DATA
STANDARDS
BODY

Auth Drop Off WG

Data Collection Issues - May 2024

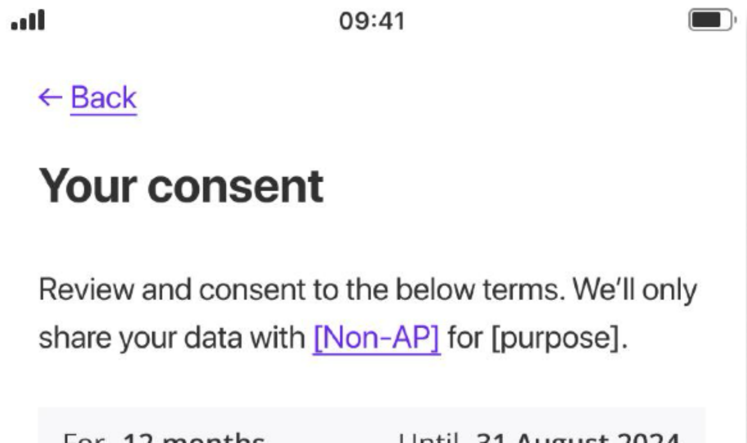
Overview 01

Barriers to Data Collection

DSB engagements over the last few years have highlighted barriers to ADRs collecting data from DHs.

Recent community input and analytics have highlighted critical issues on the DH-side, particularly in **authentication** and **authorisation** flows, but also in relation to **account access**.

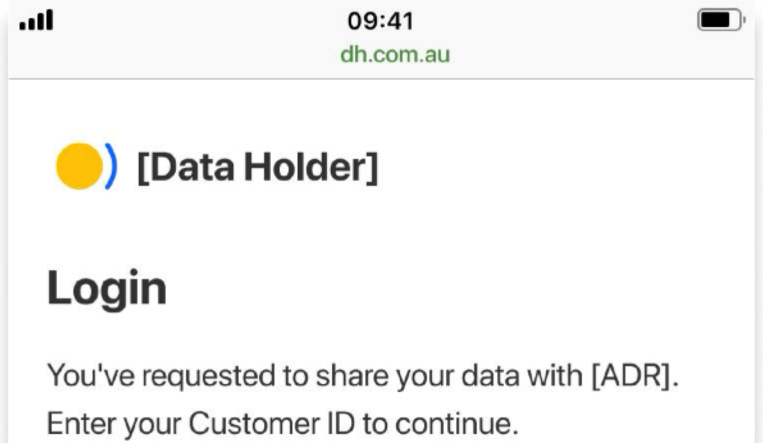
While the consent review proposed to focus on these and other issues in a second phase of work, the first phase of the consent review has been limited to ADR-side improvements.



Your consent

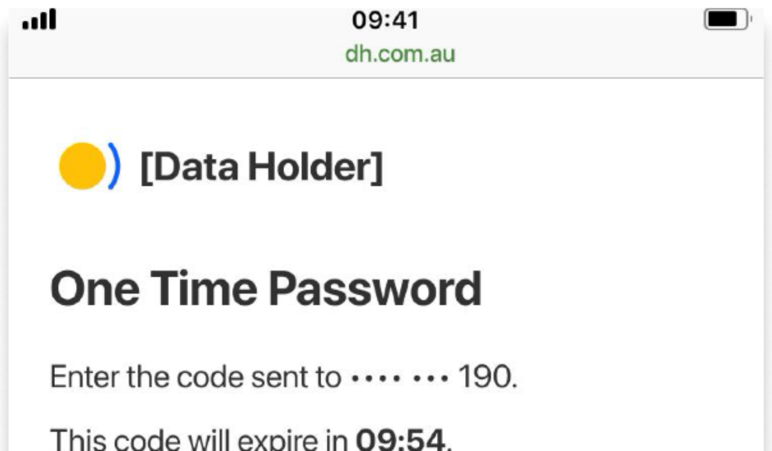
Review and consent to the below terms. We'll only share your data with [Non-AP] for [purpose].

