DATA
STANDARDS
BODY

Authentication Uplift

Research Outcomes & Proposed Approach

July 2023

Agenda

Research Approach	**4**
Overview	5
Research goals	6
Elements tested	7
Prototypes	8
Use cases	11
Research Outcomes	**12**
Research themes	13
Supporting metrics	19
Outcomes	20
Proposed Uplift Approach	**21**
Opportunities identified	22

Authentication Uplift

Context

Several reviews and inputs have proposed a review of CDR authentication and informed the research, including:

- The Government's response to the Inquiry into Future Directions for the CDR
- An Independent Information Security Review
- The Data Standards Advisory Committee, including a November 2020 presentation on 'waterfall authentication'
- Community Change Requests (CR), including CR554, CR568, CR542, and CR405
- Noting Paper 296 on offline customer authentication
- The Accessibility Improvement Plan
- Findings from internal reviews

Research Approach

What did we want to find out?
What did we do?

Research Approach

Overview

The first half of this presentation shares findings and presents a comparison from three rounds of CX research conducted as part of the Authentication Uplift project.

Round 1 | September 2022
Benchmarked the Redirect w/ One Time Password (OTP)

Round 2 | November 2022
Tested App/Web-to-App with Biometric

Round 3 | March 2023
Tested Decoupled with QR Code

Over 150 consumers participated across three rounds or research which involved 90-minute 1-on-1 interviews and 30-minute unmoderated prototype tests.

Various prototypes were used to facilitate discussion and generate insights in relation to the models tested, as well as to authentication more generally.

Research Goals

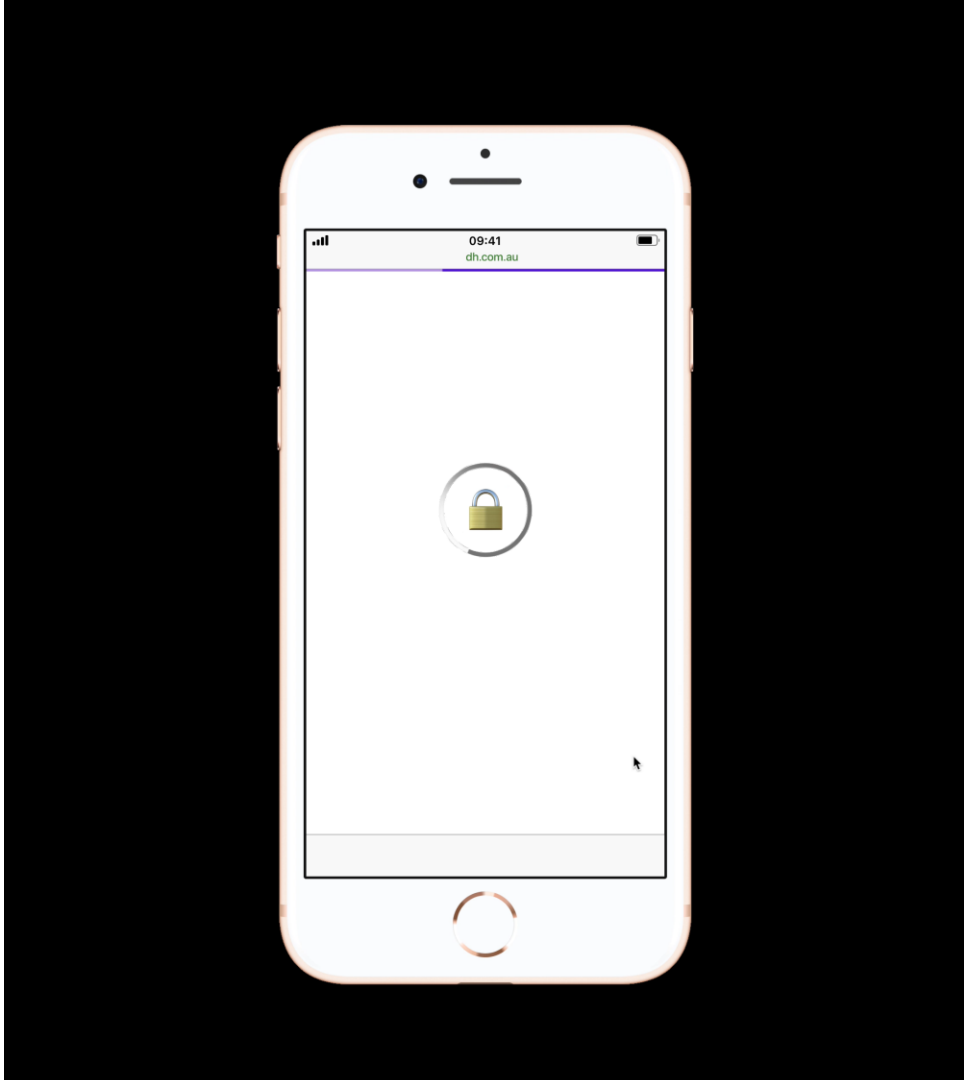
- Identify appropriate authentication models to support in the CDR;
- Provide CX input to the authentication framework to assess incoming/supported models;
- Strike a balance between security, consumer experience and value delivery;
- Help organisations provide intuitive, informed, trustworthy consent experiences with positive outcomes.

