

**CONSUMER
DATA
STANDARDS**

Consumer Experience Research Phase 3: Round 6

August 2020

Amending Consent: Account Amendment

Table of contents

Executive Summary	3
CX resources and engagement	7
<hr/>	
Research Approach	8
Approach	9
Session overview and prototypes	12
<hr/>	
Findings and Insights	
Amending Consent	17
Recommendations	24
Joint Accounts	25
Trustworthiness and Propensity to Share	29
Switching Canvas	30
Trust/Benefit Scale	31
Adoption Curve	32

Glossary	
ADR	Accredited Data Recipient
CDR	Consumer Data Right
CX	Consumer Experience
DH	Data Holder
JAH	Joint Account Holder
JAH1	Joint account holder initiating the consent
JAH2	Other joint account holder
JAMS	Joint Account Management Service

Executive summary

The Consumer Data Right

The Consumer Data Right (CDR) aims to give consumers control over information about themselves and share that information with third parties. The CDR promotes competition, encourages innovation, and consumer empowerment.

The CDR's consent and transparency requirements will facilitate more consumer control, privacy conscious behaviour, and the development of trust as a competitive advantage.

For consumers, the CDR is a safe, secure, transparent, and government regulated ecosystem that consumers can opt in to.

For ADRs, the CDR facilitates effective pathways to consumer outcomes by enabling access to machine-readable data for more accurate, tailored, and real-time insights.


The Data Standards Body's Consumer Experience (CX) Workstream is helping organisations provide simple, informed, and trustworthy data sharing experiences with positive consumer outcomes in the short and long term.

Overview

This report contains findings and recommendations based on Phase 3, Round 6 research. A qualitative approach was undertaken with 10 participants in 1:1 research sessions that ran for 60 minutes each. An additional 15 participants were engaged via an online platform for unmoderated testing.

Prototypes of the Consent Flow and related artefacts were used to facilitate insight generation. Participants were also asked to complete a series of activities to generate scores related to trustworthiness and propensity to share.

This round of research continued work on [amending consent](#), with a focus on the process of adding and removing accounts from an existing consent, including a joint account.

A detailed research approach can be found on the [Consumer Data Standards website](#) .

NB: Phase 3 reports do not necessarily reflect the position or direction of the government or Data Standards Body. Recommendations found within these reports represent a set of possibilities that will be reviewed and considered and are subject to change. Reports will inform rules and data standards development but should not be seen as indicative of the CDR's direction.

EXECUTIVE SUMMARY

Amending accounts

What we found out:

- Participants believed that the ADR is a logical starting point to add and remove accounts.
- Some participants viewed the manual process as a way of controlling how much of their data was shared.
- Generally, the tested 'unavailable accounts' pattern did not clearly convey the concept of certain accounts being 'unrequired' without further probing.
- Similar to previous research, recollection of terms improved after amending consent.
- CDR Receipts aided participants' comprehension, literacy, and recall.
- Participants had a notional understanding of 'concurrent consent' management.

We propose:

- Account amendments should be initiated from the ADR side.
- Adding new accounts should be opt-in, not automatic.
- ADRs should be able to specify the characteristics required for the use case - such as account types and other, more fine-grained details. For unrequired accounts, the unavailable accounts pattern should include explanatory information.

- CDR receipts should be provided whenever consents are amended to maintain consent quality, recall ability, and comprehension
- Concurrent consents should be distinguished using meaningful and descriptive names such as the purpose, use case, or software product. This should be consistent throughout the consent model, for both ADRs and DHs, to facilitate consent management.

Proposed next steps:

- Consider providing a generic discoverability function in future standards so ADRs can detect the existence of new accounts (but not the details of those accounts) and then prompt a consumer to initiate the account amendment flow.
- Consider future versions of the standards to allow for accounts to be removed from existing consents on the ADR side, without requiring authentication. DHs should be notified of this change so the account can be removed from the DH-side authorisation.

EXECUTIVE SUMMARY

Joint accounts

What we found out:

- Similar to previous research, there was a broad understanding that data sharing from joint accounts needed dual approval.
- Participants preferred 2-to-authorise and saw 1-to-authorise as taking away choice.
- Participants found the choice of 1-to-authorise or 2-to-authorise confusing during in-flow election. Most participants did not freely interact with links to additional content during the in-flow election.

We propose:

- If an in-flow election is supported, it should clearly outline the default option and provide instructions for how to change preferences, including in the Joint Account Management Service.
- DHs should consider notifying JAH2 whenever data is shared where a 1-to-authorise preference is in place, with details on how to manage joint account sharing.

- If in-flow election is offered, DHs could consider offering 2-to-authorise by default and, as sharing frequency and comfort increases, an 'always allow', 1-to-authorise option could be introduced.
- ADRs only know an account exists once it has been authorised; joint accounts will remain unknown to ADRs if JAH2 has not provided the necessary approval. DHs should provide consumers with CDR Receipts or equivalent confirmations, noting where a joint account has been associated with a consent but is 'pending' JAH2's approval.

Proposed next steps:

- Conduct a workshop on the CX of joint accounts to facilitate industry alignment and issue identification, focused on current state, 2 to approve, and other opportunities identified for joint accounts.

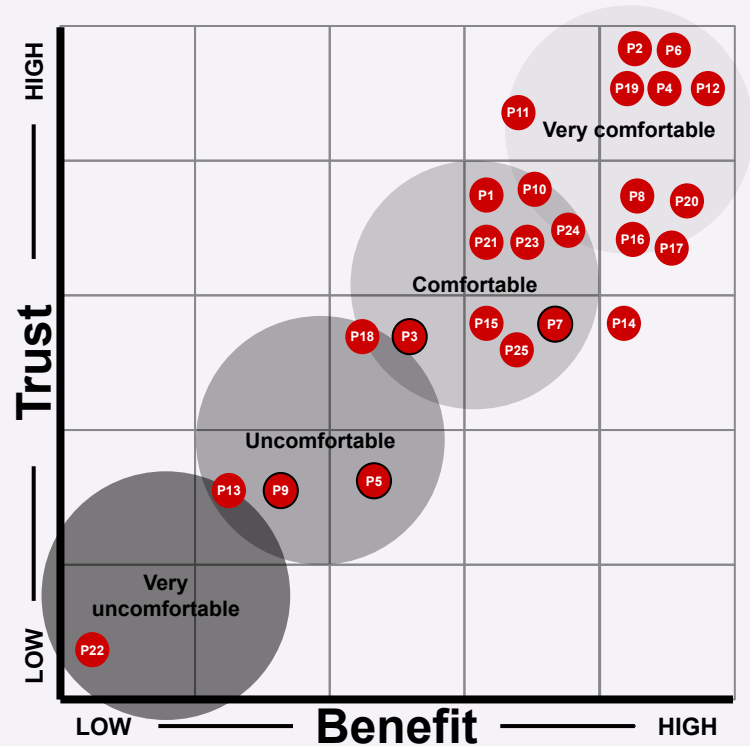
EXECUTIVE SUMMARY

Trustworthiness and Propensity to Share

What we found out:

- Consumer propensity to willingly share data increased after amending consent
- Consumer preference for CDR increased after amending consent
- The trustworthiness of CDR increases through repeated exposure to the consent model
- Participants positively likened the CDR process to their other fintech experiences, and felt the CDR process offered greater trust and comfort.
- Most participants explained that they would be willing to use CDR once it was more heavily adopted.
- Participants had greater recognition of CDR despite no prior CDR Education.
- Participants suggested that if they had a better understanding of the ADR, they would feel more comfortable to share data.