For 12 months Until 31 August 2024



Login

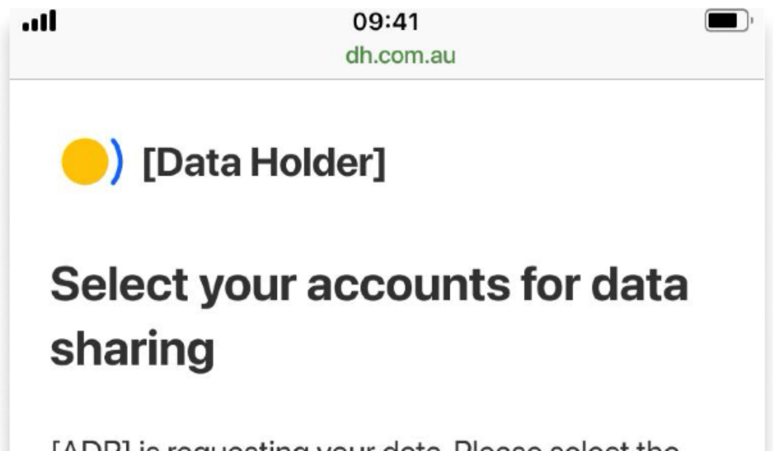
You've requested to share your data with [ADR]. Enter your Customer ID to continue.



One Time Password

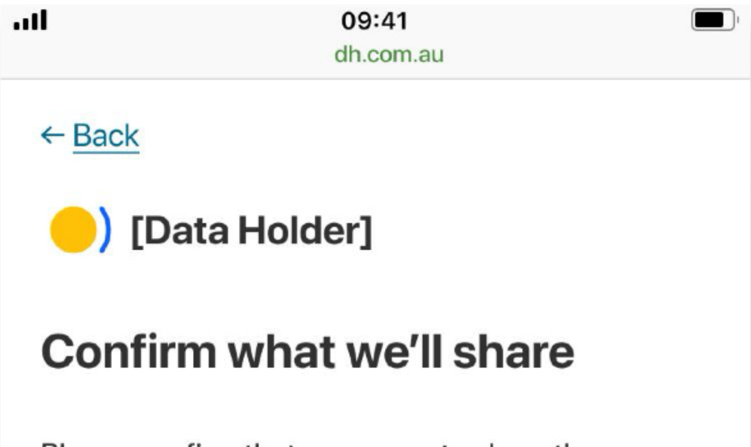
Enter the code sent to •••• ••• 190.

This code will expire in **09:54**.



Select your accounts for data sharing

[ADR] is requesting your data. Please select the



Confirm what we'll share

Community Points 02

Consent Review

Of 22 submissions, **72% supported future work on consent**, with a **strong emphasis** on **authentication** and **authorisation improvements**. These points were made by ADRs, DHs, and industry bodies.

Screen Scraping Consultations

Screen scraping consultations similarly **emphasised** that **further work on data holder authorisation processes** would be necessary **to improve consent completion rates**.

Community and Analytics

Analytics from various sources suggest that around **25-60%** of **consumers do not complete the DH process**. Around **30-50%** of **those drop offs** occur **during the authentication process**, and some data sources suggests this **may be high as 89%**.

ADR Sessions

A targeted ADR working group on consumer drop offs has validated, refined, and expanded on these points. Working with the DSB and ACCC, 5x ADRs have highlighted **drop off sites** and **barriers** that include:

- **Authentication**
- **Profile selection**
- **Account selection** and **availability**
- **Non-individual** and **secondary user settings**
- **UI issues** and **divergence**

