CONSUMER DATA STANDARDS

BIAS

Consumer Data Standards: Authenticate, notify, reauthorise

Phase 2 CX Stream 3 Report

June 2019

Table of contents

Stream 3: authenticate, notify and reauthorise

Executive summary

The Australian government is introducing a Consumer Data Right (CDR) to give consumers greater control of their data. The CX workstream is to help organisations provide consumers exercising their rights under the CDR with trusted and usable consent experience.

This report is part of the second phase of research. It is one of three streams of research, focusing on the **authenticate, notify** and **reauthorise** aspects of the consent model.

This stream's research involved a total of 20 participants. The cohort was skewed towards younger participants and early adopters, as this was a gap in phase 1.

Some of the key insights:

- **Propensity to share data**: Revocation increased consumers willingness to share data, while reputation and privacy issues decreased it.
- **Trust** in the bank, app and government: Trust varied between these three parties involved. Revocation and accreditation bought comfort, while privacy concerns were still very present.
- **Consumer privacy values**: Consumers displayed a tension between convenience and security.
- **Comprehension of the flows**: Participants had basic comprehension of the what, why and how but but added incorrect interpretations from their current understanding of data sharing.
- **Choice**: Consumers expressed a desire for choice of data and duration. Purpose of app drives their choice.

Executive summary

For the research, 9 different prototypes were built to test authentication, notification and reauthorisation needs, expectations and behaviours.

The scenario was to share data from their bank (data holder) to the Budget Guide app (the data recipient).

The key findings indicate that:

- The **Authentication with One Time Password (OTP) is recommended** to be the most preferred option. It presented the lowest level of unnecessary friction and potential drop-out compared to the other two flows.
- The **90 days notification** is deemed unnecessary by consumers. The message is unexpected and most likely be ignored. Recommend to stop notifying consumers every 90 days without a purpose.
- **Simplified reauthorisation flow from the data recipient to the data holder** is recommended for the reauthorisation flow. It has the right balance for the convenience vs security conscious consumers.

The following broader considerations are recommended to further inform the CX guidelines for the consent model:

1. Provide flexibility in the consent model
2. Carefully communicate the concept of CDR
3. Manage message fatigue
4. Continuous iterations of consent model for financial sector
5. Revisit data cluster taxonomy
6. Research data share around energy sector
7. Research for accessibility and inclusivity
8. Design for off-boarding experience

Overview

CONSUMER
DATA
STANDARDS

Overview of CX in CDR

The Australian government is introducing a Consumer Data Right (CDR) to give consumers greater control over their personal data. Part of this right requires the creation of common technical standards that make it easier and safer for consumers to access data held about them by businesses, and – if they choose to – share this data via application programming interfaces (APIs) with trusted, accredited third parties. The Consumer Data Right is intended to apply sector by sector across the whole economy, beginning in the financial sector before expanding into the energy sector, followed by telecommunications.

Data61 has been appointed as the Consumer Data Standards (CDS) team to develop standards that enable consumers to access and direct the sharing of data about them with third parties flexibly and simply, and in ways that ensure security and trust in how that data is being accessed and used. There are several work streams currently being delivered by Data61 including the API, Information security, Engineering, and Consumer Experience (CX) workstreams.

The ultimate aim of the CX workstream is to help organisations provide consumers exercising their rights under the CDR with trusted and usable consent experience.

Phase 1 of the CX workstream was recently completed. The key objectives of this phase was to develop a foundational pattern for consent, referred to as a Consent Flow, which is part of an overall Consent Model. The first report can be found https://consumerdatastandards.org.au/resources/reports/reports-cx/phase-1-cx-report/

In phase 2, the CX worksteam was split into 3 streams of work. They were tasked to specifically look into refining the consent flow, joint accounts, dashboards, revocation, reauthorisation, notification, authentication and cross sector applications.

This report is specifically about stream 3, who were looking to develop, test, and refine the **authenticate, notify** and **reauthorise** aspects of the consent model.

It also reports on the overall trust and privacy aspects of the consent flow.

The recommendations do not reflect the position of the Consumer Data Standards body, and will need to be reviewed (e.g. against security implications). This process may result in different recommendations.

Research methodology

CONSUMER DATA STANDARDS

Research methodology

Research objectives

Phase 2 Stream 3 continued to focus on consumer confidence, comfort, informed consent, and comprehension more broadly, but specifically looked at:

- Developing, testing, and refining the Authenticate, Notify and Reauthorise aspects of the Consent Model.
- Testing proposed authentication models
- Testing ‘Purpose Statement’ and ‘Revocation Statement’ in the context of reauthorisation
- Providing insight into consumer behaviour, needs, and expectations in relation to the sharing of data
- Testing and refining recommendations for how to put The Rules into effect
- Understanding users comprehension
- Understanding if users are willing to share their data after completing the flow
- What do consumers trust in the concept of sharing financial data
- Do users have any privacy/security concerns
- Do consumers understand the language used in the flow.

Second round additions

- Testing information for CDR on 1 pager
- Testing multiple bank account reauthorisation

Research methodology

Recruitment results

Numbers

2 rounds of 10 people, resulting in 20 overall.

Targets

Recruitment strived for diverse representation, including accessibility considerations. Phase 2 skewed towards younger participants (18-35) and early adopters as they were underrepresented in Phase 1 qualitative research.

Demographic was targeting Sydney metro and rural/remote Queensland.

Mandatory characteristics

- Included business owners and sole traders.
- Included over half early adopters
- Skewed towards a younger audience (18-35)

Research type

Exploratory research - Participants discussed appetite and expectations by answering open ended questions in one-on-one interviews, guided by an interview outline.

Evaluative research - Used prototype to test other qualitative areas like usability, accessibility, time to comprehension, and other metrics that assist the usability of the consent model and future adoption.

Research methodology

Research approach

Round 1

Round 1 was seeking to develop, test, and refine the Authenticate, Notify and Reauthorise aspects of the Consent Model. To do this, 5 prototypes were built:

- 2 x Authentication flow
- 1 x 90 days notification
- 2 x Reauthorisation flow

Each prototype was used to test consumers expectations and the friction of changing between 2 different parties. They were also used to understand where people went, and how much they wanted to be notified.

We wanted to test people's comprehension of data sharing and understand how that could be improved.

Business owners were also asked separate questions about language and data sharing.

Round 2

In the second round of testing, we ran through:

- 2 x Authentication flow (order varied)
- 2 x Reauthorisation flow (order varied)
- Plus, exploratory questions for multiple reauthorisation and messaging.

We learnt from the prior round that the scenario biased the test results, so for the first flow of each we set a task and runthrough unprompted. In this round, we only provided critical context and used the prototype to guide the participant. At the end of each flow, we tested for comprehension and propensity to share.

For the second flow, we probed around specific areas we wanted to learn about. This gave us a good mix of task completion, expectations and needs.

For the last round of questioning, we explored potential friction the consumer may have with multiple reauthorisation experiences. We also tested if upfront messaging would have changed a user's propensity to share.

Research methodology

Limitations and learnings

This was qualitative type research that was looking at attitudes, expectation and needs. This reports the consumer experience, not other strategic or technical considerations.

Scenario setup

We learnt from our first round of research that we biased some of the results by providing to much setup up front. We adjusted our methodology in the second round.

Measuring task completion time

We tried to test task completion time in the first round but there were too many variables. We found little value in the metric. We excluded the time completion metrics in the second round.

Measuring comprehension

We have not reported the comprehension findings from the first round, as we felt the bias made the results inconclusive. We reduced the bias in the second round by changing the methodology.

Use case

We only designed for 1 use case due to time constraints.

Rural and remote

There were no conclusive patterns of attitude and behaviours for our rural and remote participants. We were limited by the number of people we could access in the time.

Technical constraints

All flows were created to work within the technical boundaries provided to us, in consultation with Data 61 and their stakeholders.

Using fictional products

For the purpose of this research, we were limited in using a fictional products for data recipient and data holders. As a results, participants were faced with challenges around trust and reputation of the app and the bank in order for them to get through the consent model.

Accessibility needs

This was a noted gap in our research. In the next round this needs to be the focus of the research cohort to ensure this can be used by all Australians.

Joint accounts

Out of scope for Stream 3, handled in Stream 1.

Research methodology

Who did we speak to

		Round 1	Round 2
LOCATION	Sydney Metro	6	6
	Queensland (Rural)	2	2
	Queensland (Remote)	2	2
TECHNOLOGY	Early adopters	7	6
	Later adopters	2	4
	Basic use	1	0
BANK	Personal	6	5
	Business	4	5
AGE	18-35	7	7
	35+	3	3

Research methodology

Who did we speak to in round 1

Consumer | Sole trader/SME

Participant 1

- Male, 48, single, NSW
- Various casual jobs
- Budget conscious
- Late adopters of technology

Participant 2

- Female, 27, single, NSW
- Runs a small legal firm and a volunteer organisation
- Less uptight about privacy and data share
- Value convenience more than privacy

Participant 3

- Female, 41, NSW
- Married with 3 boys
- Working part-time in equities and financial planning business
- Security and privacy conscious

Participant 4

- Male, 29, single, NSW
- Runs a family business and side business in constructions
- Security and privacy conscious, especially in regards to business data
- Early adopters of technology

Participant 5

- Male, 28, single, NSW
- Emergency services officers
- Security and privacy conscious
- Early adopters of technology
- Invest in cryptocurrency (Bitcoins)

Participant 6

- Female, 28, single, NSW
- Self-employed - Legal practice
- Security and privacy conscious, especially in regards to business data
- Early adopters of technology
- Invest in cryptocurrency

Participant 7

- Female, 29, Glenlee - QLD
- Married no children
- Work in transport logistics
- Early adopters of technology
- Invest in cryptocurrency
- Use Raiz
- Value convenience more than privacy

Participant 8

- Male, 28, Bioela - QLD
- Married with 2 children
- Youth pastor
- Early adopters of technology
- Invest in cryptocurrency
- Has a few neo funds
- Security and privacy conscious

Participant 9

- Female, Toowoomba - QLD
- Married with 3 children
- Runs 3 businesses
- Converter to barefoot investor
- Early adopters of technology
- Value convenience more than privacy

Participant 10

- Male, Toowoomba - QLD
- Married with 2 children
- Project Manager
- Early adopters of technology
- Use Acorns
- Security and privacy conscious

Research methodology

Who did we speak to in round 2

Consumer | Sole trader/SME

Participant 11

- Male, 42, NSW
- Trainer and support for education software
- Late adopters of technology
- Invest in cryptocurrency
- Budget conscious
- Security and privacy conscious

Participant 12

- Female, 31, NSW
- Freelance graphic designer
- Early adopters of technology
- Use neo bank - Xinja
- Value convenience over privacy

Participant 13

- Female, 24, single, NSW
- Working as part time tutor
- No fixed income
- Has multiple term deposit accounts from parents
- Late adopters to technology

Participant 14

- Male, 39, NSW
- Runs a private investigator business
- Early adopters of technology
- Security and privacy conscious

Participant 15

- Male, 29, single, NSW
- Assistant editor
- Early adopters of technology
- Security and privacy conscious

Participant 16

- Female, 45, NSW
- A film-maker and producer and also runs a homeware online sales business
- Late adopters of technology
- Value convenience over privacy

Participant 17

- Male, 32, Gracemere - QLD
- Married with 2 children
- Primary school teacher
- Early adopters of technology
- Security and privacy conscious
- Use Raiz

Participant 18

- Female, 28, Yeppoon - QLD
- Married with 1 children
- Runs her own florist business
- Early adopters of technology
- Invest in cryptocurrency
- Bank with the local bank - Gateway Credit Union

Participant 19

- Female, 27, Bundaberg - QLD
- Married
- A contract cleaner - trying to get work
- Early adopters of technology

Participant 20

- Male, 33, Bundaberg - QLD
- Married
- Runs an IT consulting business
- Security and privacy conscious
- Early adopters of technology
- Invest in cryptocurrency (Bitcoins)


Synthesis of research

Key findings

CONSUMER
DATA
STANDARDS

Key findings

Summary

The focus of this research was to understand the needs, expectation and behaviour of authentication, notification and reauthorisation. The key findings report on:

- Propensity to share data when completing the flows
- Trust in the bank, app and government
- Consumer privacy values
- Comprehension of the flows
- Choice

The specific findings regarding authentication, notification and reauthorisation are included in the design patterns section (page 33).

Some of the key insights:

- **Propensity to share data**: Revocation increased consumers willingness to share data, while reputation and privacy issues decreased it.
- **Trust** in the bank, app and government: Trust varied between these three parties involved. Revocation and accreditation bought comfort, while privacy concerns were still very present.
- **Consumer privacy values**: Consumers displayed a tension between convenience and security.
- **Comprehension of the flows**: Participants had basic comprehension of the what, why and how but but added incorrect interpretations from their current understanding of data sharing.
- **Choice**: Consumers expressed a desire for choice of data and duration. Purpose of app drives their choice.

Propensity to Share

Score

During the consumer interviews, the participants were asked at the end of the first consent flow if they would be willing to share their data based on what they'd completed and comprehended. They were asked to rate their "propensity to share" on a scale of 0 to 6.

Those that rated low, stated the reasons were:

- No value in the app for them
- App had no reputation
  - Who's the developer
  - No reviews or research done before
- Privacy concerns from the app
  - Don't believe the data will be used the way stated.
- Not enough detail on accreditation

" I'd have to look into it, they talked about being an accredited data share, I can't remember the exact language [...] what is one of the parameters they're allowed to use the data for. When I research there, I would feel a lot more comfortable."

CDR Phase 2 | round 2 | Participant 17

Propensity to Share

Score

Consumers that rated high to share their data, stated the reasons were:

- Endorsement by government
- Value provided by the app
- Revocation available
- Easy to complete

People who rate highly to share their data had a lower comprehension of the content they'd seen.

Knowing there is choice and the ability to stop was comforting to participants. It increased their willingness to share as they felt like they could reverse their actions

"Multiple times I had been told or had been given that option, you can revoke this at any time. Seeing that automatically makes me feel more comfortable."

CDR Phase 2 | round 2 | Participant 7

Propensity to Share

Does knowing more about CDR change anything?

Nearing the end of the Round 2 sessions, users were shown a page of content with more information about the Consumer Data Rights (CDR). They were asked if this would change their propensity to share. After seeing this information, some changed their score.

Score increased

Some reported that they felt more trust and comfort knowing there was legislation behind it. By seeing and understanding more of the CDR information, they felt like there was appropriate government backing behind it.

“I'd go up to a three or four because I think you're more willing now that I feel more comfortable with knowing that there's legislation behind or penalty behind this”

CDR Phase 2 | round 2 | Participant 17

Score decreased

Those that had a decreasing propensity to share, misinterpreted the information. They felt that the CDR would restrict their choice because every company would need to be accredited to share their data. This led to feeling the government was restricting their choice to share with non-accredited or overseas agents.

Another participant felt that the government would be able to take their data as a result of accreditation. This had not been communicated in any of the copy and was a misinterpretation.

“I feel like there's some barrier that gets lifted, in the way, there's some sort of red tape that the organization have to go through”

CDR Phase 2 | round 2 | Participant 11

Propensity to Share

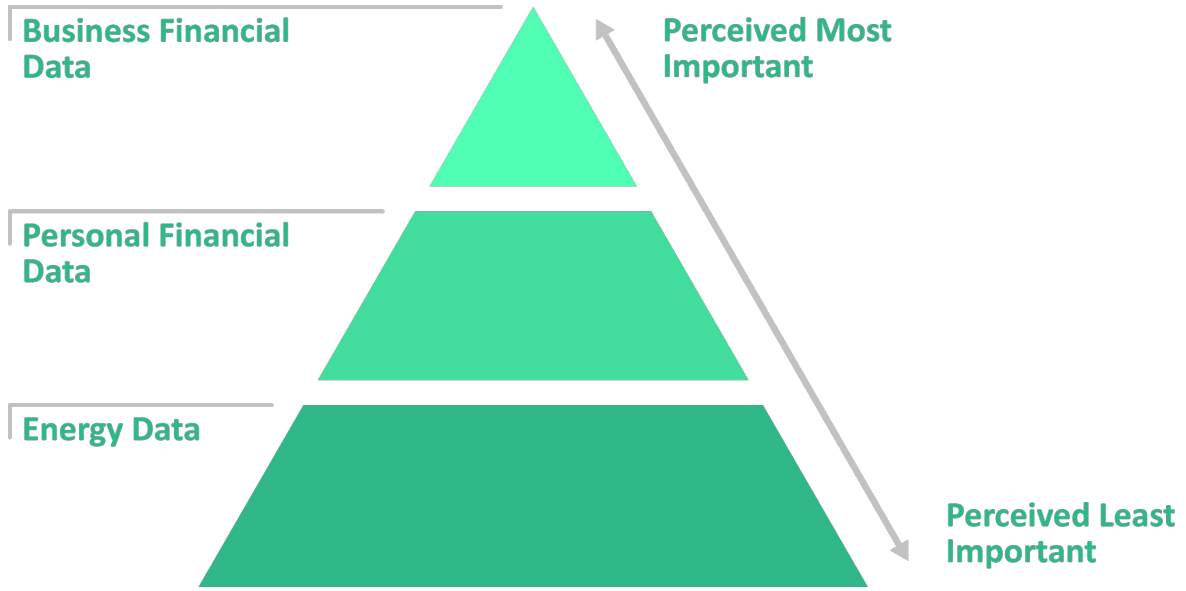
Hierarchy of willingness to share data

Although participants felt more confidence in sharing their personal data. For the business owners we spoke to, they felt their was more security risks in sharing their business data. They had fears of their data being breached or hacked. There was also a concern that they would be sharing their clients' financial data without their consent.