Elements Tested

Round/Model	Channel	Modality	Notification method	Authentication method	Authentication method
R1 (OTP)	App-to-Browser	OTP	SMS	Possession	Something the user has (Phone/OTP)
R2 (App/Web-to-App)	App-to-App	Biometric only	Push	Inherence	Something the user is (Biometric)
	App-to-App	Biometric + OTP	SMS	Inherence + possession	Something the user is (Biometric) Something the user has (Phone/OTP)
	Browser-to-App	Biometric only	Push	Inherence	Something the user is (Biometric)
	Browser-to-App	Biometric + PIN	Push	Inherence + possession	Something the user is (Biometric) Something the user knows (PIN)
R3 (Decoupled)	Browser-to-Browser	OTP	SMS	Possession based	Something the user knows (Customer ID)
	Browser-to-App	Biometric + PIN	Push	Inherence + knowledge	Something the user has (Phone/OTP)

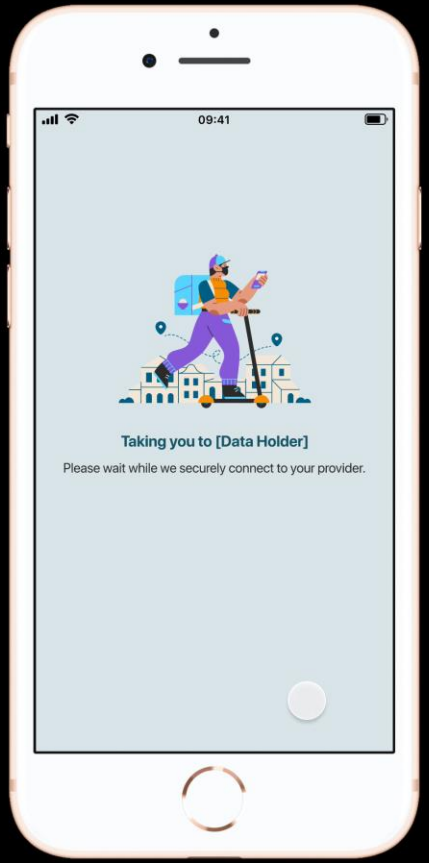
Prototypes

Redirect with One Time Password



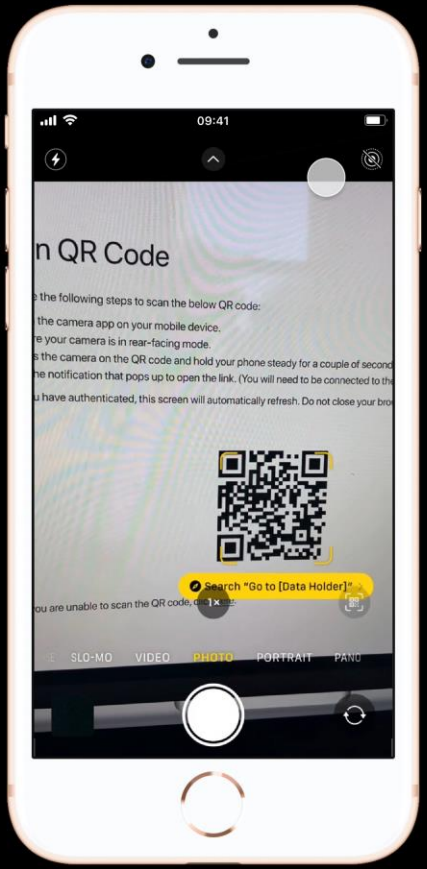
Prototypes

App/Web-to-App with Biometric



Prototypes

Decoupled with QR Code



Use Cases

Banking

A non-bank lender ADR

Telco

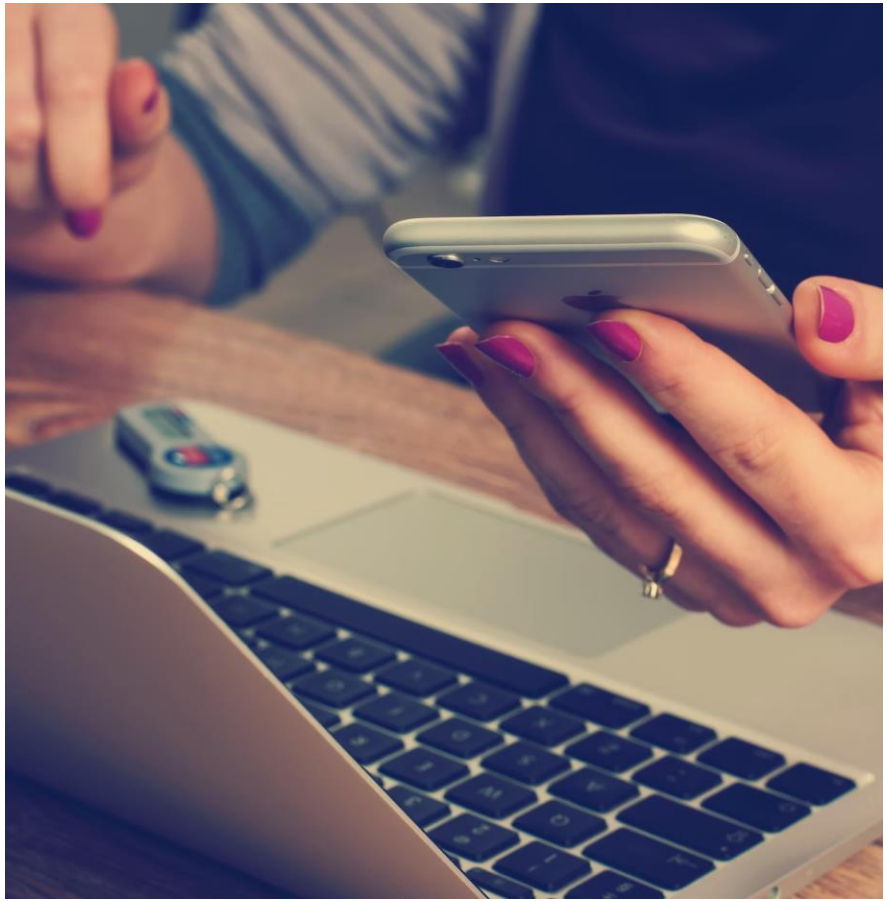
A telco comparator service ADR

Energy

An energy plan comparator ADR

Research Outcomes

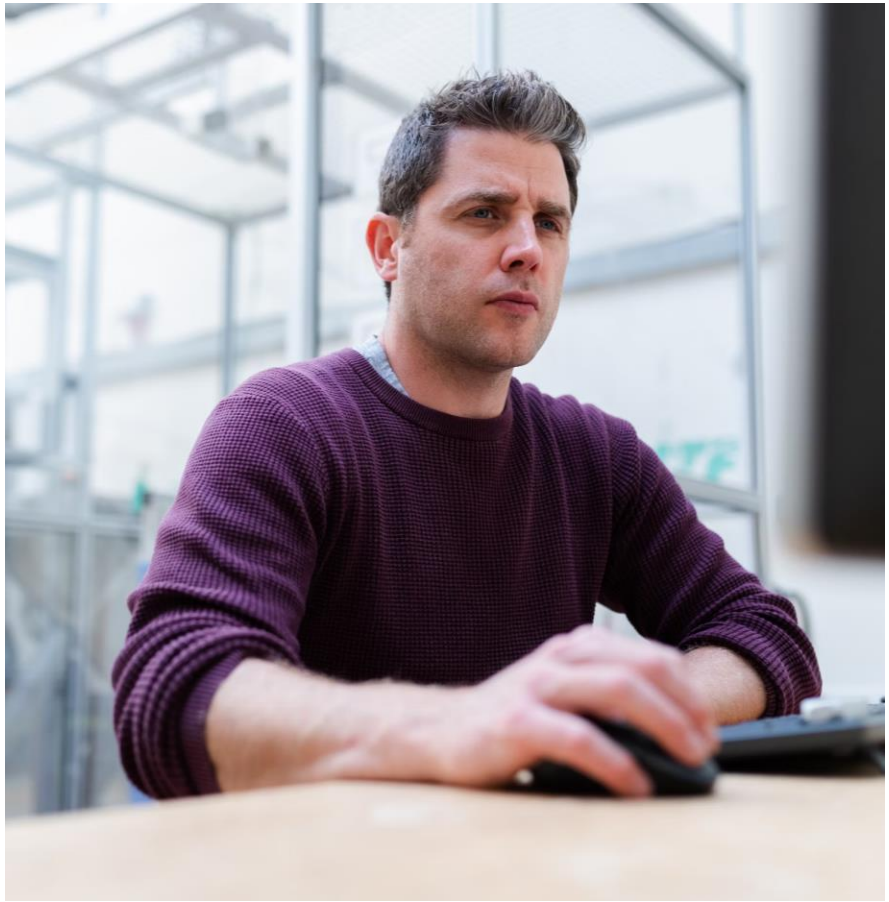
What did we uncover?



Research Outcomes

Friction is multifaceted

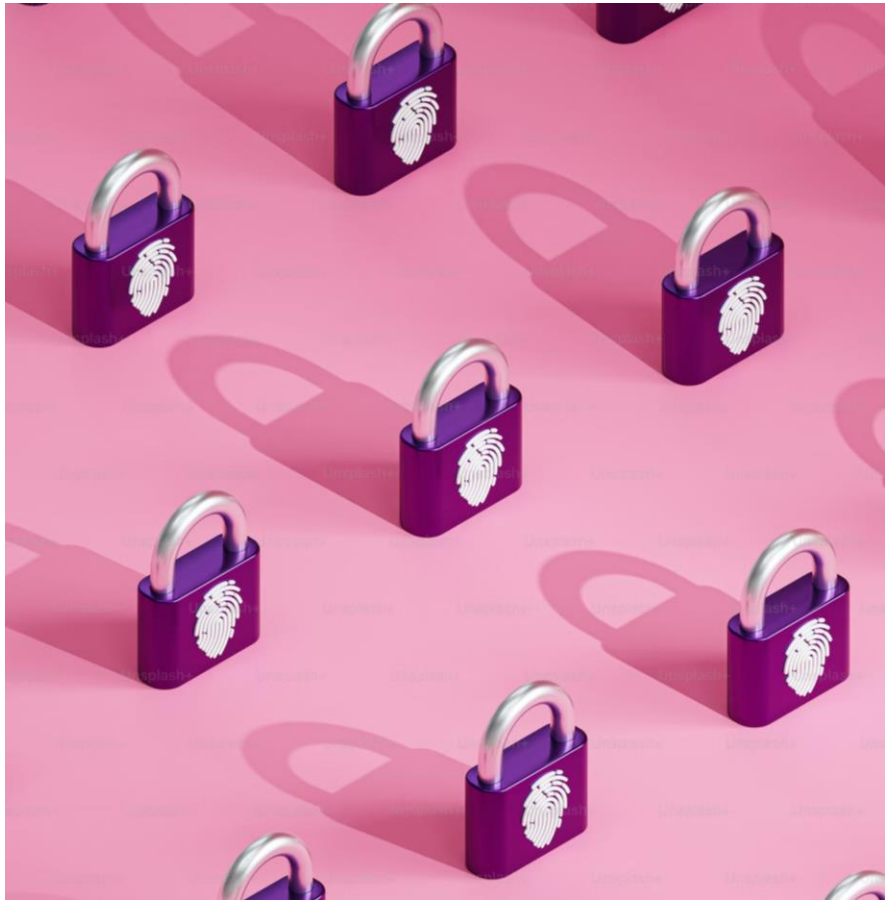
- The research found the principle of friction to be multifaceted, with factors manifesting in various ways; friction can occur both online and offline.
- Friction can be viewed by consumer participants as negatively or positively impacting on an authentication experience, i.e. ‘positive’ or ‘negative’ levels of friction.
- One may hypothesise that higher levels of online friction create more frustrating experiences for users, however the research does not support this.
- While some participants experienced frustrations when accessing devices (such as to receive OTPs or access an app), they generally appreciated lengthier processes when accessing sensitive data.