The Trust/Benefit Scale to the right plots the level of trust and perceived benefit each participant saw in the CDR process and the use case simulated in the prototype.



[Trust/Benefit scale](#) adapted from [New Zealand's Data Futures Partnership](#)

CX resources and engagement

The insights and recommendations found in this report are shared for general community knowledge; to inform the development of standards, guidelines, and the CDR more generally; and to support the rules and standards to be research-driven and centred on consumer consultation.

The Consumer Data Standards website contains the latest [CX Standards and CX Guidelines](#), which are also located on the [Technical Standards page](#).

The community can follow standards and guideline development on the relevant [CX consultation page](#) and on [GitHub](#).

CX reports containing insights and recommendations from ongoing consumer research and community workshops can be found in our [Knowledge Centre](#).

You can keep up to date with the CX Workstream's developments by signing up to our [mailing lists](#), subscribing to our [blog](#), and tracking issues on [Github](#).

You can contact the CX Workstream via email on cx@consumerdatastandards.gov.au.

Research approach

1. What did we want to find out?
2. Who did we research with?
3. What did we do?

RESEARCH APPROACH


What did we want to find out?

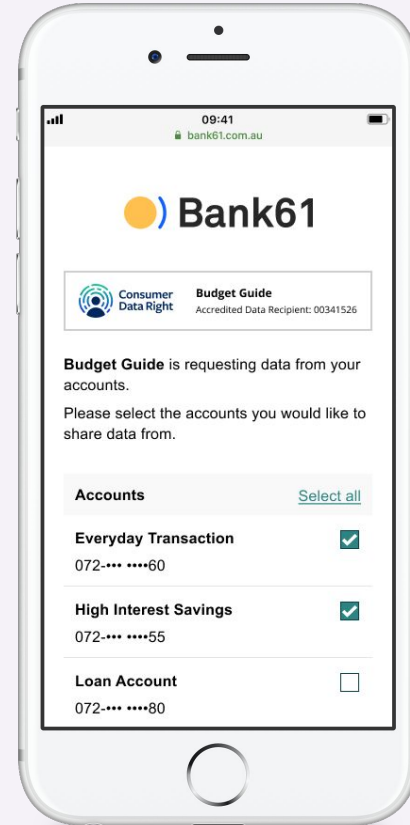
As part of our work on how to provide intuitive, informed, and trustworthy data sharing experiences, we tested a concept for how consumers could add and remove accounts from an existing consent. This flow included the adding of a joint account and the removal of an individual account.

We engaged 25 participants in total; 10 participated in moderated 1:1 sessions, and 15 participated in unmoderated online sessions.

For **Amending consent**, we wanted to:

- Simplify the experience of (un)sharing accounts with ADRs
- Simplify the account-adding experience for joint account holders
- Provide an intuitive, informed, and simple account adding and removing experience


Our research approach can be found on the [Consumer Data Standards website](#) .



RESEARCH APPROACH

Who did we research with?

A broad and diverse range of participants were recruited to help reduce bias and research out risk. A 'no edge cases' approach has been taken; deeming certain groups and needs as not important is antithetical to the design of an inclusive CDR. Instead of focusing on those who are already likely and able to adopt CDR, the research focuses on removing the barriers to CDR being inclusive and accessible, which will make CDR easier and simpler to access for everyone.

The recruitment process strives to reflect the demographic percentages outlined in the [Australian Bureau of Statistics 2016 Census Data](#) , and explicitly recruits those who may be experiencing vulnerability or disadvantage.

Participants have varying levels of:

- Digital, financial, and data literacies and experiences
- Privacy awareness
- Confidence in the English language
- Trust in Government and commercial organisations



RESEARCH APPROACH

Who did we research with?



R6P1

Male, 18-30 years
VIC - Metro



R6P8

Female, 61-70 years
NSW - Suburban



R6P15

Female, 61-70 years
NSW - Suburban



R6P22

Female, 71+ years
SA - Suburban



R6P2

Female, 41-50 years
NSW - Suburban



R6P9

Male, 71+ years
NSW - Suburban



R6P16

Male, 61-70 years
NSW - Small town



R6P23

Female, 51-60 years
NSW - Suburban



R6P3

Female, 51-60 years
WA - Metro



R6P10

Female, 41-50 years
SA - Metro



R6P17

Female, 31-40 years
QLD - Suburban



R6P24

Female, 18-30 years
WA - Suburban



R6P4

Male, 41-50 years
NSW - Suburban



R6P11

Male, 31-40 years
NSW - Suburban



R6P18

Male, 51-60 years
VIC - Suburban



R6P25

Male, 71+ years
SA - Metro



R6P5

Male, 51-60 years
ACT - Suburban



R6P12

Female, 31-40 years
VIC - Metro



R6P19

Female, 41-50 years
VIC - Metro



R6P6

Female, 18-30 years
QLD - Suburban



R6P13

Male, 31-40 years
NSW - Large town



R6P20

Female, 51-60 years
WA - Metro



R6P7

Male, 31-40 years
VIC - Rural



R6P14

Male, 41-50 years
QLD - Metro



R6P21

Male, 71+ years
SA - Suburban

Engagement with participant:

- moderated 1:1 sessions
- unmoderated online platform



Identity and diversity

- 2 have non-English speaking backgrounds
- 5 have migrated to Australia from another country
- 3 have parents with non-english speaking backgrounds
- 2 have accessibility needs
- 3 are of Aboriginal and/or Torres Strait Islander descent
- 2 identify as LGBTIQ+



Financial situation

- 17 are financially comfortable
- 5 have unstable financial situations
- 2 relied on a government allowance
- 1 has had extended periods of financial distress in their life



Level of financial literacy

- 1 has low financial literacy
- 6 have medium financial literacy
- 18 have high financial literacy



Level of digital literacy

- 3 have low digital literacy
- 8 have medium digital literacy
- 14 have high digital literacy



Level of privacy awareness

- 5 have low privacy awareness
- 12 have medium privacy awareness
- 8 have high privacy awareness

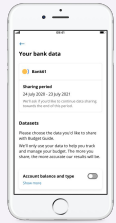
Session overview and prototypes

What did we do?

We had participants go through the 'original' consent flow prior to testing the 'add/remove accounts' flow. This established context and a baseline for the consent amendment flow. A qualitative approach was used to test low fidelity prototypes, and sessions also explored existing behaviours, expectations, and needs in one-on-one sessions for 60 minutes each. A detailed page on criteria, references, and metrics used by the CX team is [available online](#).