Participants, however, did not have as many privacy concerns over sharing their energy data. This is an early hypothesis that should be explored further in the CDR research for energy sector.

"For my business ones, it's not necessarily my information. It's my clients' transactional information as well as mine. So I feel like I'd be more reluctant to go sharing that information with third parties."

CDR Phase 2 | round 1 | Participant 6



Trust

Summary

When testing the authentication, the consumers have different trust levels with each organisation involved:

- Bank (data holder)
- App (data recipient)
- Government

When the trust is missing from one of these players, the participant is less willing to share their data.

Bank

The highest level of trust is with a consumer's bank. They provided action and assurance when there were "bad' bank experiences, like fraud or theft. The bank is accountable and is ultimately there to mitigate the damage.

App

Research and reputation was needed to build the trust in the app. Many pointed out without that, they would not see the value of sharing their data.

Government

Some of our participants had an adverse reaction to government being involved at all with the sharing of data. Some participants saw it as 1-to-1 relationship between app and the bank. Adding the government as an accreditor made them feel like an intermediary, which some found invasive.

A lack of trust was due to recent events, such as the ABC raids and My Health Record.

In addition, some participants who felt they had control over their data share, felt it could be over legislated - reducing their choice in the market, if they chose to use overseas products.

Trust

In the app (data recipient)

Consumers had apathy towards the apps, as it has no reputation. This is due to the app being a fictional app with no real reputation or history for the purpose of testing. People will have to build trust with the app before they decide to connect and share their bank data.

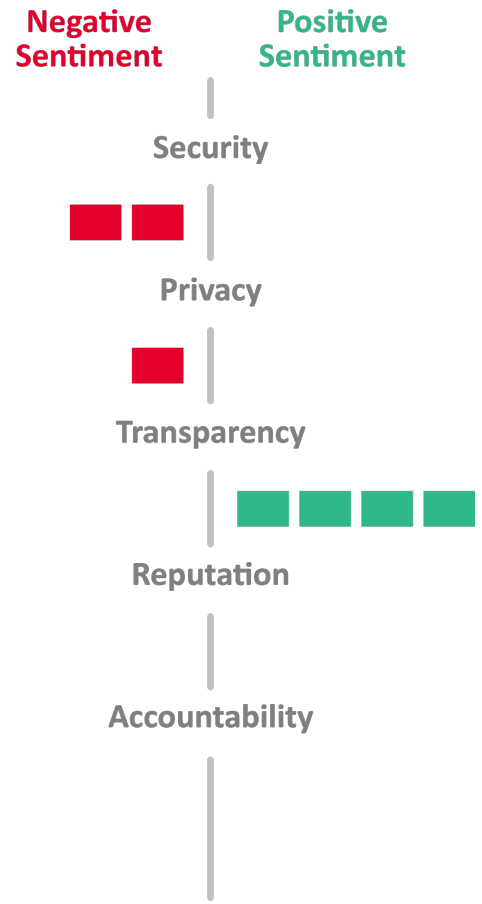
For the app to build trust it needs to utilise its relationship with government and the bank. Using the areas they are trusted for and building up its reputational trust.

Participants were not comfortable with putting sensitive information into the app such as passwords and customer IDs, particularly during redirection. Some stating that it could potentially lead to phishing scams.

Consumers acknowledged that the app was very transparent about exactly what and why it wanted to use the data. However, some met that with skepticism because of their own mental models around data and privacy.

"I'm really big on privacy, so anything that's importing all my financial data into an app, you don't know where else that data's going within that process"

CDR Phase 2 | round 2 | Participant 20



Recommendations

- Round of research with real use case, app and bank to see if attitudes and behaviour change.

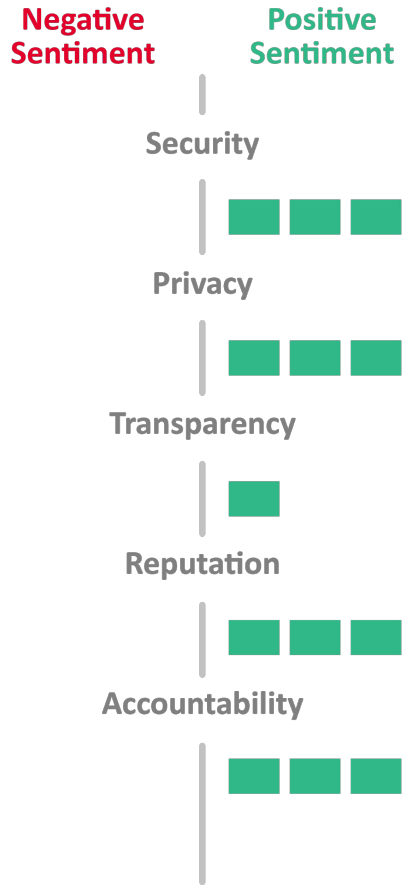
Trust

In the bank (data holder)

In both rounds of research, consumers trusted their banks with security and the privacy of their data being shared. With many holding them accountable for the data share and expected them to be available for any reversal of data sharing.

The privacy conscious trusted that the data share and personal details should be provided in the bank environment as they were more secure. They also had a known place to go/contact should anything go wrong.

For many, their bank had a good reputation and they'd used them in the past when there had been fraudulent activity on their account.



"(Talking about the experience of fraudulent activity on her bank account)...again the banks looked after me, and I wasn't out of pocket any money. So knowing there's quite a big force protection in there "

CDR Phase 2 | round 2 | Participant 16

Trust

In government

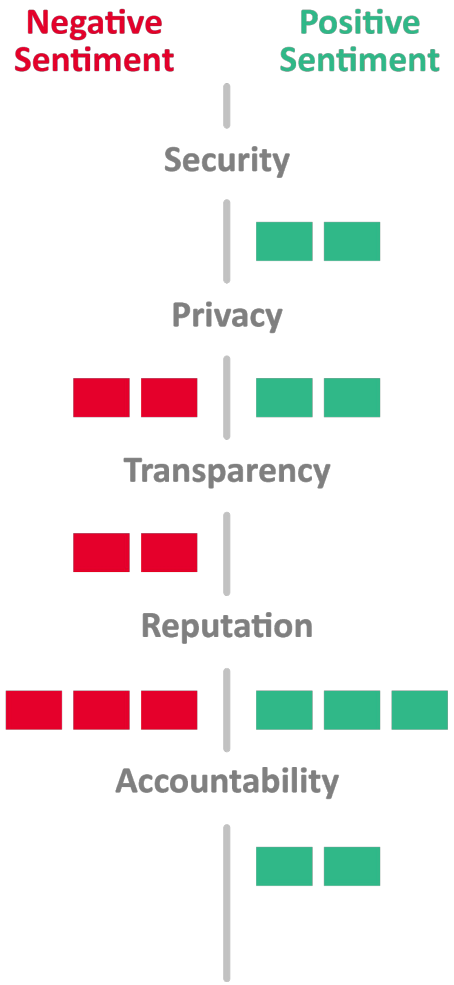
Trust in the government was polarising during the interviews, particularly when we showed further information around CDR (One pager) in Round 2. See design pattern (page 33)

Many found comfort in the government's involvement as an accreditor. It legitimised the transaction and made both parties accountable. Participants also found comfort in the revocation this provided.

However, more security/privacy conscious participants were cynical towards government and felt they couldn't be trusted.

They also assumed that by being an accreditor, it gave government access to the data. They could use this data for census-like purposes or socio economic reasons, which participants had privacy concerns over.

Government for some did not have a good reputation, with high profile breaches of trust and security. They mentioned the recent ABC's raids and My Health Record as examples.



"..Just having the power of the courts behind you, not so much the Australian government but more than the courts of if something does happen then you do lose financially, the fact that there's compensation available."

CDR Phase 2 | round 2 | Participant 17

"hang on, so something that I thought was for me actually isn't for me. It's for the government to use and access and offer research and statistics and whatever. "

CDR Phase 2 | round 2 | Participant 16

Value of individual privacy

Consumer attitude toward the value of their individual privacy varies greatly. Many value convenience over privacy, while the data literate look for privacy markers and facts for assurance.

"It's just the way things are"

As reported in other CX streams during Phase 2, many consumers have an apathetic attitude towards their privacy. They're conditioned to have this attitude and don't see a lot of choice in exchanging their data for services.

These users comprehend less. They have a tendency to skip over details, thinking they're available after and admitting they don't really read T&Cs.

They are willing to share their data in many instances but don't fully comprehend the consequences.

"I guess I feel a bit ignorant, therefore I feel quite safe."

CDR Phase 2 | round 2 | Participant 12

"You don't know where that data is going"

People who are highly privacy conscious are willing to sacrifice convenience. Privacy drives their decisions and behaviour. They're more conscious and read content more carefully. Privacy conscious participants had a higher comprehension success rate and a lower willingness to share.

They have trust issues with the app and with government, are more aware of media reported breaches, and have a higher data literacy.

Additional things they're looking for are:

- Reputation of the app they're using
- Trusted security processes
- Further transparency about
  - Where data is stored
  - How long it takes to process
  - Who has access to it in the organisation

"Once I've given something to someone, I don't feel it gets deleted. I feel like … because data is so simple to share. It's just copy and paste and stuff like that. So I feel like definitely I'd be kind of, "Why are they collecting all this data and all."

CDR Phase 2 | round 2 | Participant 15

Comprehension

Summary

As the Consumer Data Right (CDR) and the process of consenting to data sharing are unfamiliar to consumers, a high level of comprehension is necessary for adoption. To test comprehension, we got participants to complete the flow unaided and **recall** info.

Comprehension can be thought of in a 3 level hierarchy, with the most sophisticated being last:

Literal comprehension

What is actually stated. The facts of who, what, when, and where.

Interpretive comprehension

What is implied or meant, rather than what is actually stated.

Applied comprehension

Applying the concepts or ideas beyond the situation.

There's also Lexical comprehension - which is covered in language (page 30)

Using this framework, most participants were able to comprehend the literal facts that they completed but use interpretation to fill in the gaps from their applied knowledge.

Consumers use their existing mental models of data and apply it to their comprehension to interpret it when asked. This results in incorrect interpretations that will need to be changed over time.

Comprehension

Specifics

According to the Data Standards Body, a successful consumer experience will result in a clear way for consumers to understand the following. We tested for comprehension on each of these points.

Understand what they are consenting to and why their data is being requested.

All consumers understood that they had shared their data from the bank and their comprehension of that point was high. The specific data they had shared was varying - some able to replay specific examples, while others just said “bank transactions”.

Understand the scope and meaning of the data they are sharing, and how it will be used.

How the app needed that data was also understood to varying levels. Participants understood what the app was doing with the data by replaying the value prop setup at the beginning, not necessarily the detail that was featured underneath the data clusters.

Understand and trust who will have access to their data and the duration of that access

All consumers were able to identify that their bank (data holder) and app (data recipient) were using the shared data. There were assumptions and skepticism that it would only be those 2. They also believed other 3rd parties would be involved if they spent time reading the terms and conditions.

Duration also had varying levels of understanding, participants weren’t sure the exact dates it was from and to. They mixed history and collection period.

Understand how they can revoke and manage the sharing of their data

Participants understood that it was possible to back out of your data share but how to do that varied and used assumptions.

Understand the implications of revocation

The consequences of revoking were also not clear to participants, with most relying on their existing mental model.

Comprehension

Interpretative

Participants used their existing knowledge of data sharing to fill in the gaps of their comprehension after completing the task. Making assumptions about how their data would be treated.

Other third parties involved assumptions

People are conditioned to believe that data may still be sold or shared despite not seeing it in the flow. Many had assumptions that their data could still be given to a third party marketing agency, used by government for socioeconomic reasons or used by the app to make improvements. They'd expect to see where their data was being used in the terms and conditions, although current behaviour suggests they wouldn't look.

"I'm assuming that because they're accredited that the Australian Government reserves the right to pull that information when they require it."

CDR Phase 2 | round 2 | Participant 15

Data will be kept

There's an assumption that data will be kept after expiration or revocation. That the app will retain the data as you consented to this period and agreed to those terms.

Will the app work?

There's an assumption that if data sharing is revoked or expires that the app will stop working or will not be useful without automatic data.

"It would have been fed into the app, and at that time they had your authority to get that information, so I feel like that's theirs to do with whatever. And then they can't take any more data from you."

CDR Phase 2 | round 2 | Participant 15

Comprehension

Language

During both rounds of testing there were several terms and phrases that participants did not fully comprehend.

“De-identify”

Not a common term that consumers can easily understand. The process behind this was not clear. There was further confusion as it was used as alternatives to delete.

“Revoke”

A plain language phrase like “stop sharing” could replace this, as it was not always clear what revoke meant.

“Dashboard”

People weren’t always sure what this meant, and it lead to ideas of centralisation.

“Collect and use”

The “use” in this was met with questions: “use how?” It didn’t seem specific enough in some instances to explain what use meant.

“I think that it's so important that the right languages there of when people are not feeling comfortable.”

CDR Phase 2 | round 2 | Participant 17

“Duration”

The time span this covered was not clear during the first round of testing. It was changed in the second round to be clearer.

Data clusters

The understanding of what’s under each data cluster varies from person to person. There were perceived overlaps between the data clusters and the permission language underneath.

Recommendations

- All content should be written to readability score of Year 7. The lower the readability score, the easier your text is to understand. This helps people with lower literacy or English as a second language. It also meets WCAG 2.1 accessibility requirements.

Choice

Data clusters

Choice is an important need identified in both rounds of research. The purpose of the app and the participants situation is used to inform that choice.

Data choice is relevant to the features/product that consumers are using.

Choice at data cluster level

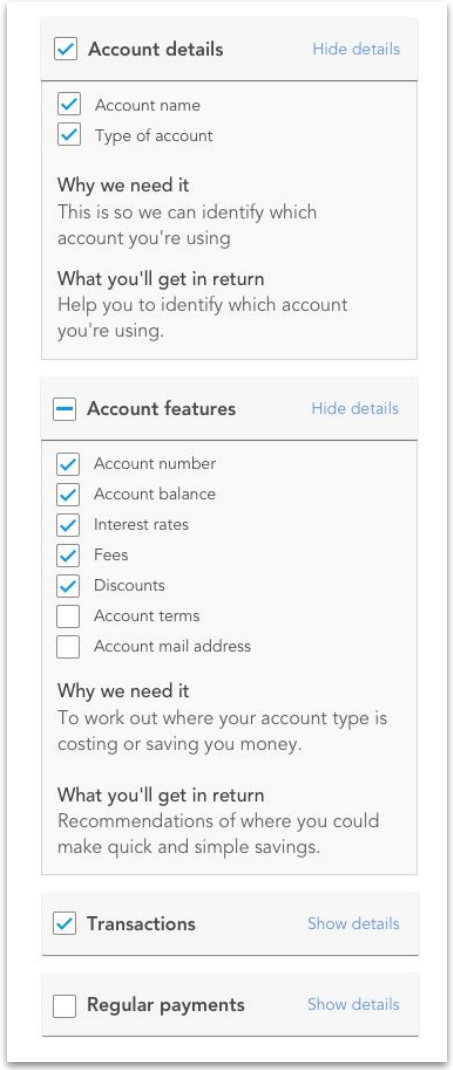
Many participants felt that it was unnecessary to share contact details for a budgeting app. They couldn't see the purpose of sharing that level of data and led to skepticism about what the app would be using the data for.

Choice at permission language

There were several instances of data clusters having permission language that participants would not want to share.

One participant said that she would provide a fake address if she was asked to provide it to use the tool. Others did not want to share "business address" and found "charity status" irrelevant about their company.

Some were also conscious of sharing transactions about sensitive financial information.



Possible idea for allowing consumer to choose which data they would like to share.

Choice

Time (i.e consent duration)

The choice of ‘consent duration’ is context specific. For example, consumers wanted it to be longer if they were budgeting for a large value item, such as a house. They didn’t want to reauthorise in such a short time frame.

In a similar fashion, there was a trend towards those that wanted a ‘trial’ period for the data share, to see if they liked it. They would then opt to revoke or continue on a much longer time.

Choice was wanted at both consent and reauthorise.