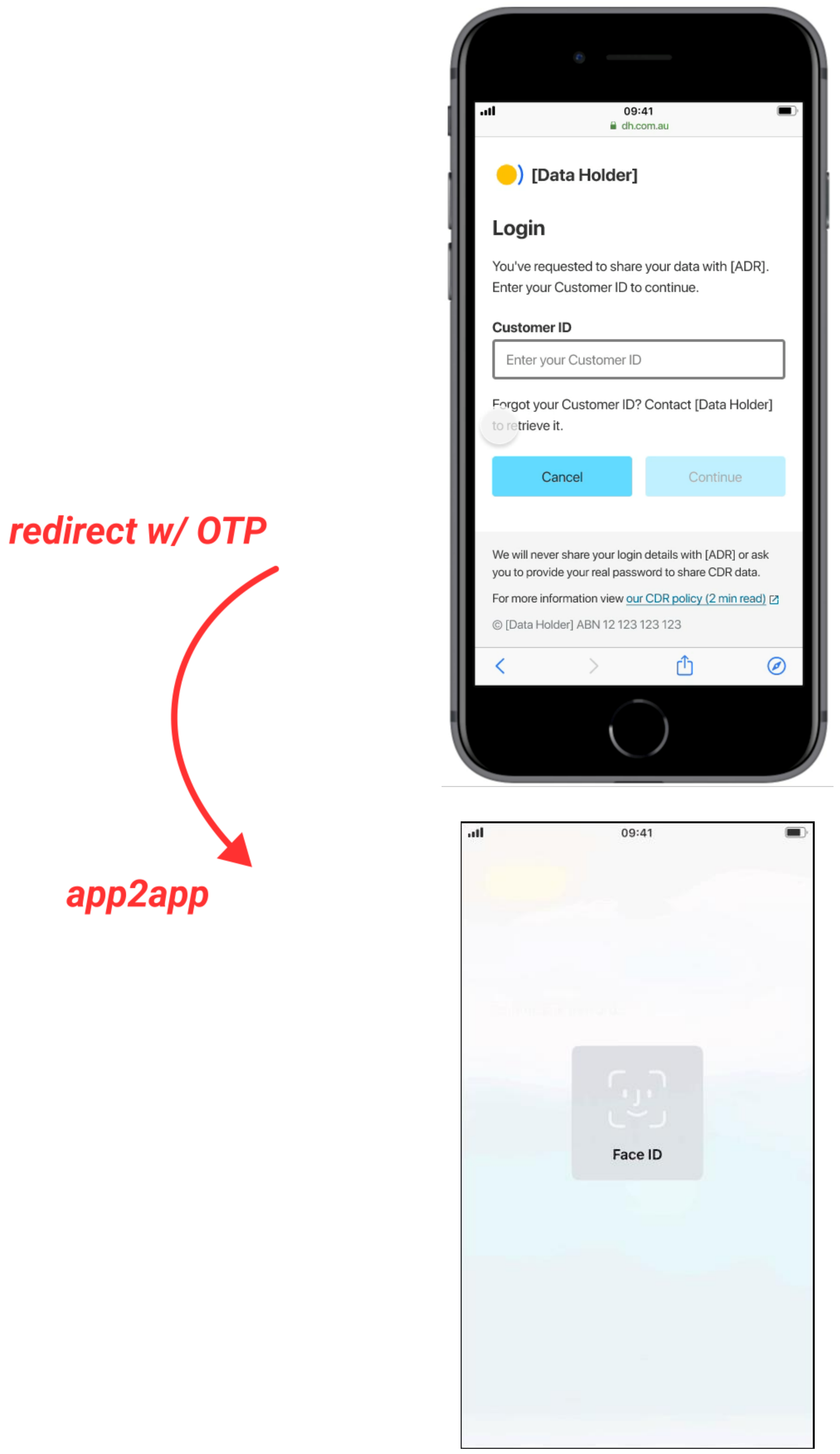
Key Opportunities 03

Authentication

Authentication Uplift [standards]

While Redirect with OTP creates completion issues, conversion rates appear to improve slightly with familiarity.

Improving the consumer experience would require other authentication processes to be familiar and simpler - and app2app is seen as a prime candidate to significantly reduce drop off rates.



redirect w/ OTP

app2app

[Data Holder]

Login

You've requested to share your data with [ADR]. Enter your Customer ID to continue.

Customer ID

Enter your Customer ID

Forgot your Customer ID? Contact [Data Holder] to retrieve it.

We will never share your login details with [ADR] or ask you to provide your real password to share CDR data.

For more information view our CDR policy (2 min read)

© [Data Holder] ABN 12 123 123 123

Authentication

Error Messages [standards]

Improved OIDC error messaging could be implemented to assist ADRs and better align with metrics stages.

User Messages [standards] or [guidance]

Standards or guidance could be introduced for data holders to provide consumers with authentication instructions. This could, for example, include instructions for how to locate your customer ID for the purposes of authentication.

Completion Benchmark [standards] or [enforcement]

A benchmark % rate for completion could be prescribed via the standards and/or enforcement activity.