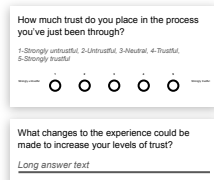
Approach

- moderated 1:1 sessions
- unmoderated online platform



'Original' consent flow Prototype

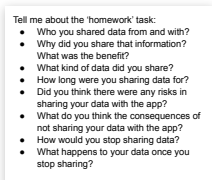
All participants engaged via unmoderated online platform.



Informed consent and Comprehension & Trust and Propensity to share data Survey form

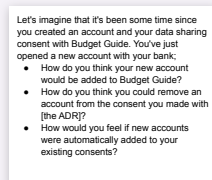
All participants engaged via unmoderated online platform.

1-3 days between 'original' and 'amending' consent



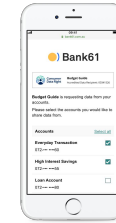
Recall of 'original' consent Interview or survey form

Participants in moderated 1:1 session were verbally questioned. Participants in unmoderated online sessions were given a survey form.



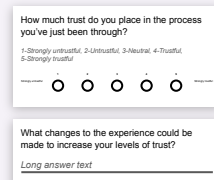
Add or remove accounts use-case and expectations Interview

Only participants in moderated 1:1 session were asked in-depth questions.



'Amending' consent flow Prototype and interview

All participants went through the prototype. Only participants in moderated 1:1 session were asked in-depth questions.



Informed consent and Comprehension & Trust and Propensity to share data Survey form

All participants were given a survey form.

'Add/remove accounts' experience

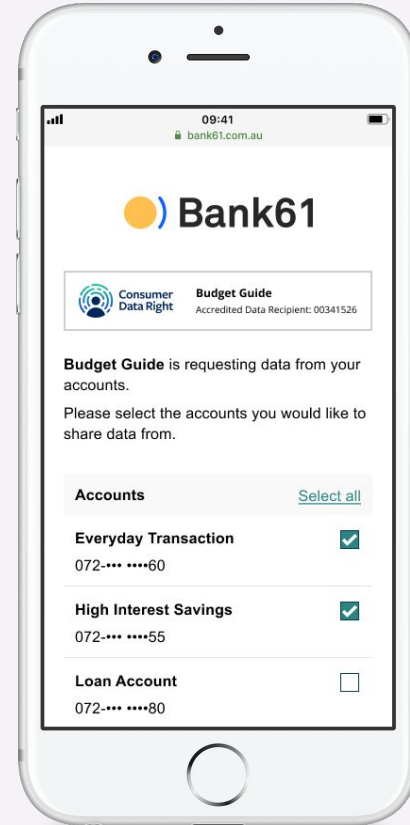
Prototype focus

- Amending consent, specifically in relation to adding and removing accounts.
- In-flow joint account election.

Scenario

- Budget Guide, an ADR, is a budgeting app that allows consumers to save money and manage their finances. Real-world bank is the DH.
- Consumer has recently opened a loan account and wants to add this account to Budget Guide. The loan account is also a joint account.
- Consumers are presented with the Budget Guide app and asked how they would proceed.

View 'Add or remove account' prototype 



Informed consent and Comprehension

Participants had to recall their consent terms multiple times. They were asked to recall:

- Who they were sharing data from and with (DH and ADR),
- Why they were sharing their data (perceived benefit),
- What types of data they elected to share,
- How long they were sharing data for (sharing period),
- Why they might stop sharing (risks or concerns),
- What happens if they don't share data (voluntary consent),
- How they might stop sharing their data, and
- What would happen to their redundant data

When recalling original consent (after time), participants were asked the above questions. Assessment and scoring was by proxy.

Directly after the Consent and Amending consent flows, participants were given a "fill in the blanks" style comprehension sheet to assess their understanding and memory of the prototype and task they had just completed.

I've shared data from [DH] with [ADR] so that I can [benefit/product purpose].

I've chosen to share the following types of data [data clusters or permissions].

The sharing period for my data is [12 months].

I am aware that by sharing this data I could risk the following [risks or concerns].

Some disadvantages of not sharing this data could be [consequence].

If I want to stop sharing my data I can do this by [contacting the ADR/DH or the ADR/DH Dashboard>Settings].

After I stop sharing my data, my data will be [deleted or de-identified].

RESEARCH APPROACH

Trustworthiness and Propensity to share

From consumer-participants, we wanted to understand:

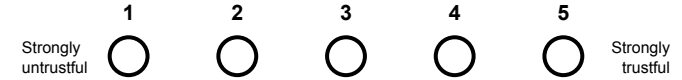
- How trustworthy do they deem the CDR and its actors to be?
- What increases or decreases their propensity to share CDR data?

To answer these questions, participants completed a form containing a series of questions relating to trustworthiness, comprehension and their propensity to share data (adapted from [Greater than X's Phase 2 research](#)). Participants were asked to:

1. Mark their response using the **Likert scale** with a score from 1 to 5. '1' being a negative indicator, '3' being a neutral indicator, and '5' being a positive indicator.
2. Provide **open-ended responses** for more qualitative questions.

How much trust do you place in the process you've just been through?

1-Strongly untrustful, 2-Untrustful, 3-Neutral, 4-Trustful, 5-Strongly trustful



Why have you given this rating?

Long answer text

Which parts of the experience DID inspire trust?

Long answer text

Which parts of the experience DID NOT inspire trust?

Long answer text

What changes to the experience could be made to increase your levels of trust?

Long answer text

Key insights for Amending consent

Consumer attitudes and experiences when adding and removing accounts from a consent.

AMENDING CONSENT

The ADR is a logical starting point to add and remove accounts

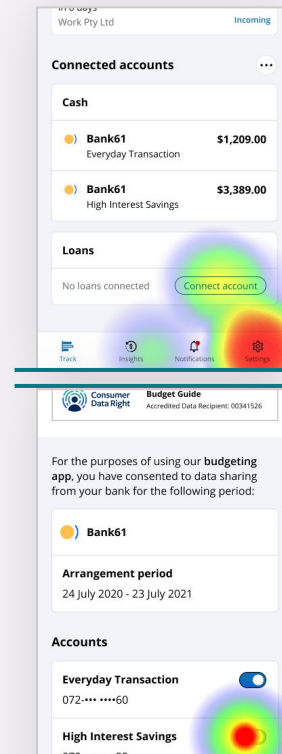
The vast majority of participants noted that amending accounts via the ADR was the intuitive choice. Only a few participants suggested that they may go to their bank (the data holder) to add or remove an account.

Amending accounts via the ADR aligned with existing experiences for participants who used similar financial apps.

While it is necessary to authenticate with the data holder when adding a new account for sharing, very few expected to authenticate with their bank when removing an account and most understood that they could remove an account by 'toggling' it off on their dashboard.

Research objective

F8: Provide an intuitive, informed, and simple account adding and removing experience



“ If you've entered that account from Budget Guide and entered all your account details from your bank there, that's where it should be removed as well. Not relying on the bank to do that on your behalf.