“I would be more comfortable with a larger timeframe because I know that, as life changes, we've gone from one to child to two children to three children, so our spending habits have completing changed. Everything keeps evolving”

CDR Phase 2 | round 1 | Participant 9

Design patterns

CONSUMER
DATA
STANDARDS

Design patterns

Summary

9 prototypes were developed for the Authenticate, Notify and Reauthorise aspects of the Consent Model:

1. 3x Authenticate in the Flow:
    a. Redirect to Known authentication flow (round 1 and 2)
    b. Decoupled authentication flow (round 1)
    c. Authentication with One Time Password (OTP) flow (round 2)

2. 1x 90 days notification (round 1)

3. 4x Reauthorisation flow
    a. 1x reauthorisation flow in the data recipient app (round 1)
    b. 1x reauthorisation flow in the data holder app (round 1)
    c. 1x simplified reauthorisation flow from the data recipient to the data holder (round 2)
    d. 1x simplified reauthorisation flow with consent confirmation at the data holder (round 2)

4. 1x CDR information page from ACCC (round 2)

The prototypes were focused on the consumers and reflect the proposed use case of **'Managing my finances'** through a **Budget Guide app** (as the data recipient). The scenario set up for the purpose of the research was for the consumer to **share data from their bank (data holder) to the Budget Guide app (the data recipient)**.

Each prototype included language and data clusters specific to the use case as approved by the stakeholders.

The prototypes were reviewed by ACCC, OAIC, Treasury and Data61 to gain consensus before they were tested and to shape the direction of the research.

The key findings from the tested prototypes can be found on the following pages.

Design patterns

Summary

Authentication flow

The authentication option 3 - **Authentication with One Time Password (OTP) is recommended** as the most preferred option. It presented the lowest level of unnecessary frictions and potential drop-out compared to the other two flows.

90 days notification

The 90 days notification is deemed unnecessary by consumers. The message is unexpected and will most likely be ignored.

Reauthorisation flow

Simplified reauthorisation flow from the data recipient to the data holder is recommended for the reauthorisation flow. It has the right balance for the convenience vs security conscious consumers.

More key findings can be found on the following pages.

Pre-consent

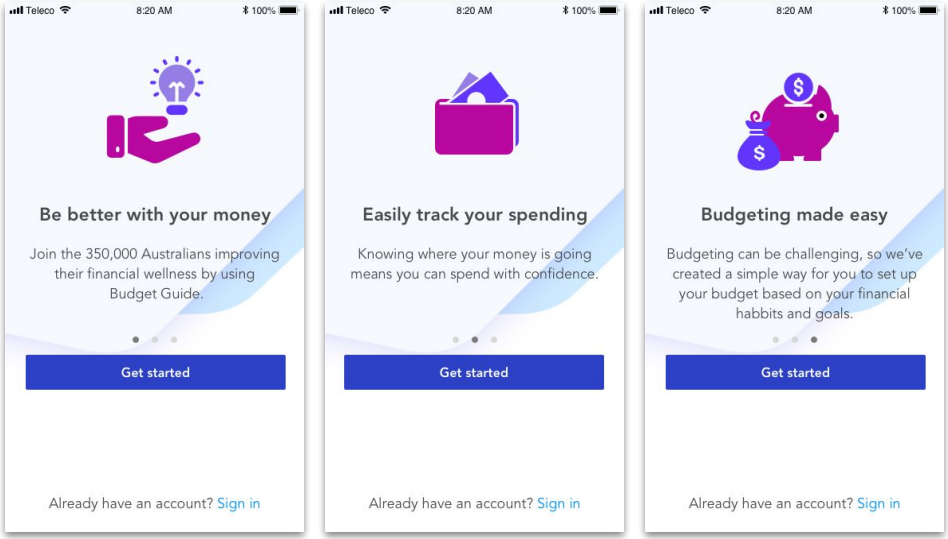
Data recipient onboarding

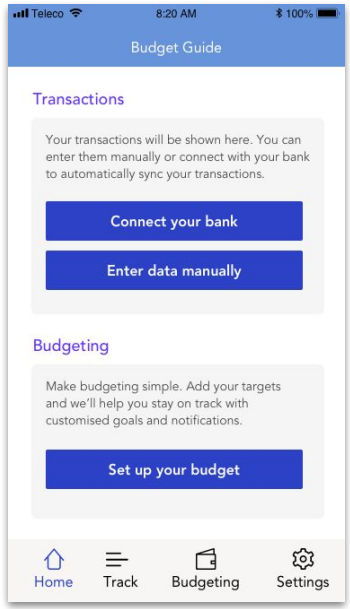
Clearly articulate the data recipient value proposition

Data recipient should clearly articulate their product value proposition to set the context of the product.

Following the recommendation from the round 1 research, we introduced the data recipient (i.e. the Budget Guide app) set up and onboarding steps (e.g. sign-up process) prior introducing the concept of data sharing. This helps consumers to comprehend the concept of data sharing and why it was needed for the data recipient.

In this scenario, the consumer is sharing data by connecting to their bank to automatically sync their transactions for the Budget Guide app.





Pre-consent

Data recipient - share data value proposition

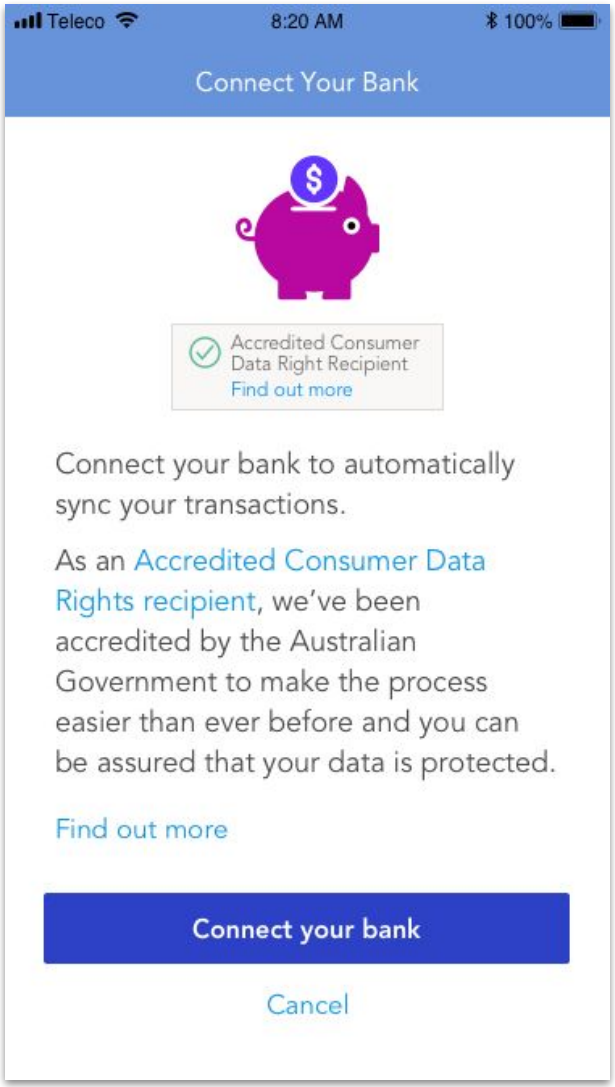
Clearly articulate the sharing data value proposition

Data recipients should clearly explain the value added by sharing data to increase the chances of consumer adoption. Introducing the concept of data sharing without a clear value proposition will not be conducive to adoption.

‘Accredited Consumer Data Rights Recipient’ trust mark is assuring

Participants felt comfortable and assured by the trust mark. It implies that the app has gone through a legitimate and rigorous process for being accredited.

Some participants will do their own research to find out more about the Consumer Data Rights to ensure that it is a legitimate process. The more privacy conscious participants clicked on “find out more” unprompted during the test, the insights for this can be found on the One pager (page 65).



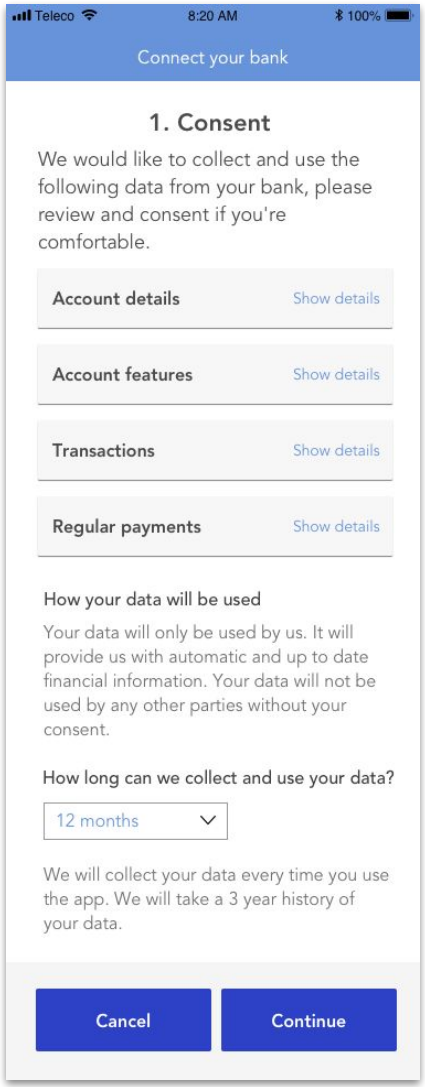
Consent

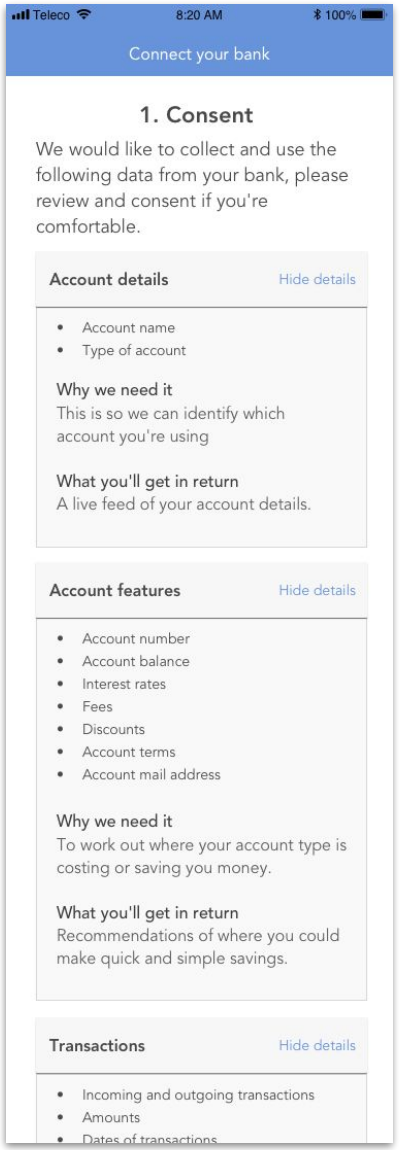
Data cluster consent

Provide clear purpose and only ask for relevant data

Data recipients should clearly explain the purpose of the data being shared. They should be relevant to the features/product that consumers are using.

From the research, it was clear that participants did not want to share personal data (e.g contact details or mailing address) as they see no relevance for the purpose of a budgeting app.





Recommendations

- Follow the data minimisation principle to only ask for what is required for the services of the data recipient. Make clear purpose and benefits to the consumer.
- Avoid asking sensitive information such as personal details, contact details, mailing address.

Consent

Consent duration

Duration relates to purpose

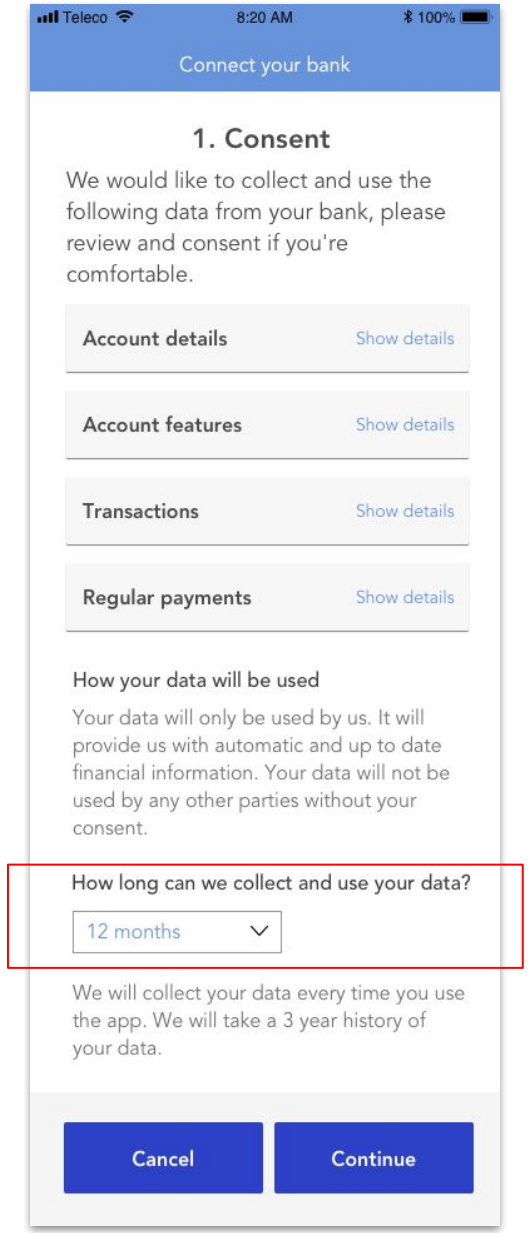
The length of time participants were willing to share depends on the purpose of the app.

Having the ability to choose the duration of consent is ideal. However participants were comfortable with the 12 months period, knowing that they can revoke the consent at anytime.

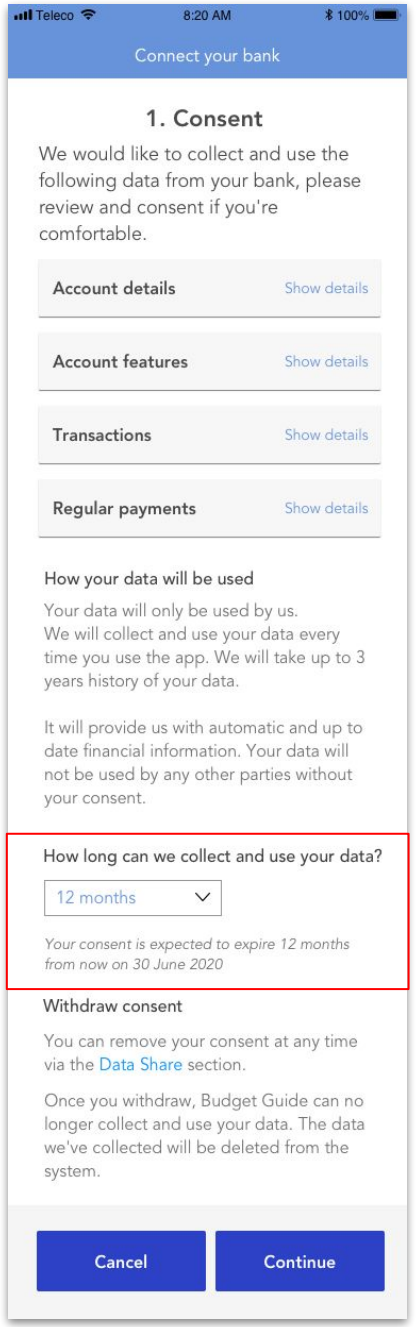
Some participants indicated that given the option, they would choose a longer period so they don't have to re-consent again or a shorter period if they just wanted to try the app.

Recommendations

- Consider the consent duration to align with the life of the product. For example if it's a paid subscription product which has a 30 days trial offer, the consent period will last for 30 days until they resubscribed.
- Add the expiry date to this page, aligned with the chosen duration.



Tested



Recommendation

Consent

Taking history of data

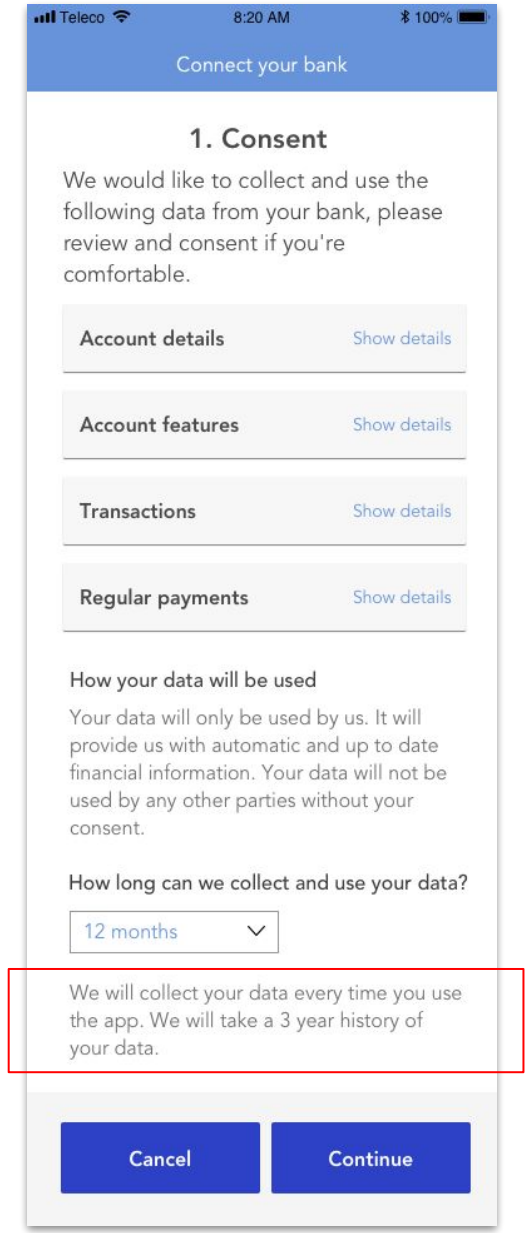
Provide a clear purpose of accessing the data history

Similarly to the data cluster consent, participants need to understand the purpose of sharing their data history.