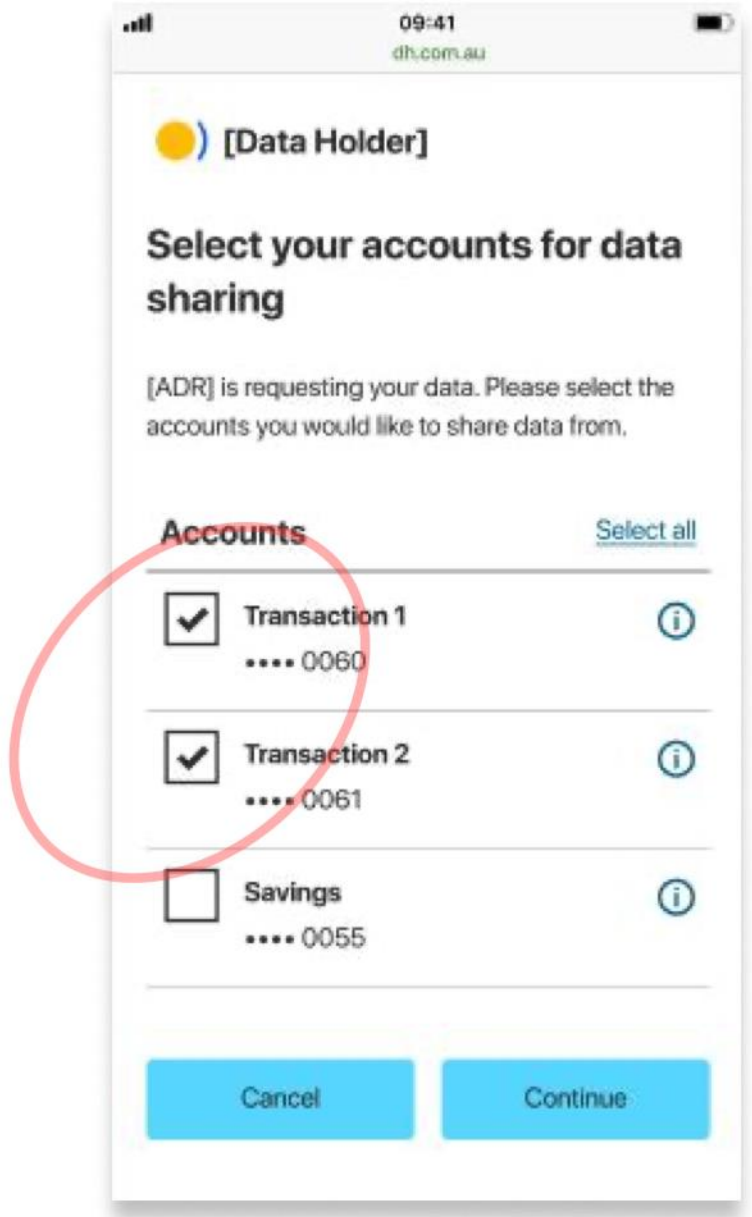
Key Opportunities 04

Authorisation

***Simplification* [standards] and [rules]**

The authorisation process could be simplified with a view to reduce/remove extraneous information and interactions.

This could include, for example, UI and step mandates, information reduction, or the removal of entire steps from the process - especially for the amending consent process.



