happens in CDR?	What else can happen?	What's missing?
Victim/survivor is not aware of abuse, does not acknowledge abuse, is prevented from disclosing abuse, or chooses not to disclose the abuse.	Nothing: CDR safeguards are not enacted.		"[How does] the victim-survivor know that they can place that flag? … And I've got to tell my bank and my energy provider and my water provider and my telco that I'm experiencing this - the expectations there on a person who's in a really vulnerable space are pretty high… so that's where those sorts of notional protection may become meaningless." – INTERVIEW 4
Victim/survivor discloses abuse to DH, but procedures do not exist or are not followed correctly.	Nothing: CDR safeguards are not enacted.		"This boils down to the [capabilities of different data holders] … banks – compared to other industries – are probably getting a lot better at being able to explain to a customer, if they know there's abuse: well we could do this, but this will be the result, and being very clear about it." –INTERVIEW 2
If a future "write access" paradigm were to arise for CDR	There was agreement that 2-to-authorise consent would be necessary for joint accounts if a write access CDR paradigm were introduced in the future.	A 1-to-authorise model for requiring consent of joint account holders would create additional layers of risk for vulnerable consumers by scaling up the consequences of data sharing (including with regard to access and pricing of essential services). A 2-to-authorise model may allow a perpetrator to bombard a victim-survivor with "nuisance" requests as psychological abuse within a broader physical and/or economic abuse scenario.	While it was recognised that 2-to-authorise could advantage those with coercive control over a joint account and disadvantage vulnerable consumers (by limiting their 'actual' ability to access CDR); the risks of 1-to-authorise write access were seen to be higher. Opportunity and need for inclusive system & service design was highlighted again – how can CDR processes play a part in identifying vulnerability and activating appropriate supports?