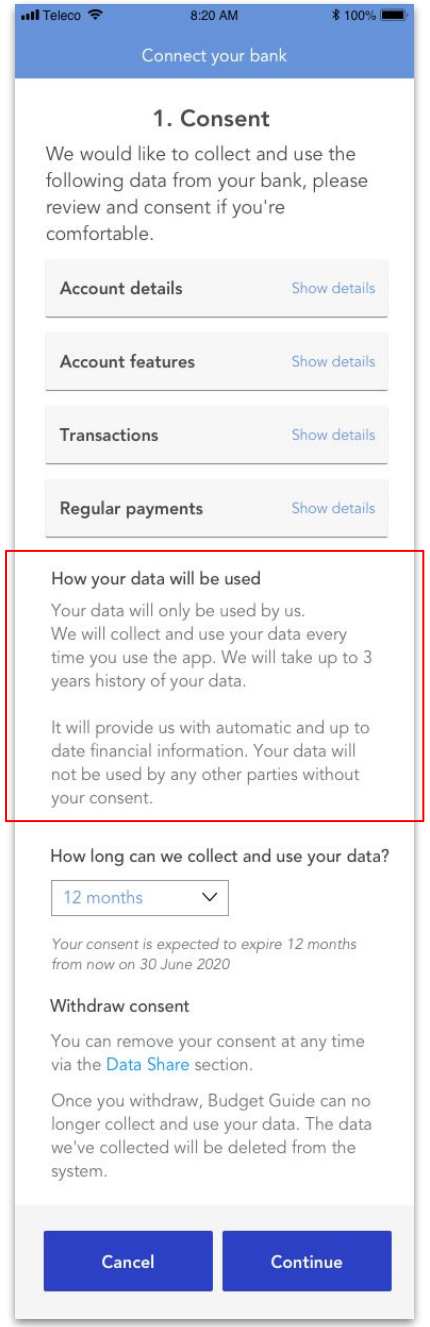
During the research, the purpose of this was unclear and it was confused with the consent durations.

Recommendations

- Allow consumer to define the duration of accessing the data history that suits them.



Tested



Recommendation

Consent

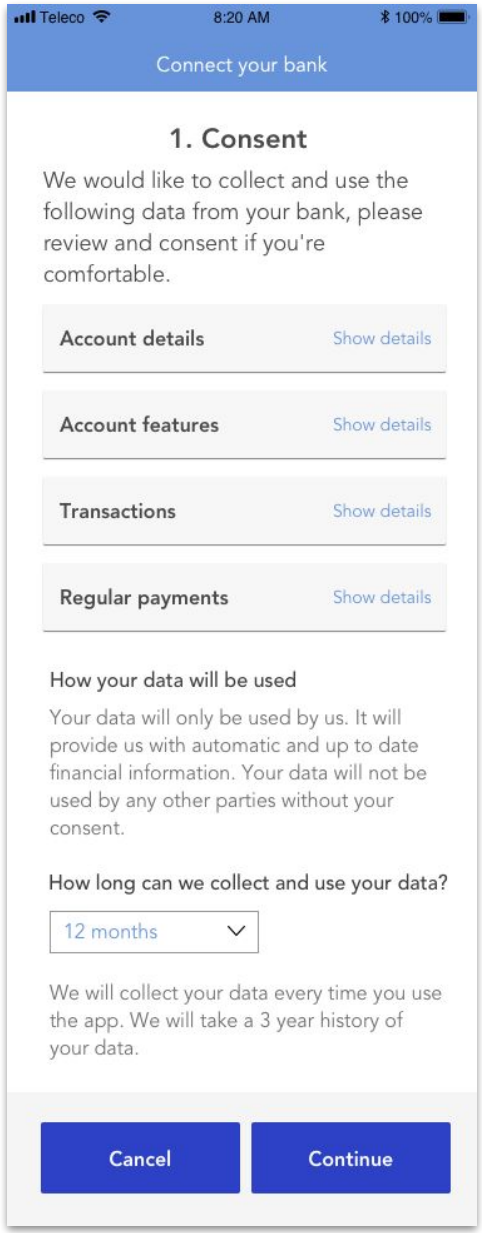
Revoking consent and its consequences

Missing the ‘revoke’ ability and its consequences

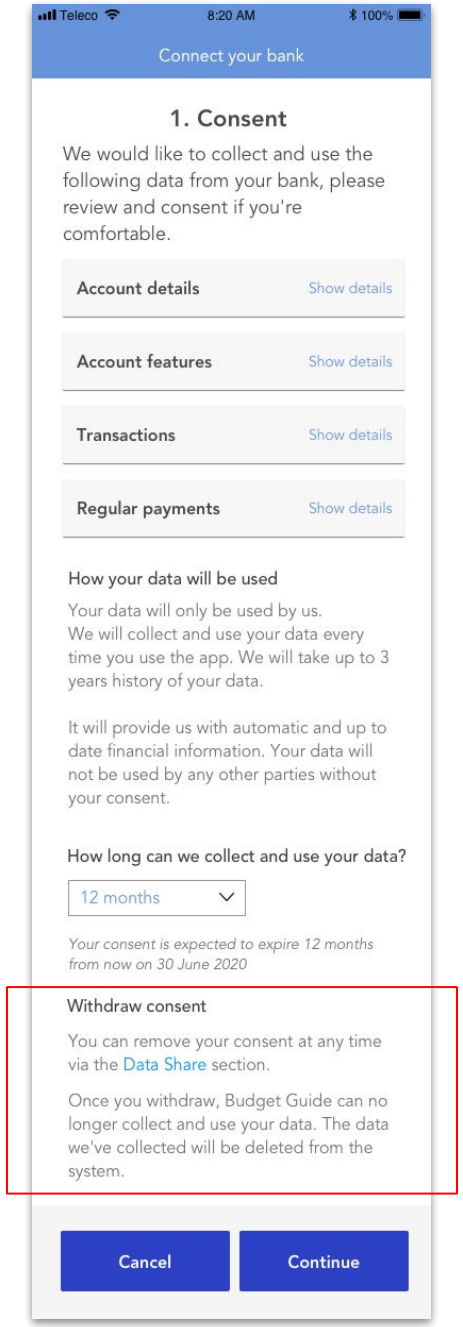
The information of the ability to revoke at any time was missing from this page. This affected participant’s comprehension of ‘revoking’ and the consequences. Many participants were not able to confidently articulate the consequences when they stop sharing their data.

Recommendations

- Add the information on the ability to revoke at any time and clearly explain the consequences of what happens to their data when they stop sharing.



Tested



Recommendation

Authentication

Three versions of authentication flows prototypes were developed and tested in round 1 and round 2:

1. Redirect to Known authentication flow (round 1 and 2)
2. Decoupled authentication flow (round 1)
3. Authentication with One Time Password (OTP) flow (round 2)

The authentication flow research was focused on answering the following key questions:

- Were authentication flows successful? How were they received?
- What is the preference for their use, and
- What level of friction is required and expected?

There was a lot confusion for the 'Redirect to Known' authentication flow in round 1. We felt that it was necessary for the design to be iterated and tested again in round 2.

We believed there was enough insight for the 'Decoupled authentication flow' that no further research was required.

Each flow has presented their own challenges with potential drop-outs, task completion and levels of friction.

The authentication option 3 - **Authentication with One Time Password (OTP) is recommended** to be the most preferred option. It presented the lowest level of unnecessary frictions and potential drop-out compared to the other two flows.

The key findings from the tested prototypes can be found on the following pages.

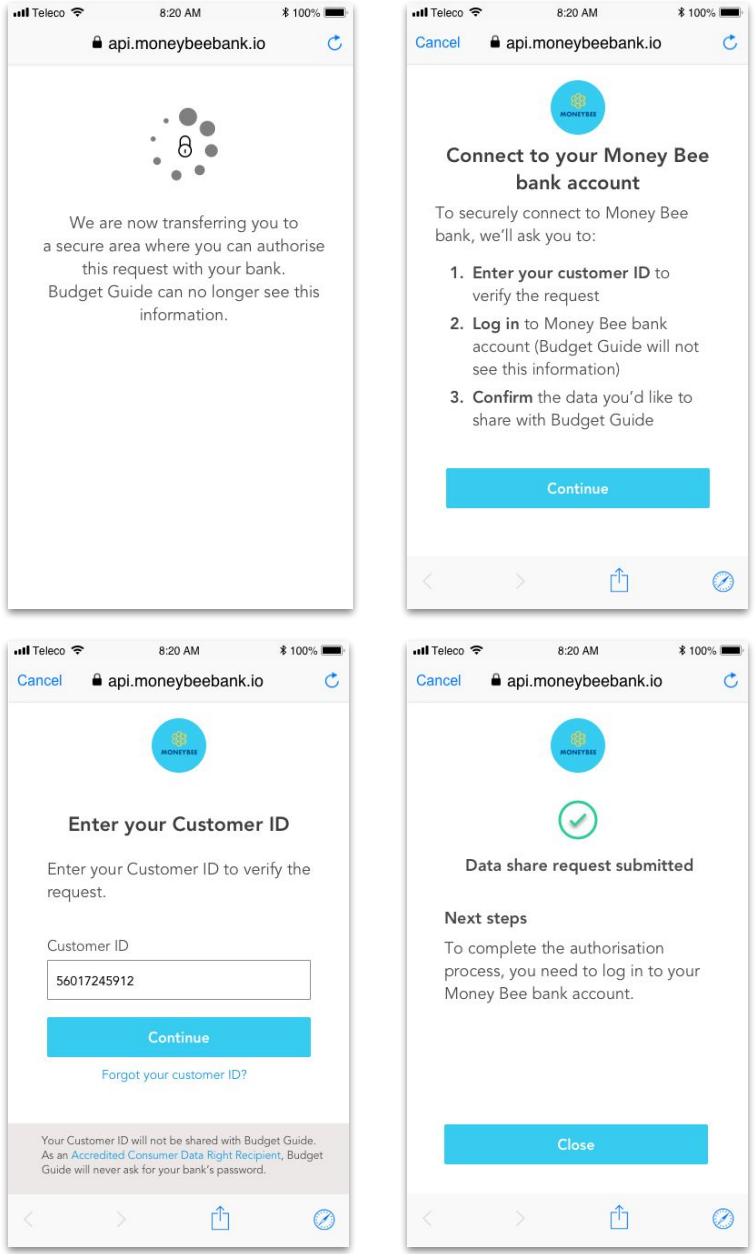
Authentication - option 1

Redirect to Known authentication flow

After following the consent process, to authenticate using the **Redirect to Known authentication flow**, the following steps are required:

1. Consumer is redirected to the data holder space from the data recipient app;
2. Consumer is required to enter their customer ID (of their bank) in the data holder space (specifically built for CDR);
3. Once the customer ID is recognised, the consumer is then asked to manually log in to the data holder environment (i.e. their bank online banking) to complete the authorisation steps.

Prototype: https://invis.io/JMS7MGL2APQ



Authentication - option 1

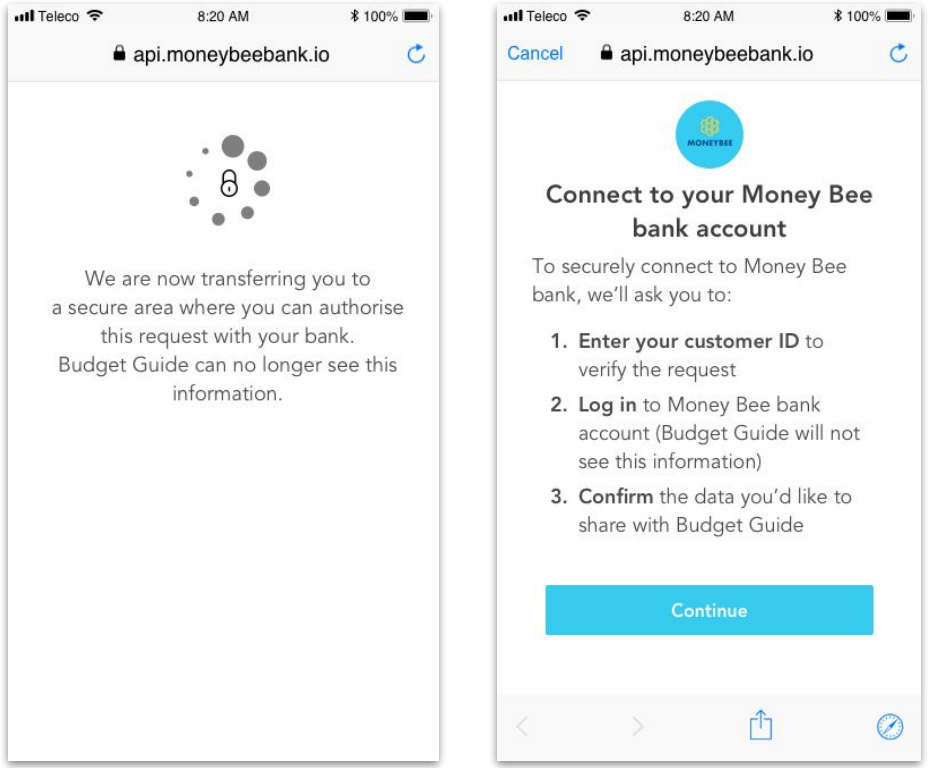
Redirect to Known authentication flow

Using appropriate security indicator provides trust

Have a visual indicator which is associated with being in a ‘secure’ environment. Use an appropriate language to assure consumers are in a secure environment, this alleviates some of the security and trust concerns raised in round 1 research.

Instructions page helps with the task comprehension

The added instruction page explains the process and the steps that the consumer needs to take in order to complete the task. On observations, this helped with addressing some of the confusions raised in round 1 research.



Recommendations

- Clearly communicate and guide the consumer through the process as this would be a new process that the consumer has never experience before.

Authentication - option 1

Redirect to Known authentication flow

Customer ID is associated with login

While it was less prevalent in round 2, there was still a friction with participants entering their customer ID. They expected to enter a password following their customer ID. They associated their customer ID with logging in to their online banking.

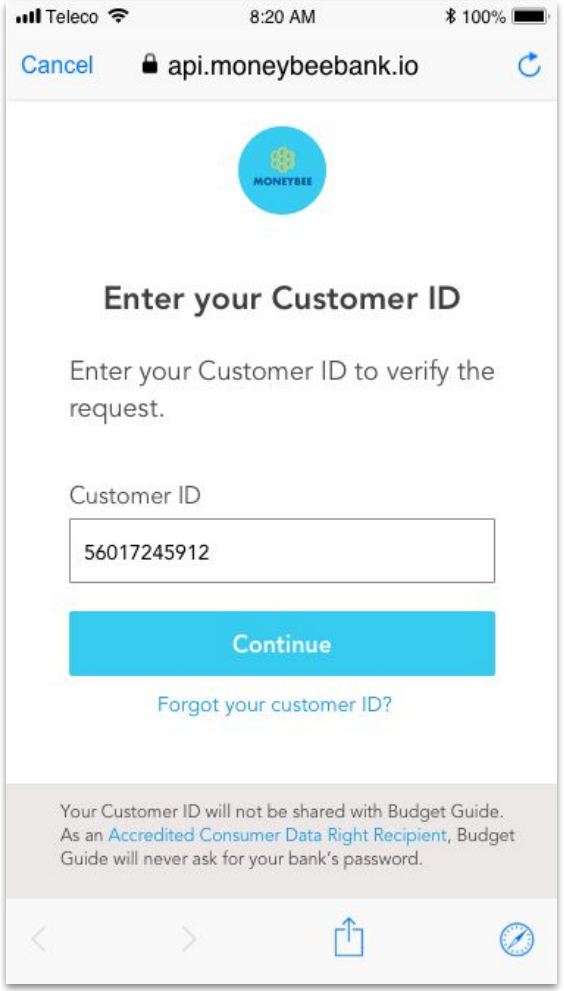
Unfamiliar steps risk abandonment

The process was seen as unfamiliar. This led to the feeling of distrust in the process and risk of abandonment.

Some participants felt that it wasn't secure as anyone with the knowledge of their customer ID will be able to set up a data share request.

"...someone could go on and pretend to be me, and suddenly access all my banking details."