— R6P7

“ I'd go back to app. Go in to manage my settings and put all the information of the new account in there.

— R6P4

Recommendations

Account amendment should be initiated from the ADR side.

Future versions of the standards should allow accounts to be removed from existing consents on the ADR side, without requiring authentication. DHs should be notified of this change so the account can be removed from the DH-side authorisation.

AMENDING CONSENT

Manually adding new accounts was expected and heavily tied to personal control

Most participants expected to add new accounts manually, based on when it was necessary or beneficial for them to do so.

Some participants viewed the manual process as a way of controlling how much of their data was shared. In particular, this control is seen as a way to 'test' out ADRs and limit their exposure to possible risks.

Some participants expected new accounts to be added automatically, but still expected substantial control over data sharing.

“ *If every time I do something... and this over here is grabbing that data that makes me a little uneasy... I would imagine that it has to be entered by me and added by me and linked by me.*

— R6P7

“ *If I were to share my personal details with such an entity, I would want it to be one that I know very well about... I'd want as many controls around it as possible and have the ability to be able to pick and choose what I'm sharing'*

— R6P7

“ *I would hope that they wouldn't just get automatic access to it... assume I would have to give [ADR] access to that account to give approval. So I'd have to nominate the account.*

— R6P8

Recommendation

Adding new accounts should be opt-in, not automatic. ADRs are not currently able to discover accounts if a consumer has not already shared them. An opportunity exists for the standards to provide a generic discoverability function so ADRs can detect new accounts, but not the details of those accounts, and then prompt a consumer to initiate the account amendment flow.

Research objective

F8: Provide an intuitive, informed, and simple account adding and removing experience

AMENDING CONSENT

Displaying 'unrequired' accounts was of limited utility

We tested a concept where an ADR could specify the types of accounts they required, and omit unrequired accounts. We repurposed the 'unavailable account' design pattern to outline unrequired accounts, but participants **did not generally notice or easily understand the concept of 'unavailable accounts' in this context.**

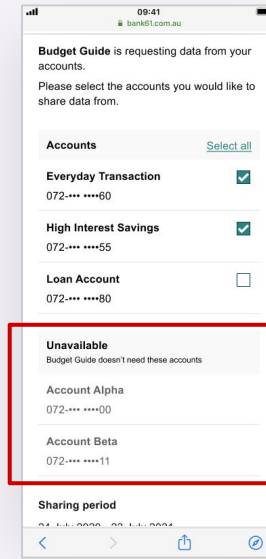
After some probing, participants suggested that these accounts could be 'unavailable' due to the type of account. They assumed that these accounts could be closed/inactive accounts, eAccounts (with limited function), company/joint account, or loan/insurance accounts.

Some participants assumed that these accounts were 'unavailable' due to technical limitations between the ADR and DH.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

F6: Simplify the experience of (un)sharing accounts with ADRs



“ *They don't automatically have the same range of functions as these accounts, so only certain named accounts you can make payment out of [...] they might not have that functionality, or you haven't granted them functionality.*

— R6P5

“ *I'd say it's some sort of limitation or something on the app side that cannot configure those accounts.*

— R6P6

← *'Unavailable' and unrequired accounts presentation*

Recommendation

ADR's should be able to specify characteristics that are required for the use case - such as account types and other, more fine-grained details. For unrequired accounts, the unavailable accounts pattern should include more explanatory information on why they aren't available.

However, we hypothesise that omitting 'unrequired accounts' altogether will be intuitive if the link between accounts and use case is clearer. For example, only showing credit accounts for a 'Credit comparison' is logical; the 'unavailable account' pattern would not add any more value than hiding unrequired accounts, altogether.

AMENDING CONSENT

Recollection improved after amending consent

Participants had to recall their consent terms multiple times:

1. After completing the consent flow (their original consent).
2. During the session, we recapped the original consent. Note: Participants had previously completed the consent flow between 1-3 days before the research session.
3. After completing the amending consent flow.

Averages for recalling the original consent terms was high at 71.6%, which dropped slightly when asked to recall those terms several days later (to 67.6%).

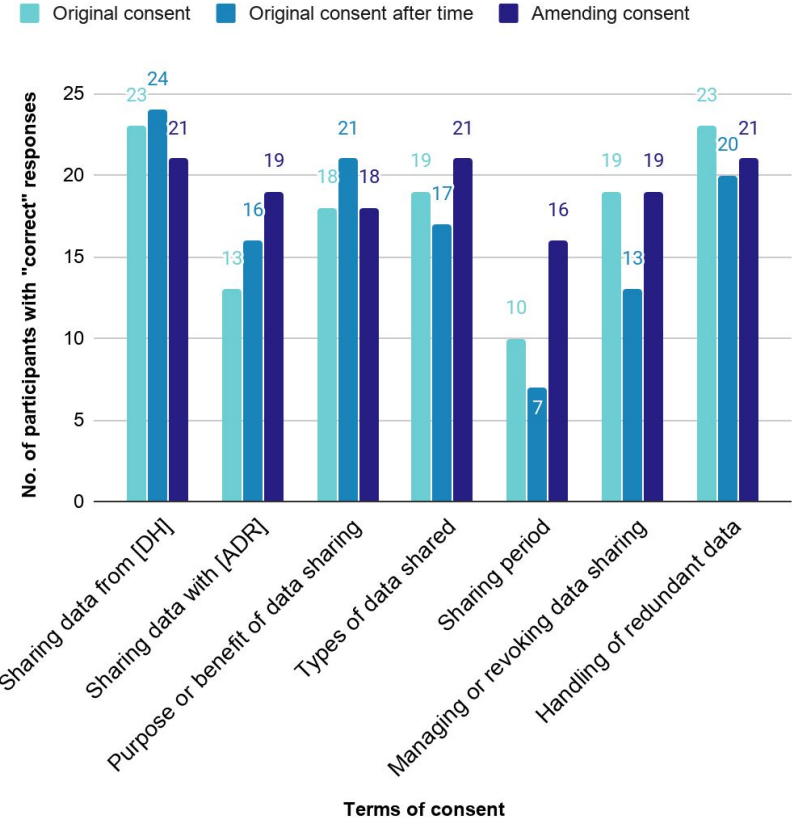
After completing the amending consent flow this average increased to 86.8% accuracy.

Research objective

F4: Understand the consumer's ability to recall the terms of the original consent.

D3: Understand how informed consumers are when/after they have given consent.