09:41
dh.com.au

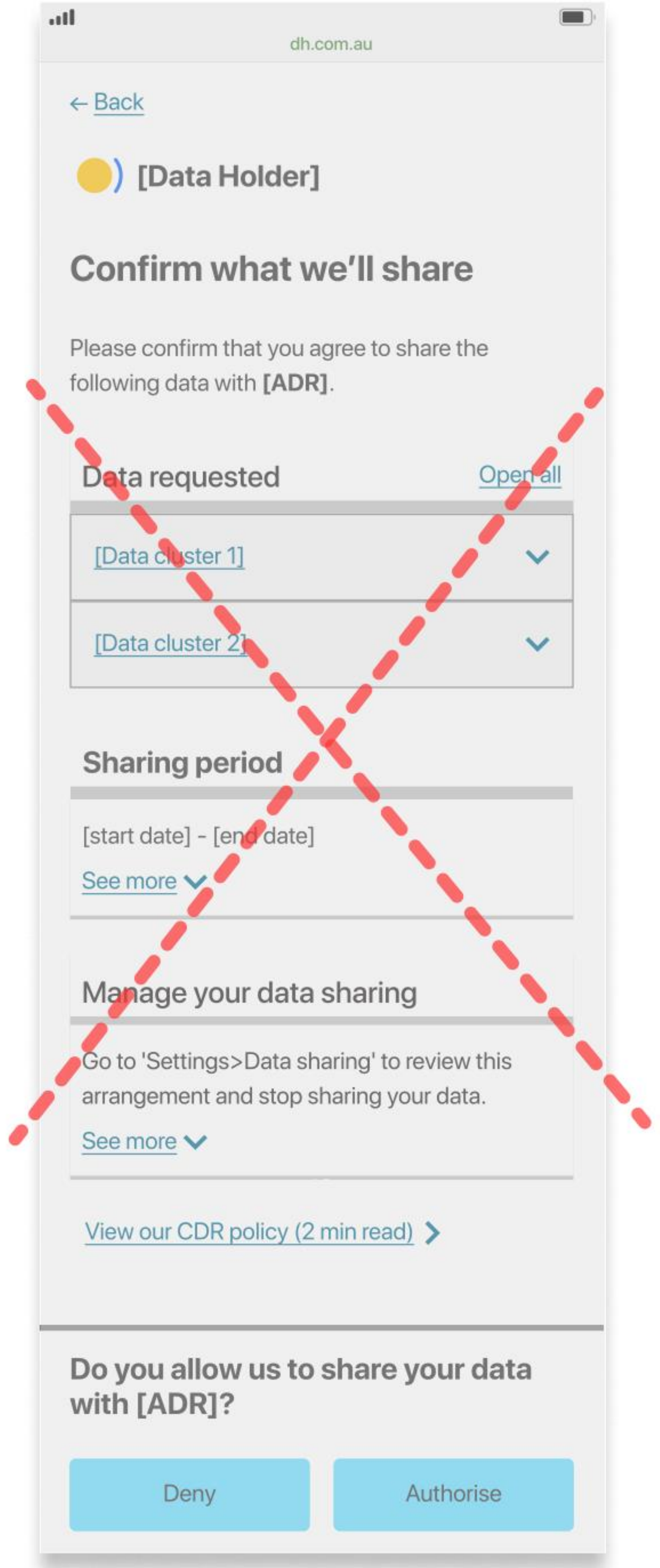
[Data Holder]

Select your accounts for data sharing

[ADR] is requesting your data. Please select the accounts you would like to share data from.

Accounts — Select all

- ☑ Transaction 1 •••• 0060
- ☑ Transaction 2 •••• 0061
- □ Savings •••• 0055



dh.com.au

← Back

[Data Holder]

Confirm what we'll share

Please confirm that you agree to share the following data with **[ADR]**.

Data requested — Open all

[Data cluster 1]

[Data cluster 2]

Sharing period

[start date] - [end date]

See more

Manage your data sharing

Go to 'Settings>Data sharing' to review this arrangement and stop sharing your data.

See more

View our CDR policy (2 min read)

Do you allow us to share your data with [ADR]?

Authorisation

***Characteristics Specification* [standards]**

With support for FAPI 2.0 Rich Authorization Requests (RAR), ADRs can specify required characteristics to simplify the authorisation flow. This could be the type of user (e.g. non-individual) to streamline profile selection, or accounts that are required for the use case, which can then be pre-selected in the authorisation flow.

***Error Messages* [standards]**

Improved OIDC error messaging could be implemented to assist ADRs and better align with metrics stages.

***UI Standardisation* [standards] or [guidance]**

Standards or guidance could be introduced for data holders to implement consistent and minimal user interfaces, interactions, flows, and language.

Authorisation

Unavailable Accounts **[standards]** **or** **[rules]**

Consumers do not always know how to make unavailable (but eligible) accounts shareable. This includes non-individual consumers, where a representative has not been nominated, and secondary users, where a secondary user instruction has not been given. Two opportunities exist to address this issue:

1. Optional CX standards already recommend that, where eligible accounts are unavailable for sharing, DHs provide in-context instructions and enabling capabilities. In the absence of voluntary DH adoption, these standards could be proposed as mandatory.

2. Alternatively, ADRs have supported ‘multi-party’ sharing permissions to be turned ‘on’ by default, in line with the customer’s existing authorities with their DH. This would reflect the recommendations of the 2017 Open Banking Review and mirror the 2022 changes to joint accounts.

Authorisation

Support ID **[standards]**

ADRs have indicated that the *cdr_arrangement_id* and the *request_uri* are created, provided, and stored inconsistently, limiting the utility of these artefacts to resolve consent issues with DHs.

A new or amended identifier could assist ADRs to pursue support and resolutions, and could also allow consumers to self-service with human-readable consent identifiers.

This could be a new and binding ID that is generated by the ADR and available throughout the process, including to consumers, or could be an extension of the *cdr_arrangement_id* enabled by RAR.