CDR Phase 2 | round 2 | Participant 16

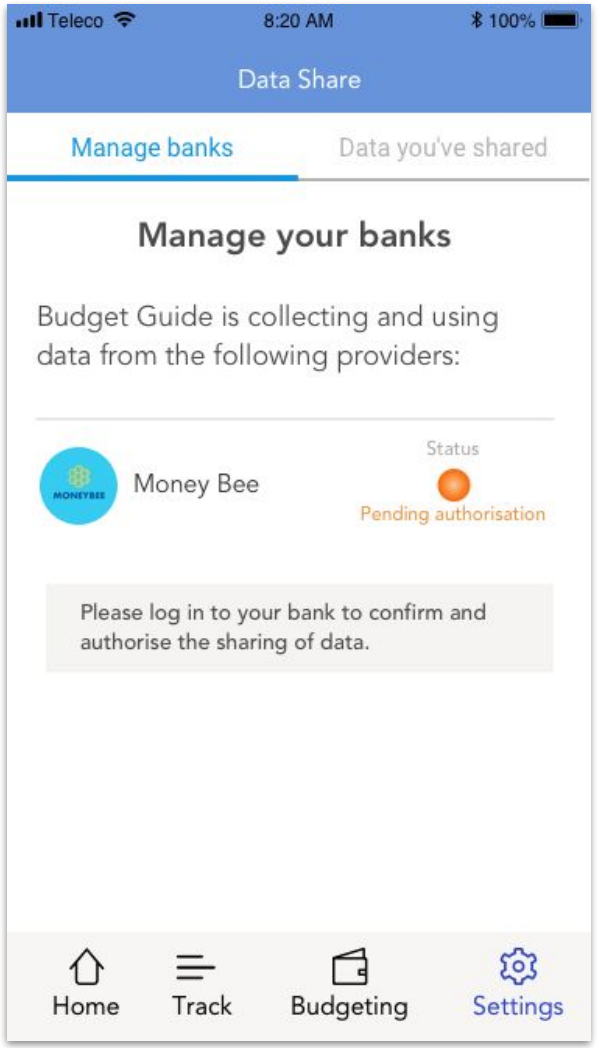


Authentication - option 1

Redirect to Known authentication flow

Provide clear separation between the app and the bank

Redirecting consumers back to the app dashboard with the status changed to ‘Pending authorisation’ helped eliminate the confusion from round 1. This helped clarify whether or not they had logged into their online banking app.



Recommendations

- Redirect consumer back to the data recipient space with a clear the status change
- Provide clear instructions to consumer for them to follow to complete the authorisation process.

Authentication - option 1

Redirect to Known authentication flow

Perceived security by manually logging in to the bank

Three (of ten) participants preferred the ‘Redirect to Known’ authentication flow. They perceived manually logging into the bank to authorise to be more secure. They were concerned that the redirection might not be secure.

They also felt that they had more control by logging into the bank separately.

“I prefer the one where I had log out and go into my bank. They’re (refer to OTP flow) redirecting me to a different website, it could be a fake website.”

CDR Phase 2 | round 2 | Participant 15

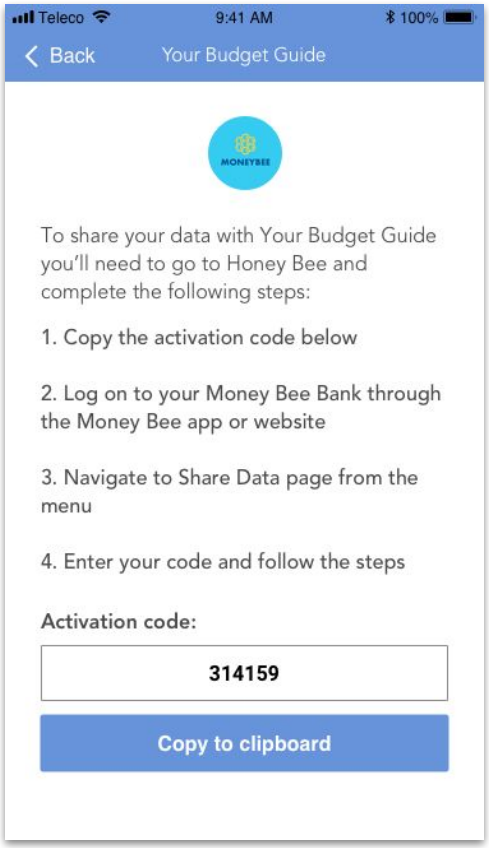
Authentication - option 2

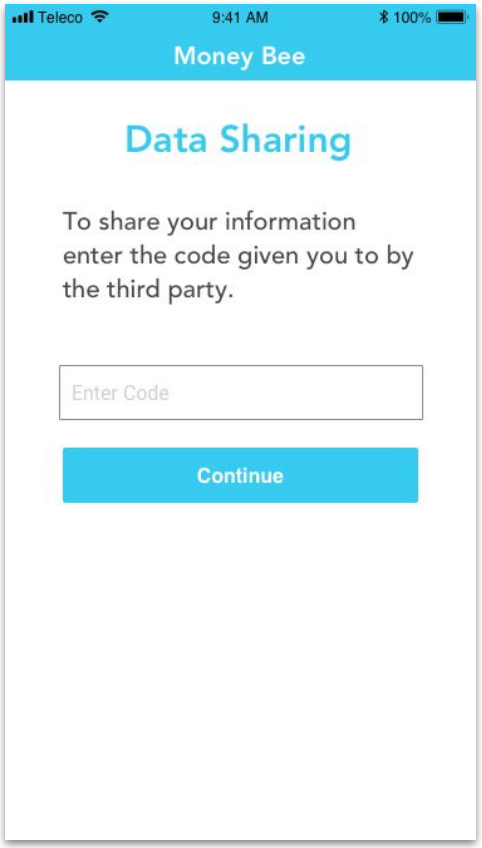
Decoupled flow

After following the consent process, to authenticate using the **Decoupled authentication flow**, the following steps are required:

1. Consumer is given an instruction and an **authentication code** which they need to copy;
2. Consumer is then required to manually log in to the data holder (i.e. their bank);
3. Consumer navigates to the page where they can enter the authentication code;
4. Consumer enters the copied authentication code to complete the reauthorisation.

Round 1 prototype: https://invis.io/5FRWJ7PJ829





Authentication - option 2

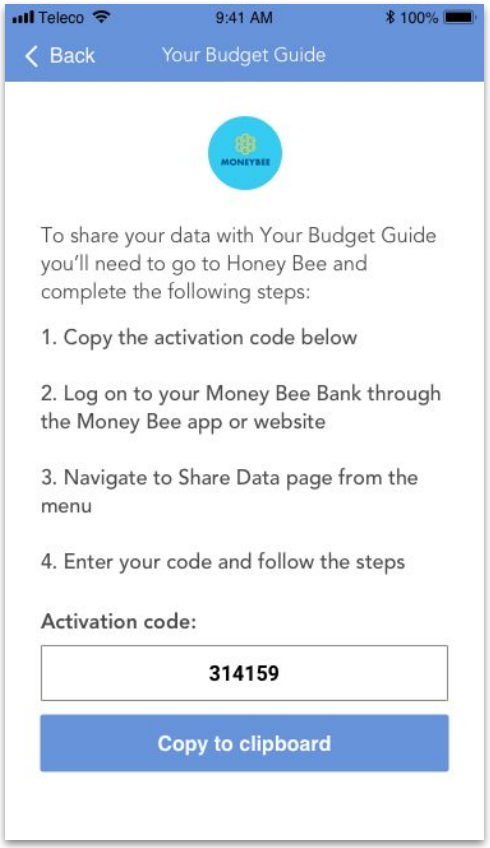
Decoupled flow

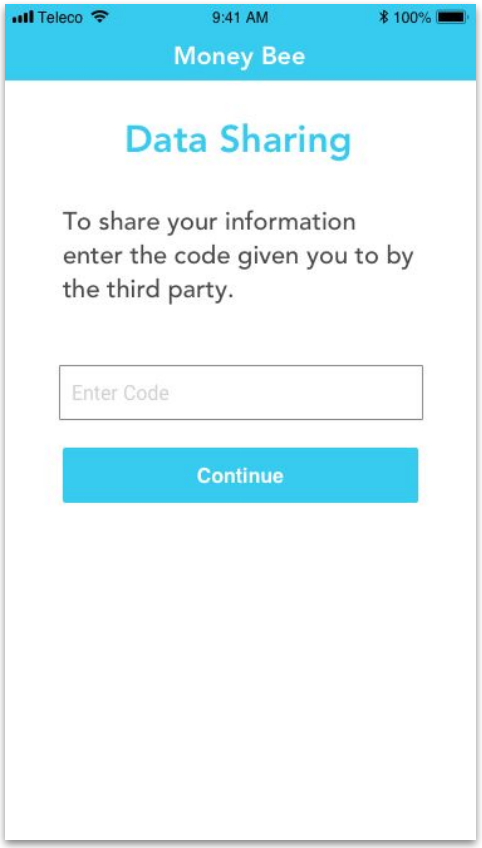
Clear separation from the app perceived as more secure

The decoupled flow provides a clear separation between the app and the bank (compared to the 'redirect to known' flow in round 1). Going to the bank to authorise the data share was perceived as more secure and legitimate.

Feels a familiar process

Receiving codes and entering them felt like a familiar behaviour and process. Consumers were used to entering codes for 2-factor authentication, so it had perceived legitimacy and trust.





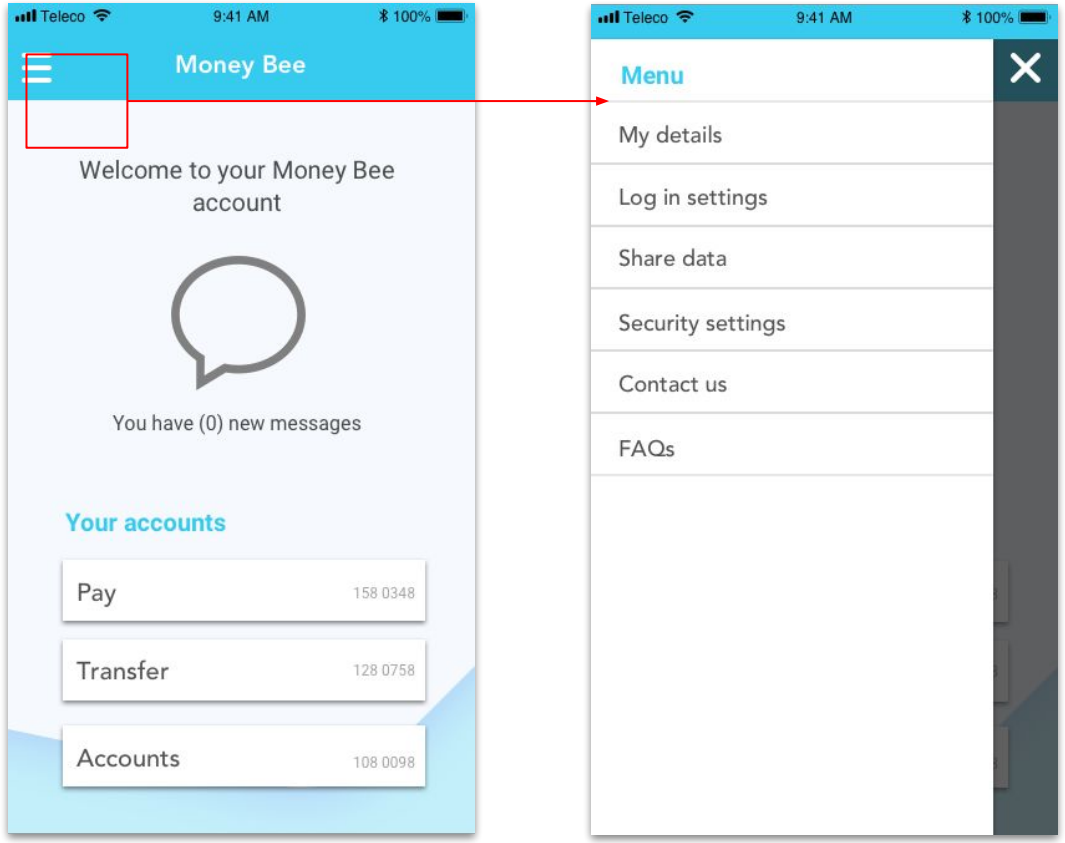
Authentication - option 2

Decoupled flow

Potential navigation issue risks abandonment

The need to navigate to the right page in the data holder (i.e. bank) to enter the authentication code presented a potential friction and drop out point.

Participants who were familiar with mobile apps, were able to locate the data share area in the bank app through the burger menu. They were looking for the data share to be under ‘settings’ menu. However, some participants struggled to navigate to the page. They didn’t know what to look for in the bank app. They had to be prompted to find what they were asked to look for.



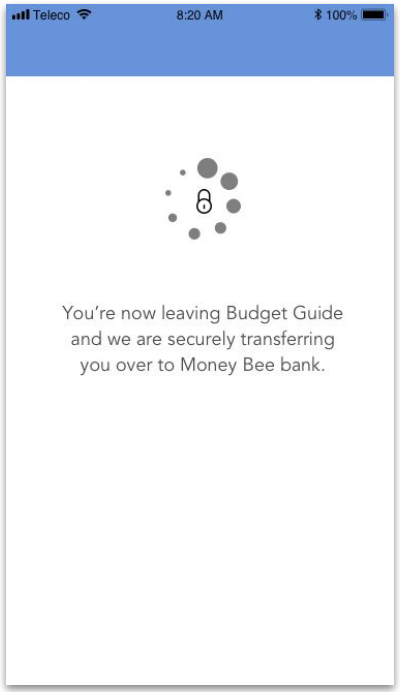
Authentication - option 3

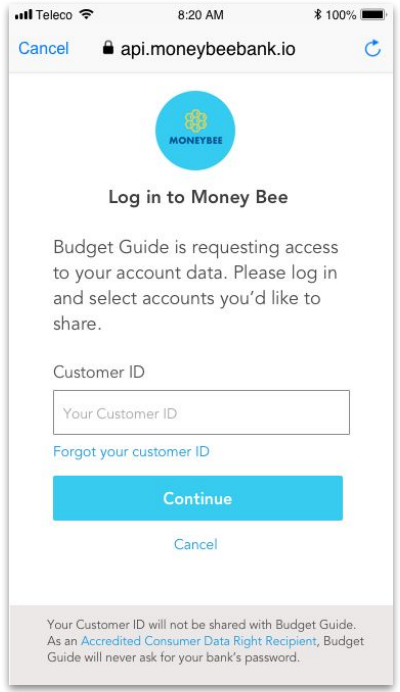
One Time Password

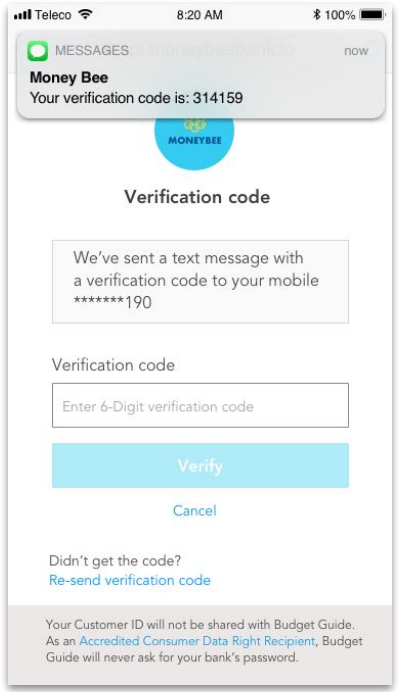
After following the consent process, to authenticate using the **One Time Password (OTP)**, the following steps are required:

1. The consumer is securely redirected to the data holder space from the data recipient app;
2. Consumer authenticates with their customer ID and a one time password delivered by SMS (or email).

Prototype: https://invis.io/NUS7LISFAR6







Authentication - option 3

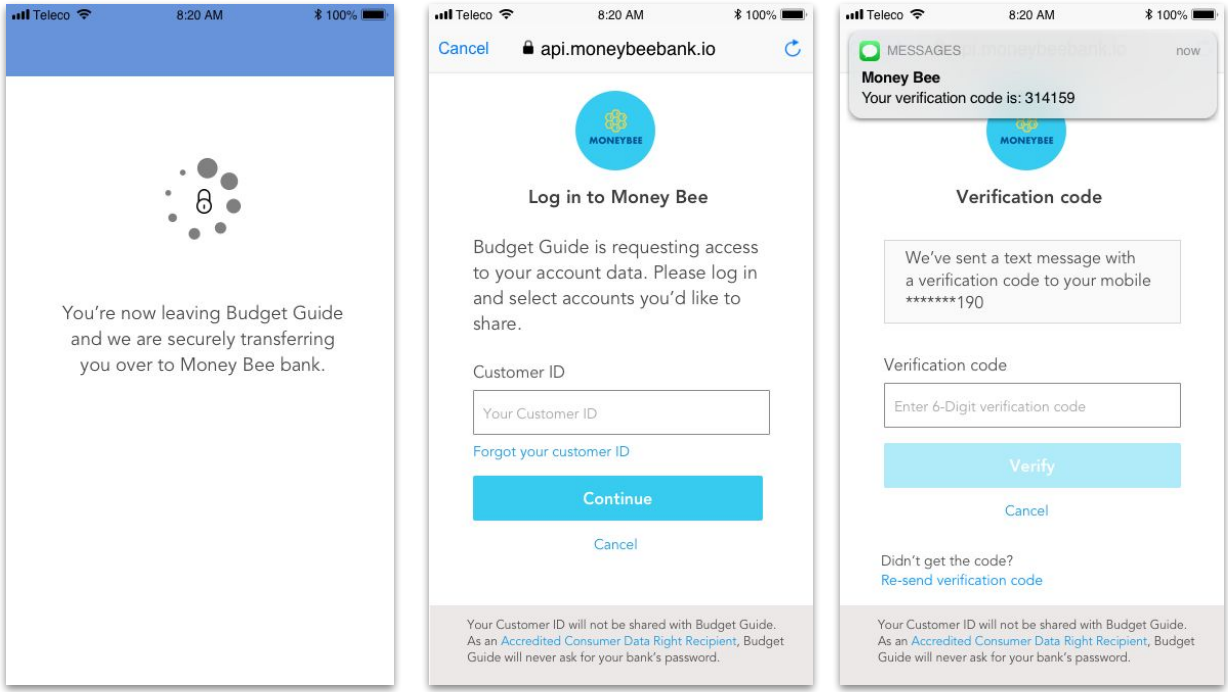
One Time Password (OTP) flow

Smoother and seamless is preferred

While most participants didn't notice major differences between the 'Redirect to known' flow and the 'OTP flow', six participants (of ten) preferred the authentication with OTP option when prompted.