Recalling terms of consent



AMENDING CONSENT

CDR Receipts aid comprehension, literacy, and recall

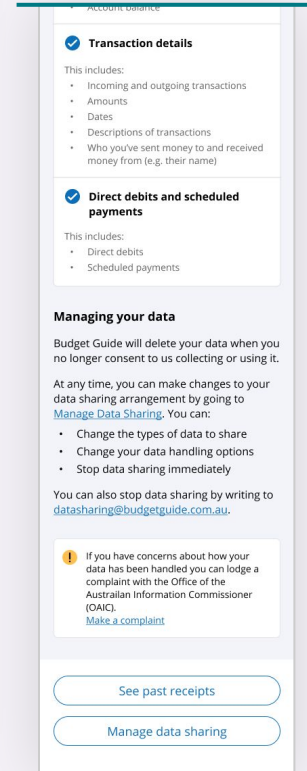
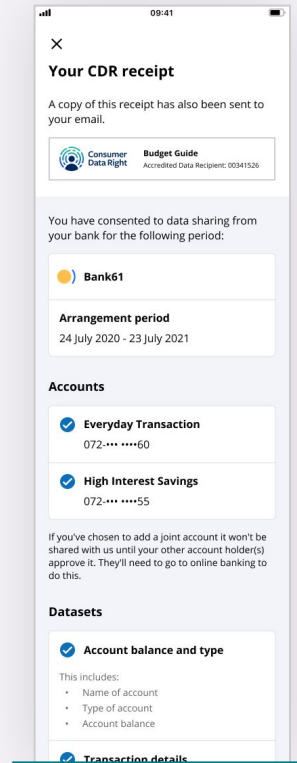
Even without prototypes or other stimulus, all participants were able to describe what the process of adding a new account would likely involve.

Omitting Authorisation (review of datasets/uses) did not adversely impact quality of consent. Participants did not note its absence and recall ability remained very high (86.8% accuracy on average).

Probing at the end of prototype completion found high levels of comprehension of the amending consent process, demonstrating the importance of providing an updated CDR receipt to facilitate recall and comprehension.

Research objective

F2: Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent)



Recommendation

CDR receipts should be provided whenever consents are amended to maintain consent quality, recall ability, and comprehension

AMENDING CONSENT

Notional understanding of ‘concurrent consent’ management

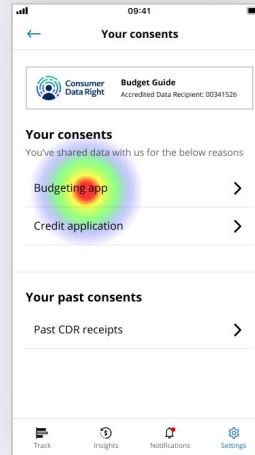
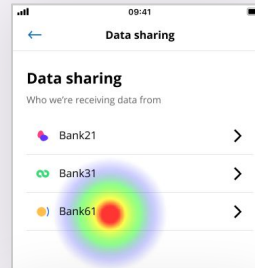
The prototype also tested concurrent consent management. When asked to manage the consent they had just amended, participants understood that they the consents were tied to different ‘sharing agreements’, such as different services provided by the one ADR.

High comprehension for the concept of concurrent consents was displayed across participants. This is particularly encouraging as participants did not complete consent flows for different use cases.

The idea of ‘multiple’ or ‘concurrent’ consents, and the way that this was represented in the dashboard, was intuitive.

Research objective

F2: Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent)



“ There’s obviously another section on [ADR] where you can nominate what you can use it for. So credit application was one of them.

— R6P7

Recommendation

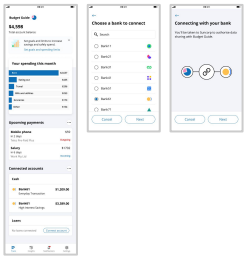
Concurrent consents should be distinguished using meaningful and descriptive names such as the purpose, use case, or software product. This should be consistent throughout the consent model, for both ADRs and DHs, to facilitate consent management.

Add or remove accounts

Add account

Remove account

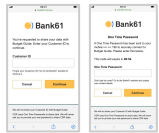
Trigger



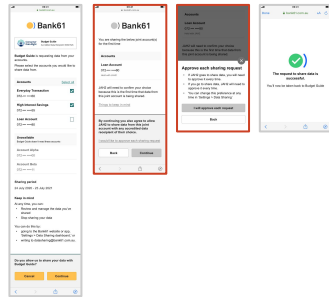
Refer to:

4 5

Authentication



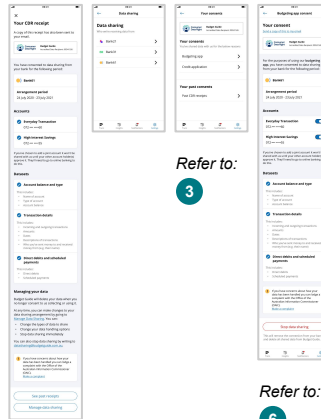
Authorisation



Refer to:

1

Post-consent



Refer to:

3

Refer to:

2

Amending consent flow

- Add/remove accounts
- In-flow joint account election

General 'amending consent' recommendations

1. ADRs should be able to specify characteristics that are required for the use case - such as account types and other, more fine-grained details. For unrequired accounts, the unavailable accounts pattern should include more explanatory information on why they aren't available. | [Insight on pg. 20](#)
2. CDR receipts should be provided whenever consents are amended to maintain consent quality, recall ability, and comprehension. | [Insight on pg. 22](#)
3. Concurrent consents should be distinguished using meaningful and descriptive names such as the purpose, use case, or software product. This should be consistent throughout the consent model, for both ADRs and DHs, to facilitate consent management. | [Insight on pg. 23](#)

Add/remove account recommendations

4. Account amendments should be initiated from the ADR side. | [Insight on pg. 18](#)
5. Adding new accounts should be opt-in, not automatic. ADRs are not currently able to discover accounts if a consumer has not already shared them. An opportunity exists to provide a generic discoverability function so ADRs can detect new accounts, but not the details of those accounts, and then prompt a consumer to initiate the account amendment flow. | [Insight on pg. 19](#)
6. Future versions of the standards should allow accounts to be removed from existing consents on the ADR side, without requiring authentication. DHs should be notified of this change so the account can be removed from the DH-side authorisation. | [Insight on pg. 18](#)

Key insights for **Joint accounts**

Understanding consumer attitudes and experience with joint accounts and data sharing.

AMENDING CONSENT

Providing choice during in-flow election can be confusing

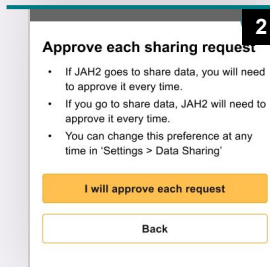
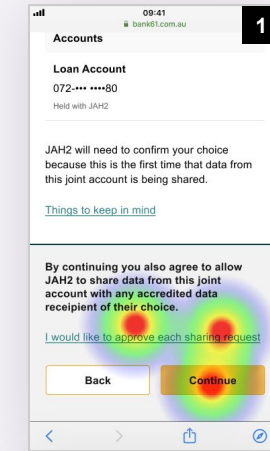
While participants expected in-flow joint account election, the presentation of the 1-to-authorise and 2-to-authorise options led to **confusion and oversight**. This led participants to proceed with the 1-to-authorise option despite expecting 2-to-authorise by default.

Most **participants did not freely interact with links to additional content during the in-flow joint account election**. Only after being prompted did participants begin interacting with links to further information about the 1-to-authorise and 2-to-authorise option.

The **presented design did not facilitate informed decision-making**, with many participants assuming that the 2-to-authorise copy was merely supplementary information for 1-to-authorise. For some participants, offering the 'choice' led to confusion and abandonment of the flow.