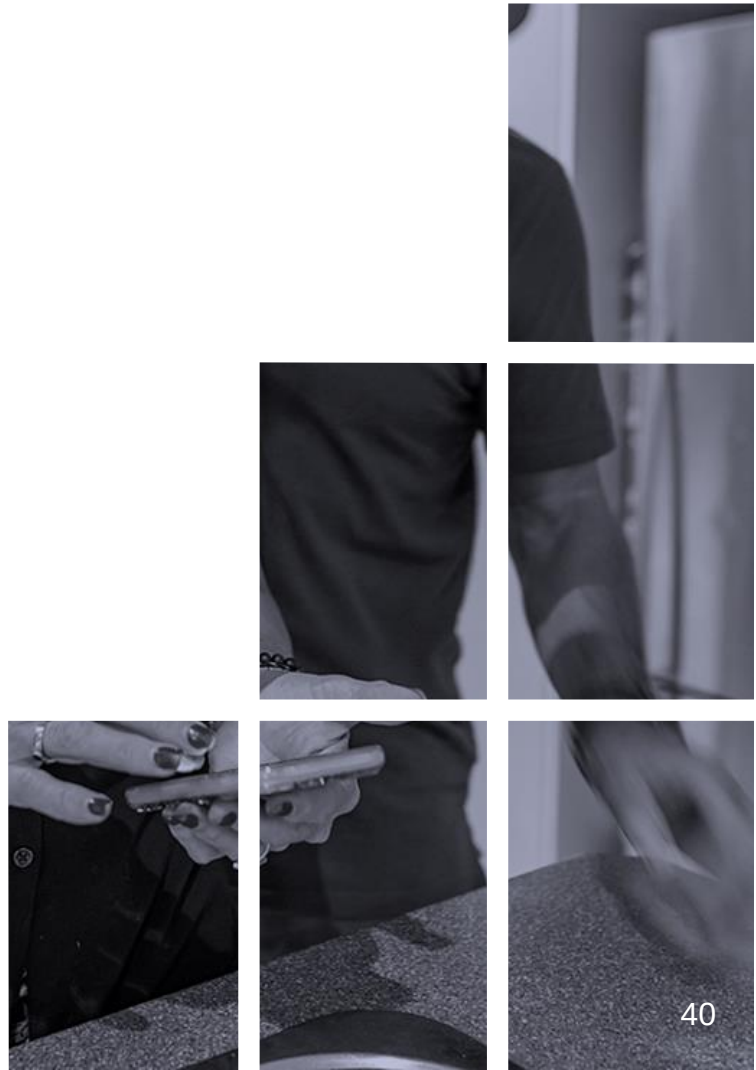


Scenario	What happens in CDR?	What else can happen?	What's missing?
JAH1 and JAH2 share an existing mortgage and maintain separate personal bank accounts. JAH1 has always liked a bet, but this has recently escalated into problem gambling. JAH2 is not aware of the changes to JAH1's spending on gambling. JAH1 and JAH2 are seeking to refinance their mortgage and decide to use CDR to help them find a good deal.	JAH1 and JAH2 each use the JAMS to elect their mortgage account as eligible for data sharing. JAH1 finds an ADR value proposition for home loan switching and goes through an ADR consent flow to share data from the existing joint loan account as well as from the individual accounts held by JAH1.	JAH1's increasing transactions to online betting accounts are visible in the CDR data. As a result, the pair are now considered higher risk borrowers for a home loan and the offers received as a result of using CDR are limited. They are not able to refinance their existing loan at the more competitive rate they had hoped for – and JAH2 does not understand why.	Simple mechanisms for JAH1 to self-disclose their gambling addiction (if they choose to do so) from both DH and ADR side. Ability for JAH1 and JAH2 to *both* share their CDR data from individual accounts alongside the joint account data for a single ADR value proposition relating to a joint product.
Risks due to sensitivities in energy data.	Participants had differing views on the sensitivity of energy usage data. May expose patterns which could place a victim-survivor of violence at risk of harm if an abusive party remained on the account as a JAH after moving out. Others noted that those kinds of insights cannot objectively reveal whether a dip in use at the same time every day means someone has left the house.	"Niche areas … for example life support … at the moment when a consumer switches to a new retailer they have to give all new information, like medical confirmation, to stay on the register. There's lots of potential that they could slip off, and if there's a third party switching them then there's a very high chance that they could slip off the register. That becomes a very real risk – of death really." – INTERVIEW 4	

Appendix 3:

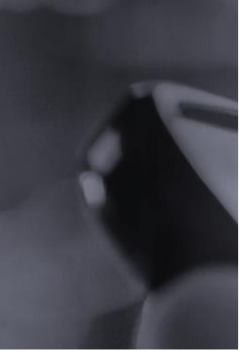
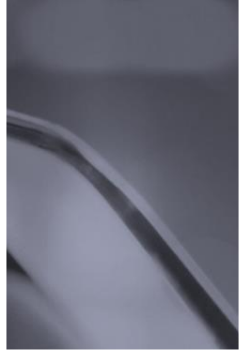
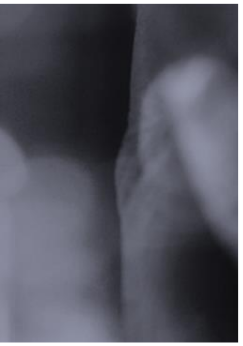
Interview matrix.



Interview matrix

Interview	No. of participants	Areas of expertise and organisational focus (*)
1	one	Consumer advocacy; legal services; financial hardship and resilience
2	two	Economic abuse and financial recovery; legal services; domestic and family violence
3	one	Social services; social policy and vulnerability; financial hardship and resilience
4	three	Consumer advocacy; energy sector; social policy; legal services
5	two	Consumer advocacy; telco sector
6	one	Domestic and family violence; advocacy; social policy
7	two	Financial services
8	one	Energy sector; social policy
9	two	Consumer advocacy; financial counselling; indigenous experience
10	two	Legal services; consumer advocacy; domestic and family violence
11	three	Legal services; advocacy; social policy and vulnerability

(*) Note: In some cases, interviews included participants representing more than one organisation.

Endnotes

[1] Josh Harle, Angie Abdilla and Andrew Newman (eds.) (2019) 'Introduction', *Decolonising the Digital,* p9. Sydney: Tactical Space Labs.
http://ojs.decolonising.digital/index.php/decolonising_digital/issue/view/DecolonisingTheDigital/2

[2] *CDR rules expansion amendments Consultation Paper* (September 2020), p29.
https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf

[3] ACCC *CDR Energy Rules Framework Consultation* (July 2020), p26.
https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf

[4] Australian Bankers' Association *Industry guideline: Financial abuse and family and domestic violence policies*, pp2-3.
https://www.ausbanking.org.au/wp-content/uploads/2019/05/ABA_Industry_Guideline_-_Financial_Abuse_and_Family_and_Domestic_Violence-Nov-2016.pdf

[5] *Consumer Data Right Support Portal '*Number of CDR consumer complaints received for each complaint type'
https://cdr-support.zendesk.com/hc/en-us/articles/900002460626-Number-of-CDR-consumer-complaints-received-for-each-complaint-type

[6] *CDR rules expansion amendments Consultation Paper* (September 2020), p39.
https://www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf

Note on methodology

Some scenarios included in this report were fully played out in a single conversation, others represent amalgamations of scenarios identified by multiple interviewees and described to us from a range of perspectives.

As such they do not always suggest a single point of agreement; nor do they necessarily reflect CPRC's own policy positions on the issues, which are articulated in documents separate to this piece of research.

We also recognise that discussions with a different universe of participants would have surfaced a different set of scenarios. This report is not intended to provide a definitive list of how the underlying issues will manifest in CDR data sharing from joint accounts.

Rather, we are pointing to the diversity and complexity of consumer circumstances; and voicing a need for the CDR regime to remain clearly accountable to all consumers whose data it is enacting rights to.

October 2020