The OTP flow was perceived to be more seamless and smoother. It felt quicker and easier. They did not have to close the data recipient app and open the banking app to manually authorise data share.

Some participants were used to receiving verification codes from their bank as an extra layer of security measure (i.e. 2-Factor authentication). Hence, using the verification code here provided a sense of security for them.



"Having it switch automatically to the bank. this feels a lot smoother"

CDR Phase 2 | round 2 | Participant 17

"Log in to the bank inside the app and with verification code as well. Feels more secure"

CDR Phase 2 | round 2 | Participant 12

Authentication - option 3

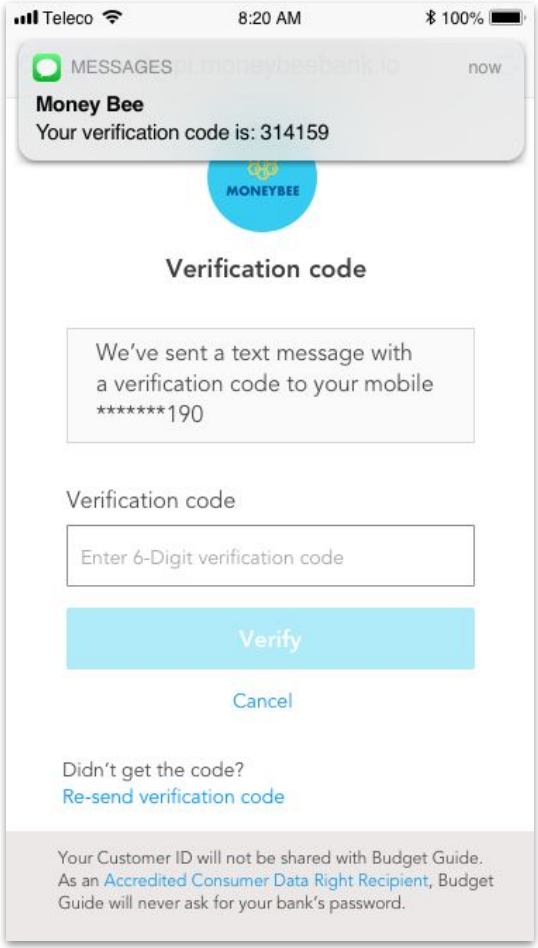
One Time Password (OTP) flow

Differentiate between One Time Password and verification code

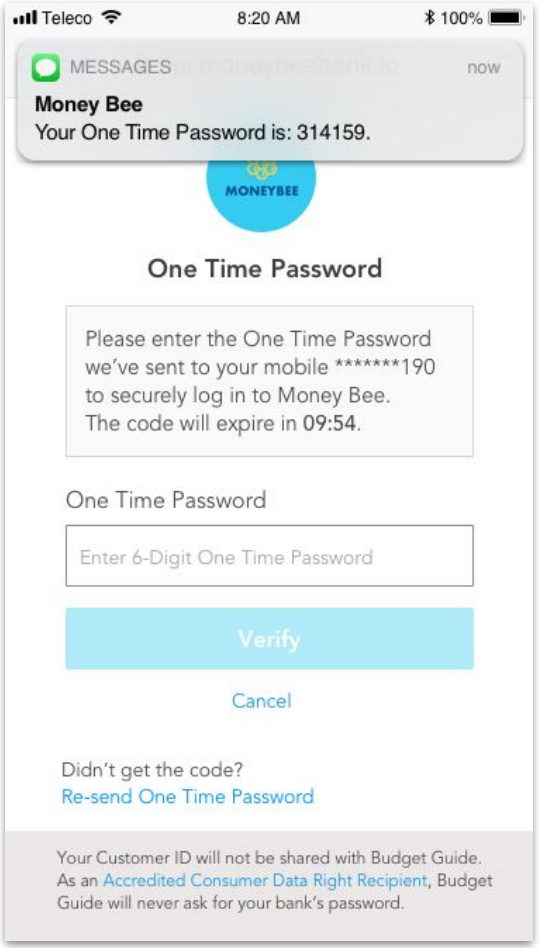
Some participants expected to enter the password following the customer ID. The differentiation between 'One Time Password' and 'verification code' isn't clear in the prototype. They are used to entering verification as a 2-factor authentication method but not as a password replacement.

Recommendations

- Adjust the copy to clearly explain the use of verification code as a one time password.
- Apply a time limit to the code for additional security measure.
- The code should also be delivered by other methods such as email as alternative to SMS via mobile number.



Tested



Recommendation

- *Clearer message for OTP*
- *Display the time countdown (mm:ss)*

Authentication - option 3

One Time Password (OTP) flow

‘Redirection’ was seen as redirection to a 3rd party intermediary

Some participants correlated ‘redirected’ to being redirected to a 3rd party as the intermediary service to securely connect the app to the bank.

While this wasn’t causing any issues or concerns of drop out, it might be something to watch out for.

Recommendations

- Clearly explain the redirection steps to the data holder space.
- Use appropriate branding for the data holder space for brand recognition and trust.

90 days notification

As per ACCC rules, consumer will be given a notification every 90 days after they have consented.

The notification includes the following information:

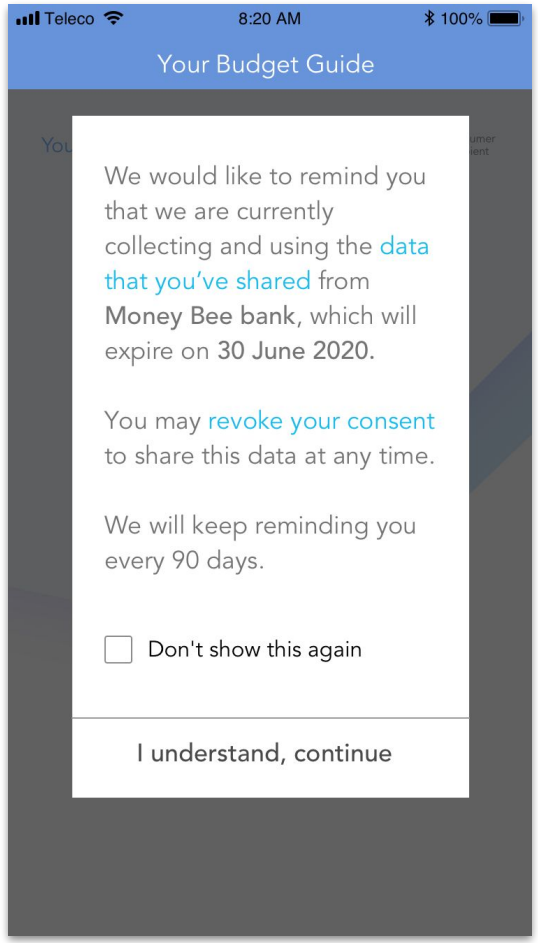
- The frequency of data sharing
- When the expiry of agreement will happen and possibility to extending data sharing agreement (reauthorisation)
- How to revoke consent if consumer chooses to do so
- Ability to opt out of receiving notification via the dashboard on app/website

The research was focused on answering the following key questions:

- What are their expectations in being reminded of their data share agreement?
- Did the participants find the notification useful?
- Do they feel the frequency of notifications are appropriate?

For the purpose of the research, the notification was communicated to the consumer in the form of a pop-up notification on the data recipient dashboard.

Round 1 prototype: https://invis.io/5FRWJ7PJ829



90 days notification

Pop-up notification on the data recipient dashboard

Message is unexpected

For most users the 90 day notification was unexpected and felt like an update rather than a purposeful message. As the consumers were told that they were actively using the app, they felt that it was an unnecessary message if they were presumably finding utility.

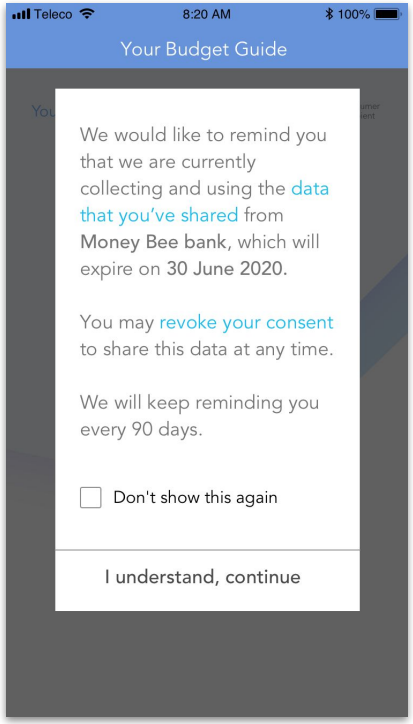
Some people assumed that the message was required to be sent in order to be accredited.

Message ignored

Most users dismissed the message and didn't see much use. They chose to not see it again. While 2 users did say they would find it useful, they likened it to software updates and a reiteration that they could revoke at any time.

Misunderstanding that consent was renewed

2 users misinterpreted the message and thought that clicking on "I understand, continue" that they had renewed their consent again.



Recommendations

- Consider changing the rules to only send the notification for consumers who have not used the service/product after 90 days.
- The notification should be an opt-in choice. Consider whether consumers would like to be notified.
- The notification should be less intrusive than a pop-up message on the app dashboard. It might be delivered by email or a simple push notification.

Reauthorisation

Four versions of reauthorisation flows prototypes were developed and tested in round 1 and round 2:

1. 1x reauthorisation flow in the data recipient app (round 1)
2. 1x reauthorisation flow in the data holder app (round 1)
3. 1x simplified reauthorisation flow from the data recipient to the data holder (round 2)
4. 1x simplified reauthorisation flow with consent confirmation at the data holder (round 2)

Round 2 research focused a reauthorisation flow which was not tested in round 1 - **simplified reauthorisation flow from data recipient to data holder.**

We hypothesised that customers will find the above flow to be too long for users to complete reauthorisation. Hence, we introduced a variation to the simplified reauthorisation flow (i.e. flow no.4) for the purpose of answering the key questions of:

- How is the reauthorisation flow received?
- Did participants feel comfortable with the proposed reauthorise flow?
- Did participants feel that the proposed reauthorisation flow (flow no.3) too long for the purpose of reauthorisation?
- Were there any frictions to reauthorisation?
- What level of details is appropriate for reauthorisation?

To simplify the flow for research purposes, the **authentication flow by OTP** was used as the authentication flow to test the reauthorisation flows.

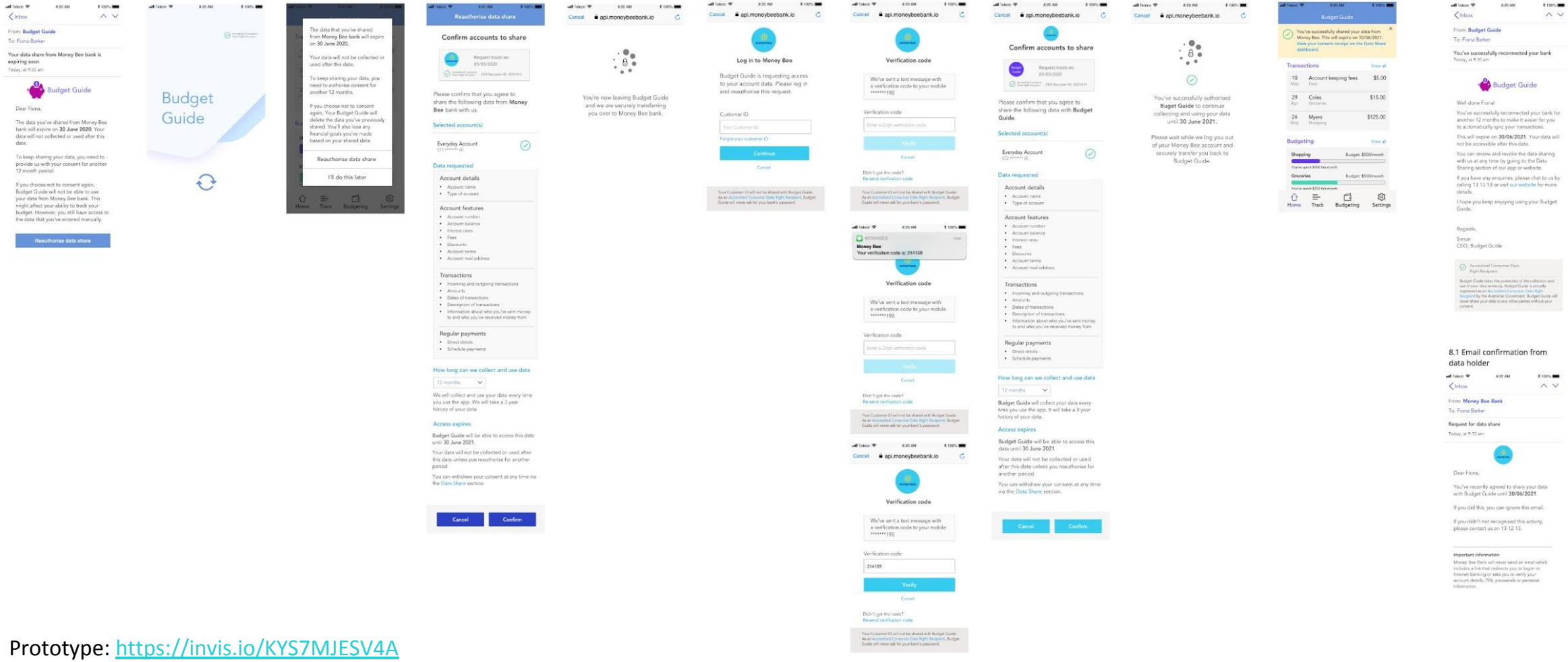
The following pages outline the key findings from the round 2 research.

Reauthorisation

Data recipient space

OTP authentication

Data holder



Prototype: https://invis.io/KYS7MJESV4A

Reauthorisation

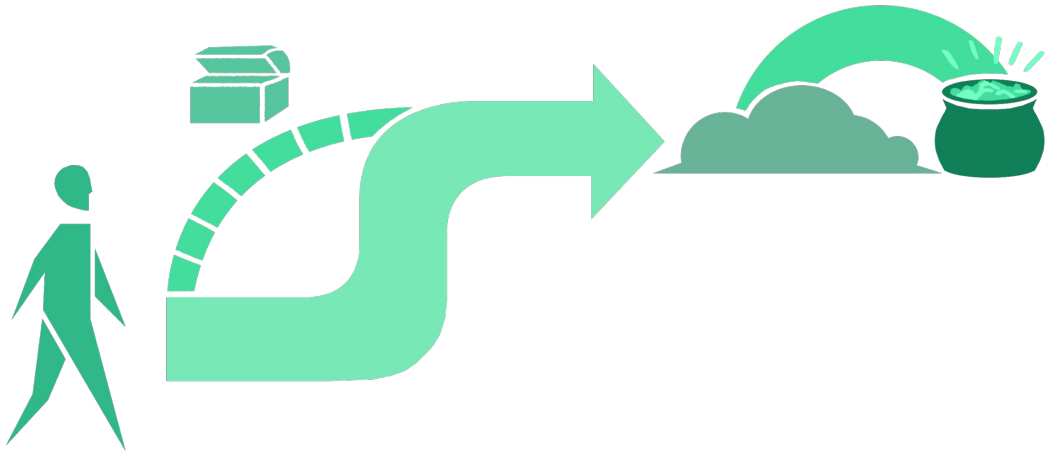
Overall insights

Let me get on with it

Consumers are looking for quick and easy reauthorisation so they can get back to the main task of using the app.

The screens flows (in round 1) felt longer than expected and very repetitive. Many commented that if they were using the app, they were familiar with what and how data is being shared.

This finding remains true from the round 2 research.



Recommendations

- Keep the reauthorisation flow as simple as possible within the allowable rules.

Reauthorisation

Reminder notification/email

Expect to be notified 1 month before

The same findings as round 1 - All participants, unprompted, expected to be notified 1 month before expirations and then again 7 days before the expiration date.