Research objective

F7: Simplify the account-adding experience for joint account holders.



“ *This is getting a little messy as far as I'm concerned so I would be hesitant to click on the blue line that says 'I would like to approve'* ”

—R6P9

“ *You have to jump through 50 hoops to get to what I want in the long run. I think it's too late. You shouldn't have to go through that process. I definitely would not do it [1-to-authorise]* ”

—R6P8

←

¹ A 1-to-authorise, in-flow election

² A 2-to-authorise option, in-flow election

NB: JAH1 refers to the joint account holder initiating the consent. JAH2 refers to the other joint account holder; the tested prototypes used a real name to represent JAH2

Recommendation

If an in-flow election is supported, it should clearly outline the default option and provide instructions for how to change preferences in the Joint Account Management Service. DHs should consider notifying JAH2 whenever data is shared where a 1-to-authorise preference is in place, with details on how to manage joint account sharing.

AMENDING CONSENT

1-to-authorise seen as taking away choice

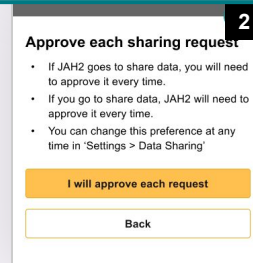
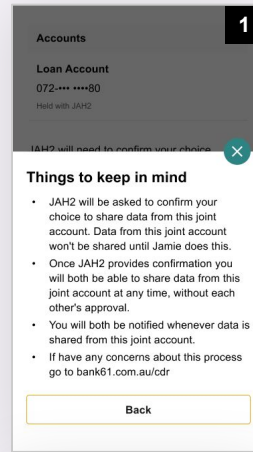
Most participants preferred both parties to approve each time data was shared (2-to-authorise), and suggested that 1-to-authorise was disempowering for both joint account holders. A 1-to-authorise preference felt "like giving full access", taking away "choice", and the ability to give consent.

The deciding factor for participants who preferred 1-to-authorise was convenience. They went on to explain that the other joint account holder didn't usually handle their joint finances. Based on screener and interview responses, it can be inferred that these participants had an amicable relationships with the person who was the other joint account holder.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

F7: Simplify the account-adding experience for joint account holders.



↑ ¹JAH1 additional information,
²JAH2 in-flow election

“ Since it's a joint account both parties need to be aware of what activities is happening. So I mean, there's no fraudulence [...] Otherwise it's like giving full access.

—R6P2

“ No, don't like that... Indicates to me that [JAH2] can choose, and you don't get to make the choice. By giving [JAH2] a choice to share data with whoever they feel like but they don't have to tell you about it.

—R6P8

“ I would be concerned that [...] one individual in that joint account is making these decisions to share that data, and the other person doesn't seem like [...] they're getting a say whether the information is shared or not.

—R6P10

Recommendation

If in-flow election is offered, DHs could consider offering 2-to-authorise by default and, as sharing frequency and comfort increases, an 'always allow', 1-to-authorise option could be introduced.

AMENDING CONSENT

Broad understanding that joint accounts need dual approval

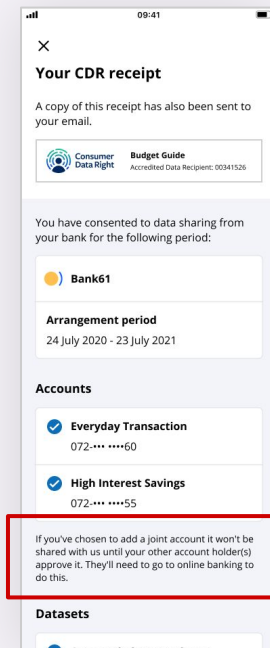
Similar to previous research, participants **believed that all parties needed to approve before data could be shared from a joint account.** This expectation allowed easy comprehension as to why joint accounts weren't on the CDR receipt; participants understood that it was because the other account holder had not yet approved data sharing.

Participants likened the CDR receipt to a 'success' screen. Some participants suggested that **showing the joint account with visual aids or text to indicate 'pending' status would be desirable.**

If the other joint account holder didn't have an online account, participants assumed that approval could also occur through the data holder's other channels— such as in-branch, over the phone or email. In these instances, participants believed that the other joint account holder would have to "prove who they were."

Research objective

F7: Simplify the account-adding experience for joint account holders.



↑
CDR receipt after adding a joint account

“ *What about pending? I think it just confirms your process. It'd be nice to see the account number and that it was pending, subject to your other account holder.*

— R6P8

“ *I would like to see that joint account in this accounts [section] here but maybe like greyed out. I guess that's showing me what I've got configured now, I know I've just gone through and done the process, but it's not confirming.*

It would be cool if like a notification come up, saying '[JAH2] approved your sharing requests.'

— R6P6

Recommendation

ADRs only know an account exists once it has been authorised; joint accounts will remain unknown to ADRs if JAH2 has not provided the necessary approval. DHs should provide consumers with CDR Receipts or equivalent confirmations, noting where a joint account has been associated with a consent but is 'pending' JAH2's approval.

Key insights for Trustworthiness and Propensity to share

Consumer attitudes around trust and their propensity to share CDR data.

TRUSTWORTHINESS & PROPENSITY TO SHARE





Switching canvas

This switching canvas provides an **overview of consumer behaviour and attitudes towards data sharing and CDR.**

This includes aggregated themes from 8 rounds of consumer research with 96 participants over a 14 month period.

NB: Phase 3 themes have been tagged [R#], with # referencing the research round. Themes specific to Round 6 have also been highlighted in a darker shade.

Adapted from [Greater than X's Design Toolkit](#) 

	Factors that <u>decrease</u> propensity to share	Factors that <u>increase</u> propensity to share
Current methods	<p> I'm fine with the way things are (apathetic to change)</p> <ul style="list-style-type: none"> Societal acceptance of current data sharing methods [R1,R3,R4,R5] No benefit/value from ADR's product [R1,R2,R3,R4,R5,R6] General hesitance to share personal data [R3,R4,R5,R6] 	<p> I'm dissatisfied with current solutions</p> <ul style="list-style-type: none"> General understanding of current data sharing methods [R2,R4] Involvement of authoritative and recognisable parties [R2,R3,R4,R5,R6] Transparency of ADR accreditation fosters trust [R2,R3,R6]
CDR process	<p> I'm averse to CDR proposition(s)</p> <ul style="list-style-type: none"> Low confidence in the Government's ability to enforce or handle data [R1,R2,R3,R6] Effort and uncertainty when withdrawing consent [R5] Fear of on-selling and unsolicited interactions [R2,R3,R4,R5] Access, use and mediation of data by unknown entities [R4,R5] CDR is "new" and "unknown" [R3,R4,R5] General concerns about ADR's data handling policies and practices [R2,R3,R4,R5] 	<p> I'm drawn to CDR proposition(s)</p> <ul style="list-style-type: none"> Clear benefit/value from ADR's product [R1,R2,R3,R4,R5,R6] CDR creates simple, easy and informed consent when data sharing [R2,R3,R4,R5,R6] CDR facilitates an increase in data literacy [R2,R3,R4,R5] Greater control and management of data [R2,R3,R4,R5] Requested data is minimised and specific as to purpose [R2,R3,R4,R5] Trust in ADR and CDR process is built over time [R4,R5] Familiarity with parties involved [R2,R3,R4,R5,R6]

TRUSTWORTHINESS & PROPENSITY TO SHARE

Trust/Benefit scale

This scale compares consumer trust of the CDR process and the perceived benefit from the ADR.

Participants were asked to separately rank their trust and benefit with the situation on a 5-point Likert scale. Their responses have been mapped on this trust/benefit scale.



Based on this cohort

Generalised characteristics and attitudes for:

High trust/benefit

- Mixed levels of digital literacy and privacy awareness
- Found the CDR process and accreditation assuring and secure
- Valued aggregation of multiple accounts in one place

Low trust/benefit

- Low-medium digital literacy
- High privacy awareness
- Prefers to manage finances the “old fashioned way”
- Does “not like using mobile phone for banking”

After amending consent, averages incrementally increased:

- Trust went from 3.5 to 3.9, indicating '3-Neutral' to '4-Trustful.' | [Insight on pg. 36](#)
- Benefit went from 3.6 to 4.2, indicating '4-Beneficial' to '5-Very Beneficial.' | [Insight on pg. 38](#)

[Trust/Benefit scale](#) adapted from [New Zealand's Data Futures Partnership](#)

TRUSTWORTHINESS & PROPENSITY TO SHARE

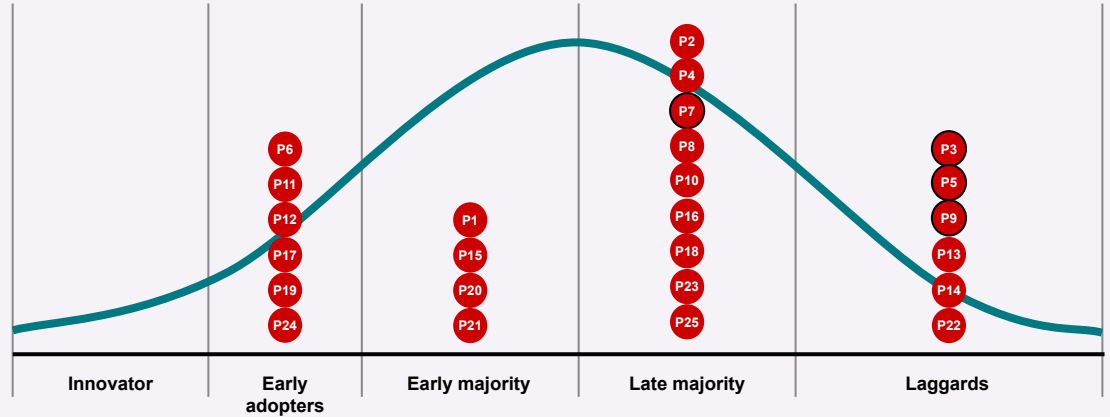
Adoption curve

This diagram highlights consumer willingness to share data if CDR was the 'new way of doing things.'

Categorisation is based on participants responses to:

- 'How willing would you be to share your data if this was the new way of doing things?'
- 'How does this way of sharing data compare to current ways of sharing data?'

Mapped to Diffusion of Innovations by Everett Rogers



Based on this cohort

After amending consent, averages incrementally increased:

- 'Willingness' went from 3.3 to 3.9, indicating '3-Neutral' to '4-Willing.' | [Insight on pg. 33](#)
- 'Preference for CDR method' went from 3.4 to 3.9, indicating '3-Indifferent' to '4-A bit better.' | [Insight on pg. 33](#)

■ Early adopters

- Medium-high digital literacy
- Low-medium privacy awareness
- Had previously used similar sharing methods
- Believed "benefit outweighs the risk"
- Found the CDR process and accreditation assuring and secure

■ Early/Late majority

- Early majority has medium-high digital literacy. Late majority has low-medium digital literacy
- Mixed levels of privacy awareness
- Believes they would "get used to it with time and exposure"

■ Laggards

- Low-medium digital literacy
- High privacy awareness
- Prefers to manage finances the "old fashioned way"
- Does "not like using mobile phone for banking"

TRUSTWORTHINESS & PROPENSITY TO SHARE

Willingness to share data increased with familiarity

After amending consent, participants on average expressed an incremental increase to 'willingness' and preference towards CDR.

Most participants were apathetic to the CDR process and explained that they would be willing to try it after it was more heavily adopted.

While they expressed confidence in the process, they wanted to "wait until all issues/problems had been ironed out first."

Participants who had already shared their data with existing fintech apps expressed a greater willingness to use the CDR. They believed this process felt familiar yet provided more trust and comfort than current experiences.

Other participants explained that they prefer to avoid data sharing altogether. When managing their finances, they would use their bank app or non-digital means.

Research objectives

D4: Understand if consumers have a propensity to share their data with the CDR.

“ *Have to move with the times and this app instills confidence.*

— R6P21

“ *I am quite willing already. CDR and use of app has increased this.*

— R6P6

“ *I do not do any current data sharing for budgeting as I do not need to.*

— R6P13

	Willingness to share data through CDR		CDR compared to current ways of data sharing	
	After original consent ¹	After amending consent ²	After original consent ¹	After amending consent ²
Average score	3.3 <i>indicating 3-Neutral to 4-Willing.</i>	3.9 <i>indicating 3-Neutral to 4-Willing.</i>	3.4 <i>indicating 3-Indifferent to 4-A bit better</i>	3.9 <i>indicating 3-Indifferent to 4-A bit better</i>

Scores were given on a 5-point Likert scale, with 1 being 'very negative' and 5 being 'very positive.'

¹ After original consent flow scores from 25 participants.

² After amending consent flow scores from 21 participants.

CDR is better than the current experience

Some participants had previously shared their bank data with existing fintech apps.

While there was a common understanding that there is "always risk" when sharing data, participants positively likened the CDR process to their other fintech experiences. Compared to their current experiences, participants felt the CDR process promoted greater trust and comfort through:

- data sharing assurance throughout the experience;
- sense of security;
- greater choice and control; and
- accreditation of companies

Research objectives

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

D4: Understand if consumers have a propensity to share their data with the CDR.

“ *I think there's always risk [...] when you share data. But if I was to compare the prototype to when I set up [existing fintech app] [...] this felt like data sharing was at the forefront, [...] so you felt reassured at every step of the way that you were at, you had the choice of whether you shared your data and you knew what you were sharing.*

I felt like there was less risk because it was very clear what was happening and I felt like I was in control of it. I guess with [existing fintech app], I'm still in control, but I don't know that they look to clearly spell out everything in the way that the prototype did. So yeah. I definitely felt a lot more reassured.

— R6P6

“ *I already use [two fintech apps] (and it never came across as secure as what this app did). My banking data gets transmitted to both of them. [...] This app looks more professional / sophisticated than others I've seen or used.*

I am familiar with the technology and less hesitant now to sign up with another app doing a similar thing (but better)!