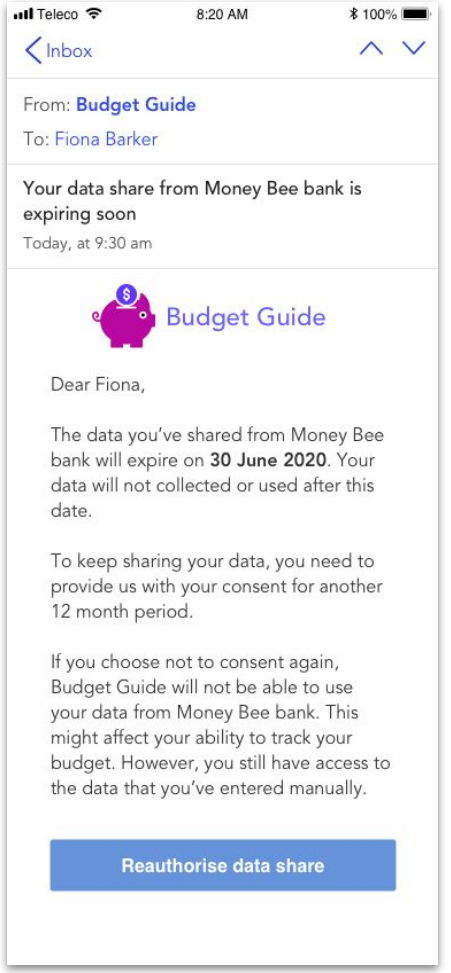
Other delivery methods of notification

Some participants have suggested of other delivery methods of the notification, such as push notifications.

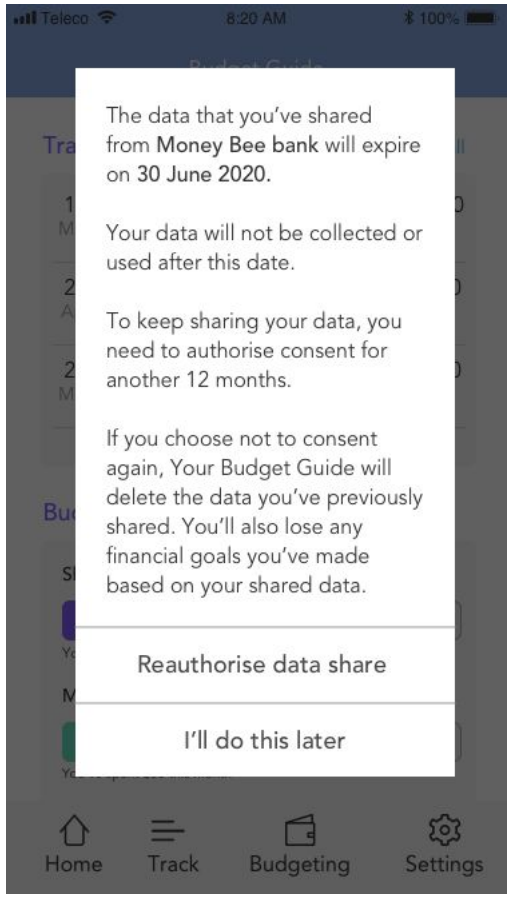
Many of participants highlighted that they might have missed the emails in their inbox.

Communicate revoking method

The option to revoke and how to revoke should also be communicated at this time, as the consent has not yet expired. The consumer should be told they can still revoke the consent at any time.



Email reminder from data recipient



Notification reminder on data recipient dashboard

Reauthorisation

Consent expire/revocation consequences

Expect to have access to the data that they consented to (even after it expired)

Participants understood that if they don't reauthorise, the app (data recipient) will no longer have access to their data. However, they expect that they still have access to the data and the outcome (e.g. financial report created) that they've given consent to in the last 12 months.

They felt unease when told that they might lose what they have created in the data recipient if they don't reauthorise. They wanted to keep it as a record at least.

"I should still be able to see the data in the budget guide. I should be able to send that to my accountant. If I just disconnect and everything is being wiped, I don't have anything to show when I get audited."

CDR Phase 2 | round 2 | Participant 16

Reauthorisation

Confirm consent

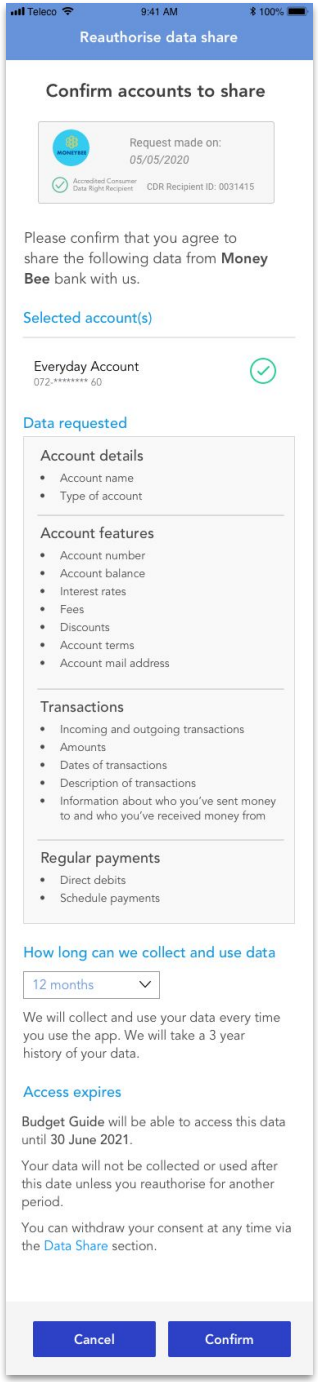
Comfortable with the amount of information presented

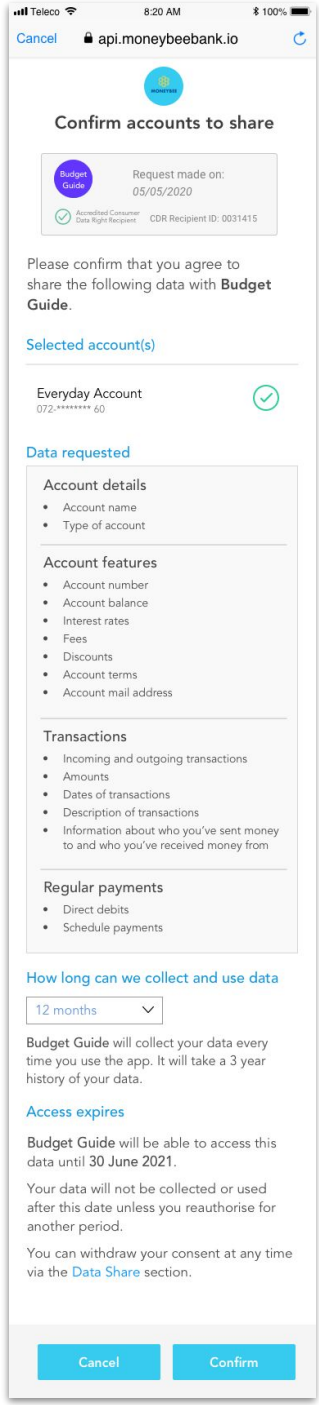
All participants were comfortable with the amount of information presented on this page. They felt that it reiterates the information that they need to know.

Participants assumed that it was the same data that they've consented to at the start. If they were happy to use the app until this point, they were happy to confirm and continue with the process.

Longer consent period at reauthorisation

Participants indicated while they were happy with the 12 month consent duration, they would like to choose a longer time frame so they don't have to reauthorise again after 12 months. They felt that after the first 12 months they have built trust with the app and would be comfortable with a longer period.





Reauthorisation

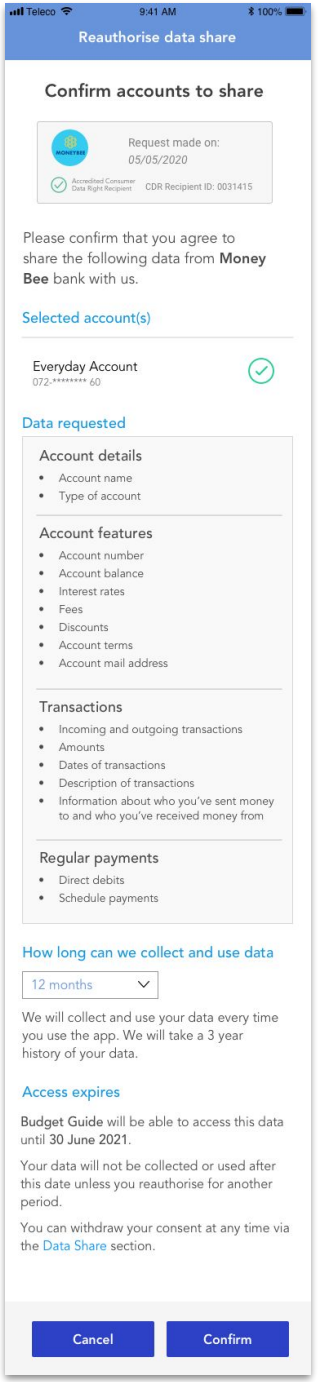
Confirm consent

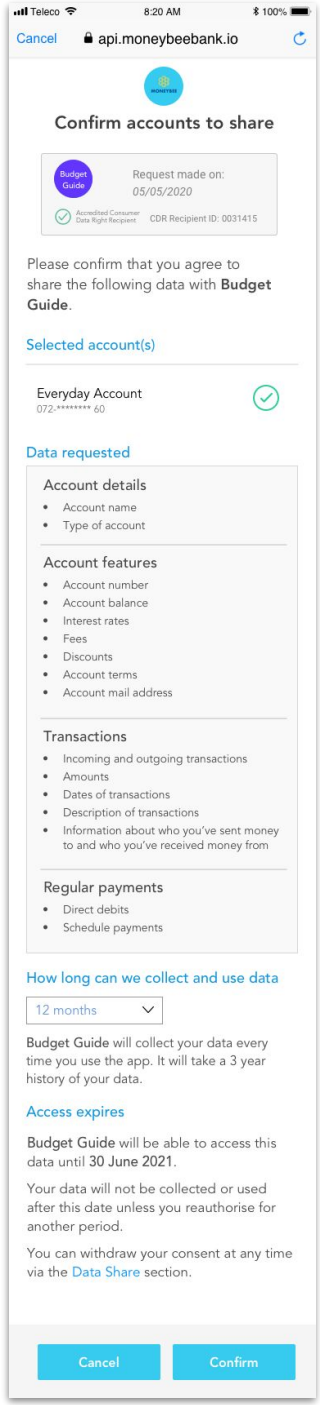
No unnecessary frictions found to reauthorise from data recipient to data holder

Contrary to our earlier hypothesis that consumers might find the reauthorisation process too long and daunting, our research from round 2 found that was not the case.

All participants found the **simplified reauthorisation flow from the data recipient to the data holder** was easy and straightforward. They were comfortable to complete the reauthorisation flow.

Some participants expressed preference for this. It was perceived more assuring that they had to reauthorise from both the recipient and data holder.





Reauthorisation

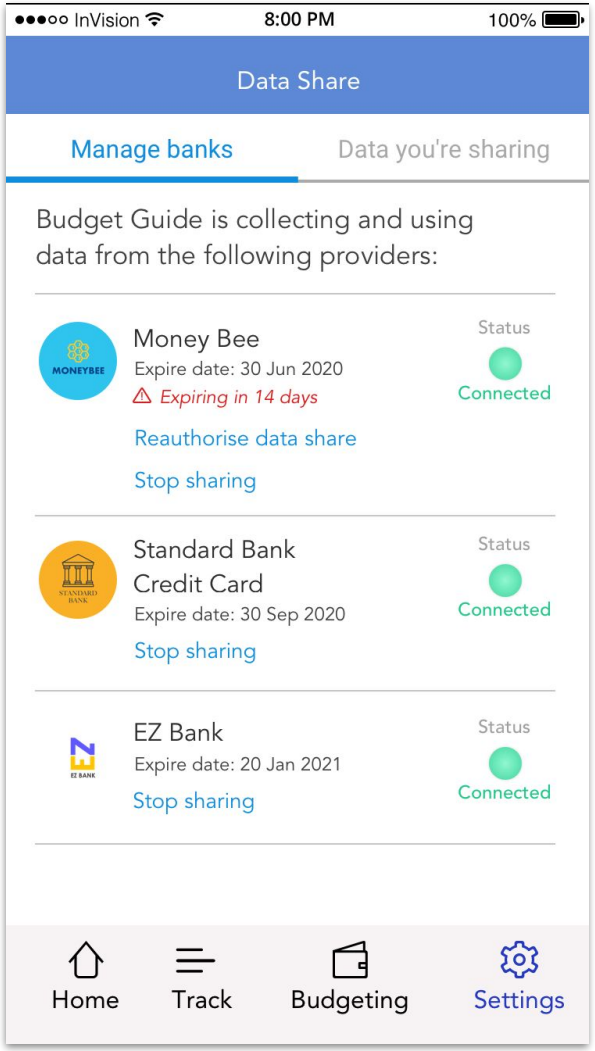
Multiple accounts

During the second round of testing, we wanted to test if there was perceived friction reauthorising multiple accounts.

During the exploration, no participant expressed any concern with this.

Reauthorise individually

The expectation for all consumers was to authorise individually with each bank. They saw each bank as separate and it should remain that way. While there were minor comments that it could be repetitive, it was expected to be this way.



One pager

Additional CDR information

During Round 2 testing, the participants were shown 1 page of CDR content. There were 2 potential ways the user could have seen this - if they chose to click on ‘find out more’ during the consent flow. If they didn’t access it unprompted, they were then shown the content at the end of the research session. Key insights are below.

Legitimises CDR

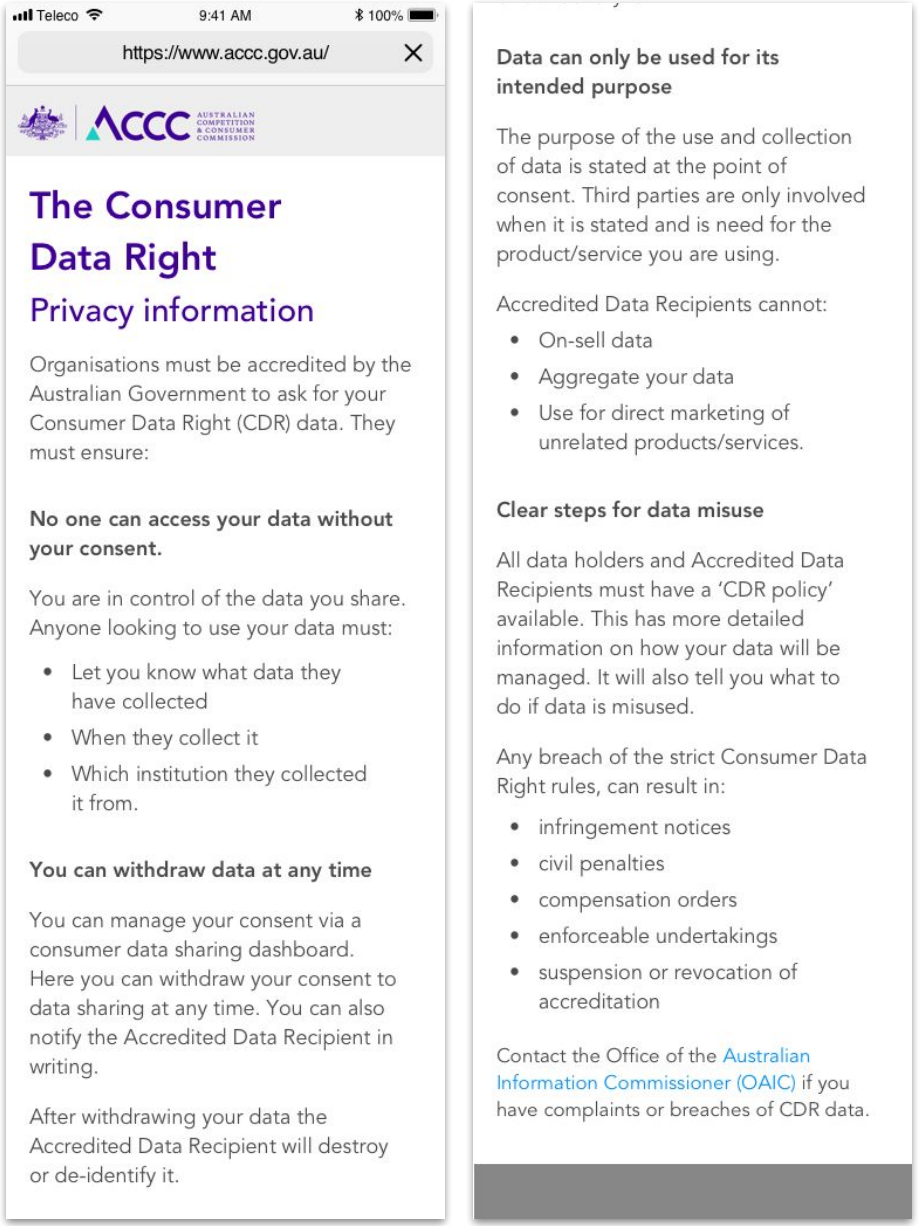
As a new initiative the information provides comfort that the power of the court is in there. The ACCC also carries clout and reputation for many participants we interviewed.

Can government access the data?

Introducing the government as another party in a 2 party data share added confusion. Some consumers felt like the government could access their data and felt like they were interfering.