— R6P17

Greater recognition of CDR despite no prior CDR Education

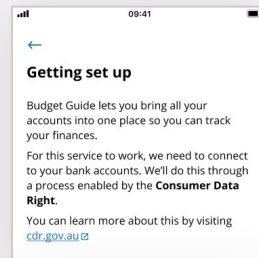
Similar to previous rounds, during the Consent Flow participants were given the option to explore additional CDR Education via a mock landing page with 'About' and 'FAQs' sections.

Although none of the participants in this round chose to engage with this page, it did not affect their ability to recall or describe CDR. **More than half of participants could recall the term 'Consumer Data Right' or CDR. An even larger number of participants were able to describe or infer what the CDR is or does.**

Compared to previous rounds, descriptions of what the CDR is or does have been more accurate and comprehensive. Most participants understood the CDR as "a legislative or data sharing requirement imposed by government or an institution in how institutions are to share data with one another." Some participants understood the CDR as the "consent" between them and the ADR.

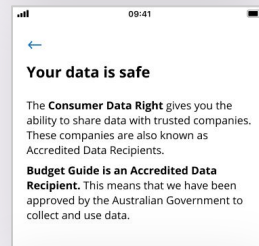
Research objective

D1: Understand if and how knowledge of CDR shapes trustworthiness and propensity to share.



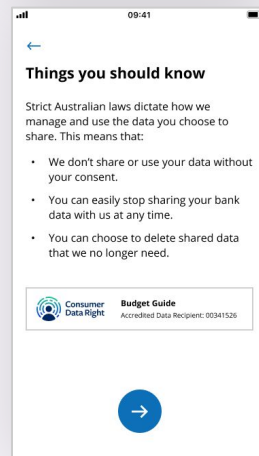
“ *[CDR] is my consent, that I give my consent to share data to [ADR].*

—R6P4



“ *[CDR] would be some sort of legislate protection for the consumer in consenting to providing by consent to provide the data to various third parties.*

—R6P5



“ *It gives us as the consumer the ability to know that the organisation we are dealing with has some integrity.*

—R6P17

“ *Some form of watchdog of consumer rights.*

—R6P25

←
CDR explanation during ADR onboarding

TRUSTWORTHINESS & PROPENSITY TO SHARE

Trust increases with repeated exposure to the CDR

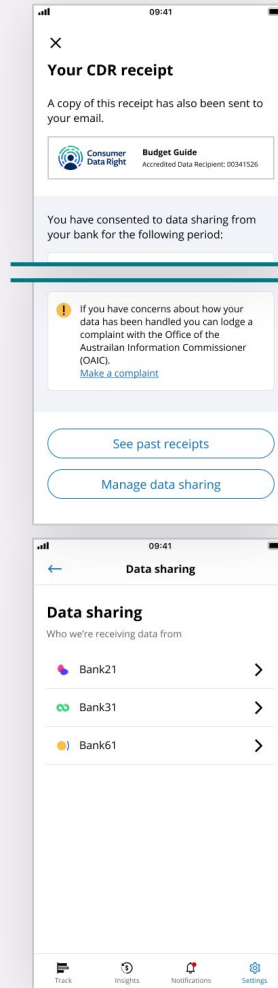
We asked participants to assess their trust levels with the situation. On average, participants gave a Likert response of 3.5, indicating '3-Neutral' to '4-Trustful' after the original consent. **This average increased slightly (3.9) after amending consent.**

Similar to previous research, this cohort initially expressed hesitance around sharing financial data. Participants attributed their increased trust to:

- CDR accreditation and the involvement of their bank and government
- Assurance and links to additional information throughout the process
- The easy, intuitive and transparent process

Research objectives

D2: Understand how trustworthy consumers deem the CDR.



“ **CDR accreditation instills much more trust than previous [fintech app process]**

— R6P6, when asked 'How much trust do you place in the process you've just been through?'

“ **I trust my bank and I'm certain that my information is safe.**

— R6P2, when asked 'How much trust do you place in the process you've just been through?'

“ **I could see that accounts from other institutions were linked [...] the fact that it was easy made it seem like the tech was sound and therefore the app/provider was legit.**

— R6P23, when asked 'Which parts of the experience DID inspire trust?'

Comfort increased after amending consent

After going through the original and amending consent flows, participants assessed their level of comfort around data sharing.

On average, participants gave a Likert response of 3.2, indicating '3-Indifferent' to '4-Comfortable' after the original consent. This average increased slightly (3.5) after amending consent.

While some participants felt "safe and secure" others believed that there was "no real security visible." There were concerns around ADR and DH privacy and security breaches.

Some participants suggested that **if they had a better understanding of the ADR, they would feel more comfortable to share data.**

Research objectives

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

D4: Understand if consumers have a propensity to share their data with the CDR.

“ *I have limited budget requirements, but I can see the need for this app if my finances were more complicated.*

— R6P21, when asked 'How comfortable would you be to share your own bank data with [ADR]?'

“ *My main concern is still privacy/security - if even the banks themselves have data breaches then surely a third party is at even more risk! Also, who owns the app and hence who am I actually sending all my data to?*

— R6P23, when asked 'How comfortable would you be to share your own bank data with [ADR]?'

“ *Unless I had full confidence in anything I would be reluctant to share my bank data on an app that I knew nothing about unless it was endorsed by someone I trusted.*

— R6P15, when asked 'How comfortable would you be to share your own bank data with [ADR]?'

Perceived benefit increased after amending consent

After going through the original and amending consent flows, participants assessed the benefit of sharing their bank data for budgeting and account aggregation. **After amending consent, the average of perceived benefit incrementally increased from 3.6 to 4.2, indicating '4-Beneficial' to '5-Very Beneficial.'**

While participants recognised that their DH app had in-built features to track spending, they generally believed that this functionality was limited. They also saw the value and the convenience of having multiple banks in one app. Participants understood that they needed to provide the ADR with "specific the information" for "better advice/guidance/insights."

Research objectives

D4: Understand if consumers have a propensity to share their data with the CDR.

“ *I like to be able to track spending against a budget and most banks don't have good functionality to do this. Can also configure multiple accounts from various banks.*

— R6P6, when asked 'How much benefit do you see in sharing data with [ADR]?'

“ *A one stop shop for all things money could be very handy. I could see real benefit in it. Currently I jump from at least 6 different platforms to arrange money and budget.*

— R6P20, when asked 'How much benefit do you see in sharing data with [ADR]?'

“ *The app can't work to its full potential without your cooperation as the user (and to some extent, your trust in them).*

— R6P17, when asked 'How much benefit do you see in sharing data with [ADR]?'

“ *App would need to be in possession of relevant information to work better.*

— R6P21, when asked 'How much benefit do you see in sharing data with [ADR]?'

Data Standards Body | Consumer Experience Workstream

t +61 2 9490 5722

e cx@consumerdatastandards.gov.au

w consumerdatastandards.gov.au