Over legislation

One participant raised an interesting insight that he felt this would reduce his choice. This legislation would restrict his access to overseas products or products that couldn’t get the accreditation.



One pager

Additional CDR information

Damage is done

Penalties for breaches of data felt too late, if data is ever breached then the damage wouldn't be reversible.

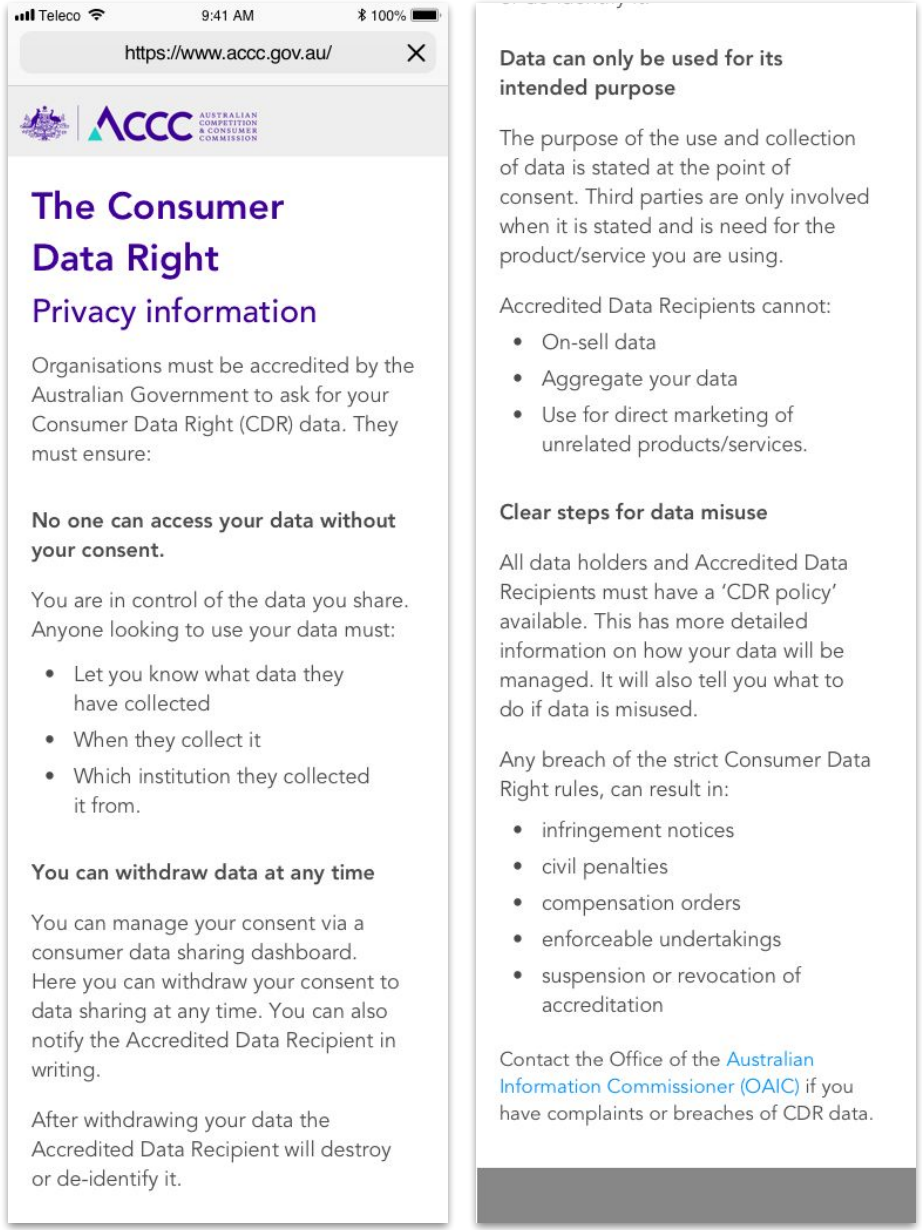
What will happen to my data if I revoke my consent?

The consequences of what will happen to the data when the consent is revoked or expired is not clear.

All participants expected that their data will be completely deleted/destroyed from the systems. However, when stated that their data will be de-identified, this implies that their data is still accessible. This made participants feel uncomfortable which led to distrust.

Contact perceptions

Some participants had past experiences of contacting government departments and felt like it would be complicated or that they'd be passed round from department to department.



One pager

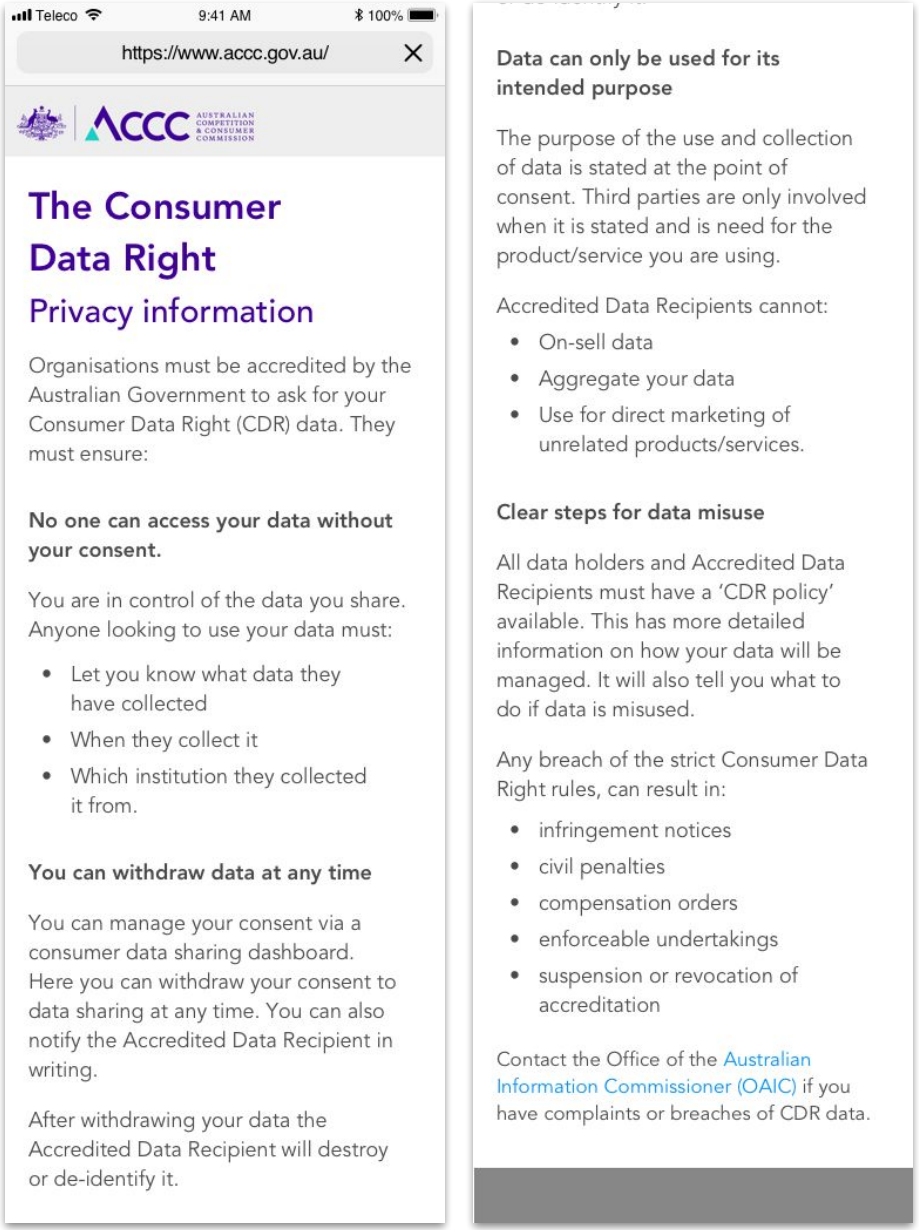
Missing information

Consumers were asked if they felt anything was missing from the content. The more privacy conscious participants said they needed more detail. This included:

- They didn't know how long organisations had to process the deletion or deidentification of data.
- They were expecting monetary figures on penalties, as they felt it wasn't enough.
- Tougher penalties like imprisonment
- Resolution time for penalties
- Where the data is stored/servers
- Be clearer about 'aggregation'

Recommendations

- The one pager suggests that 'aggregation' will be prohibited. This is incorrect. This statement could be rewritten as 'building information about other people without their consent is prohibited'



Next steps and broader considerations

CONSUMER DATA STANDARDS

Next steps

Overview

We recommend following the design patterns (page 33) listed in the report for the immediate release of the consent flows.

As the first release for the Consumer Data Standards begins, further considerations need to take place. Based on the research, we recommend the following:

1. Provide flexibility in consent model
2. Carefully communicate the concept of CDR
3. Manage message fatigue
4. Continuous iterations of consent model for financial sector
5. Revisit data cluster taxonomy
6. Research data share around energy sector
7. Research for accessibility and inclusivity
8. Design for off-boarding experience

Broader considerations

1. Provide flexibility in consent model

Options to change terms during reauthorisation

Some participants expressed their desire to make a change to the consent terms during reauthorisation, such as changing accounts and adding new accounts. This would stop them having to go through the consent flow again.

Choice of data and time

From the research, we identified the desire for selection of data clusters and permission language. This was influenced by the purpose of the app and the participants use case. Consumers want flexibility on consent duration as they experience the app.

Caution of 'Paradox of choice'

While we found the consumers expressed their desire for more flexibility and having more choices, we caution on the notion of 'Paradox of choice'. Providing more choices can be debilitating rather than liberating for consumers. We recommend treating this carefully and follow the data minimisation principles as the first principle before thinking about providing more choices.

Proposed approaches

- Build prototype with more choice at reauthorise and data cluster.
- Test with financial sector
- Look into changing the rules

Broader considerations

2. Carefully communicate the concept of CDR

Some participants had polarising views about government involvements in CDR. The communication strategy for CDR needs to be carefully considered to earn trust and provide comfort to consumers. It also needs to mitigate potential risks, like being compared to other government initiatives such as My Health Record.

Clearly define no intermediary party

Some participants misunderstood CDR as having a government agency as the intermediary party of data share. They expressed negative views around this. They don't trust the government to be transparent about how their data is being used.

Rationale

The recent events involving government agencies such as MyHealth Records and ABC raids have been widely publicised. It had a negative impact in the consumer's perception of how government is handling their data and privacy.

A clear communication strategy with risks and objectives needs to be in place. The comprehension of CDR can not be achieved through the consent flow alone. Clear communication needs to happen so that existing mental models around data sharing and government involvement begin to change.

Proposed approaches

- We recommend clearly communicating the role of government agency in the CDR policy. This can be explained clearly in the 'One pager' or in the trust mark.
- Continue to test and build upon the messaging needed.

Broader considerations

3. Manage message fatigue

The research has been using a single data recipient and data holder relationship. However in reality, once it is rolled out and implemented across sectors (i.e. banking, energy and telco), consumers will be faced with multiple data consent relationships. As a consequence, they will also be faced with managing the number of messages and notifications they received from different providers. The number and timing of notifications needs to be considered.

Rationale

The research showed that consumers felt the 90 day notification was unnecessary and cluttering their inbox. While the intention of this notification was good, it would more likely be ignored by consumers.

However, receiving notifications about their consent expiration was considered important. All participants expected to be notified at least 1 month in advanced, followed by more reminders as the date gets closer.

Message fatigue is well documented to have a reverse effect for people engaging with a service.

Proposed approaches

- Be intentional on the timing and the purpose of sending notification messages to consumers.
- Design notifications and consider their importance, urgency and if it requires action from users.
- Give users control to opt-out from receiving notifications, or to be able to adjust the time period.
- Use appropriate cross-channel delivery method, such as modal/dialog, push notification, text message and email.
- Further research and test the appropriate messaging, timing and delivery of notifications.

Broader considerations

4. Continuous iterations of consent model for financial sector

Continue research as the consent flow moves towards pilot and implementation with real applications. The research scope was limited to fictional scenarios and brands. Reputation of real banks and applications will impact trust and propensity to share.

Rationale

The recommendations from the Phase 1 report still remain true - The implementation of Open Banking in UK demonstrated how, despite the creation of CX guidelines, banks and third parties chose different solutions to consumer consent, authentication and authorisation. The usability of these models naturally differ.

We suggest running a pilot and conducting a comprehensive study to map and evaluate the consent models emerging in Australia post-pilot to inform further refinement of the CX guidelines. This allows this initial implementation to be a test bed and foundation for further innovation.

Proposed approaches

- Map consent models implemented by banks and third party providers and outline differences and similarities.
- Test spectrum of consent models with Australian consumers to explore usability and consumer comprehension.

Broader considerations

5. Revisit data cluster taxonomy

Continue to test and iterate taxonomy/categories of data clusters with multiple use cases, such as business data vs personal data.

Rationale

The data clusters and permission language were only tested for one use case. When probed about the data sets, some also found overlap in their understanding.

The data clusters need to be tested with more use cases and across multiple sectors. This will ensure potential combinations of data clusters and use cases will reduce overlap between category perception.

Proposed approaches

- Moderated open card sorts with a wider range of data cluster and permission language.
- Scale to closed card sorts with unmoderated tools.
- Set multiple tasks across different sectors to see if participants understand the data sets.

Broader considerations

6. Research data share around energy sector

Participants indicated that they were more willing to share data around their energy usage over their financial data. Energy usage was seen as less personal than financial data. However, this was an early hypothesis which needs further research and testing.

Rationale

As we saw in our research, participants have different attitudes towards use case and type of data. Further research needs to go into the energy sector and the use cases.

We saw areas in the financial consent flow that brought trust, friction or comfort. The flow should be tested to see if these still remain true. There should also be a focus on any variables introduced like intermediary parties, longer durations or authentication models.

Proposed approaches

- Engage key stakeholders from energy sectors to develop consumer facing data language and data clusters.
- Test the designated data and language with a spectrum of consumers, through interviews & surveys.
- Develop and test consent models incorporating proposed language.
- Explore consumer appetite in these sectors, including a focus on trust and privacy.

Broader considerations

7. Research for accessibility and inclusivity

More work needs to be done for Consumer Data Standards to be fully accessible and inclusive. This will impact all Australians, so needs to include all Australians in the research. This is a recommendation that has been carried over from the first phase and still needs to be considered in further research.

Rationale

To ensure CDR is accessible to Australian's with specific accessibility needs. We suggest conducting further research to explore, i.e. visual and audio consent flows and consent in languages other than English (e.g. Mandarin and Arabic).

Proposed approaches

- Develop prototypes adapting existing consent language and consent model to multiple languages.
- Develop visual and audio consent prototypes.
- Test prototypes with Australian consumers with specific accessibility and language needs

Broader considerations

8. Design for off-boarding experience

Like any relationships, there comes a time when the consumer will end their relationship with the product/services that they have been using.

Most participants found comfort in knowing that they can stop sharing and revoke their consent at any time during the consent period. However what will happen to their data after this was not clear.

Consumers need to fully understand what happens to their data when they sign-out from the service.

Rationale

The research showed that most participants expected that their data will be deleted when they revoke or it expires.

However, some participants also assumed that the data will not be completely deleted from the systems and that they might be used for other analytical purposes.

Proposed approaches

- Clearly define how data will be handled when the consent period has ended.
- Clearly define how data will be handled when the service has stopped either by the consumer themselves, the recipient or the data holder.
- As per Data Trust by Design principles, make it simple and easy for Consumer to manage what happens to their data when they stop using the service.
- Consider similar approaches to the GDPR - 'Right to be forgotten' - which regulates how personal data should be handled when the data is no longer needed or when the consent has been withdrawn.

Appendices

CONSUMER
DATA
STANDARDS

Prototype

Round 1

The prototype that was used in round 1: https://invis.io/5FRWJ7PJ829

This consists of:

1. 2x Authenticate in the Flow:
   a. Redirect to Known authentication flow
   b. Decoupled authentication flow
2. 1x 90 days notification
3. 2x Reauthorisation flow
   a. 1x reauthorisation flow in the data recipient app
   b. 1x reauthorisation flow in the data holder app

Round 2

1. 2x Authenticate in the Flow:
   a. Redirect to Known authentication flow (v2): https://invis.io/JMS7MGL2APQ
   b. Authentication with One Time Password (OTP) flow: https://invis.io/NUS7LISFAR6
2. 2x Reauthorisation flow
   a. 1x simplified reauthorisation flow from the data recipient to the data holder: https://invis.io/KYS7MJESV4A
   b. 1x simplified reauthorisation flow with consent confirmation at the data holder (round 2): https://invis.io/TES9RPSZNSR
3. 1x CDR information page from ACCC: https://invis.io/TES9RPSZNSR#/366135257_ACCC-OnePager
4. Multiple account reauthorisation: https://invis.io/TES9RPSZNSR#/366130755_00_ManageBanks-Multiple

CONSUMER
DATA
STANDARDS

BIAS

THANK YOU

Consumer Data Standards | Consumer Experience Workstream

t +61 2 9490 5722
e cdr-data61@csiro.au
w consumerdatastandards.org.au