Research Outcomes

Users look for, and rely on, visual trust markers to assess risk

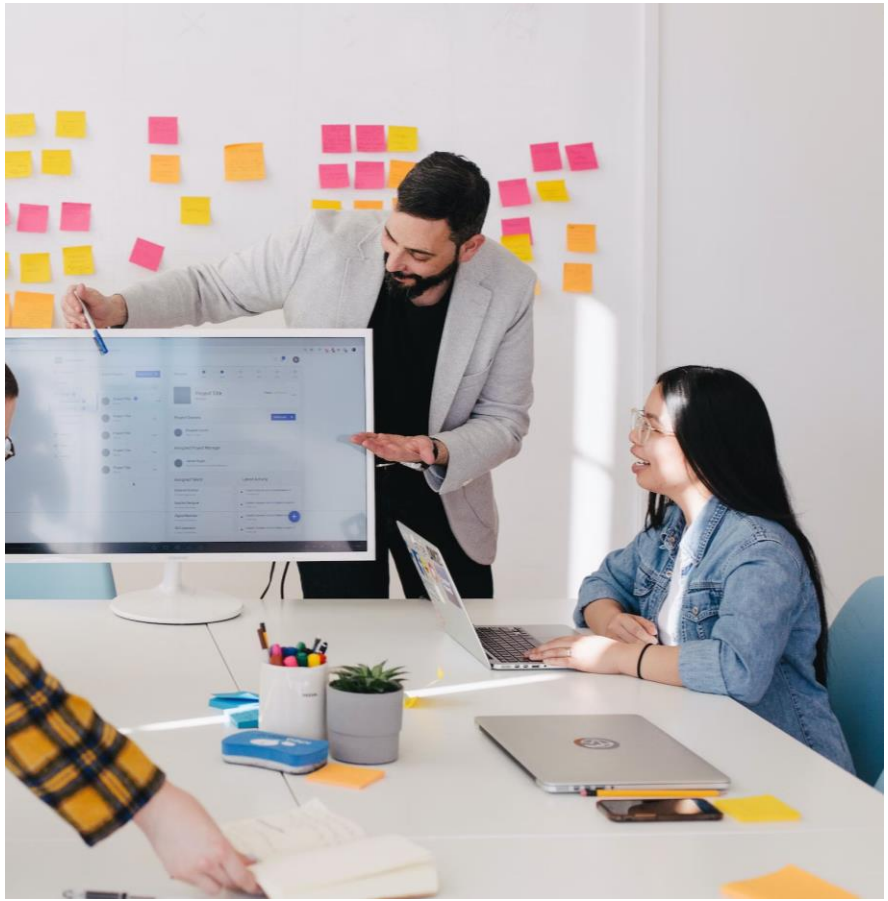
- Consumer participants across all age demographics were conscious of the risks involved with using the internet and implement practices and habits to ensure online safety.
- Each research round saw an uptick in participant awareness of the potential for data breaches, and an increased understanding of scams.
- Those who had been impacted by previous security breaches are proactive in their approach to online safety.
- The research found participants heavily relied upon visual cues to determine whether a platform was trustworthy.



Research Outcomes

Extra authentication factors are appreciated

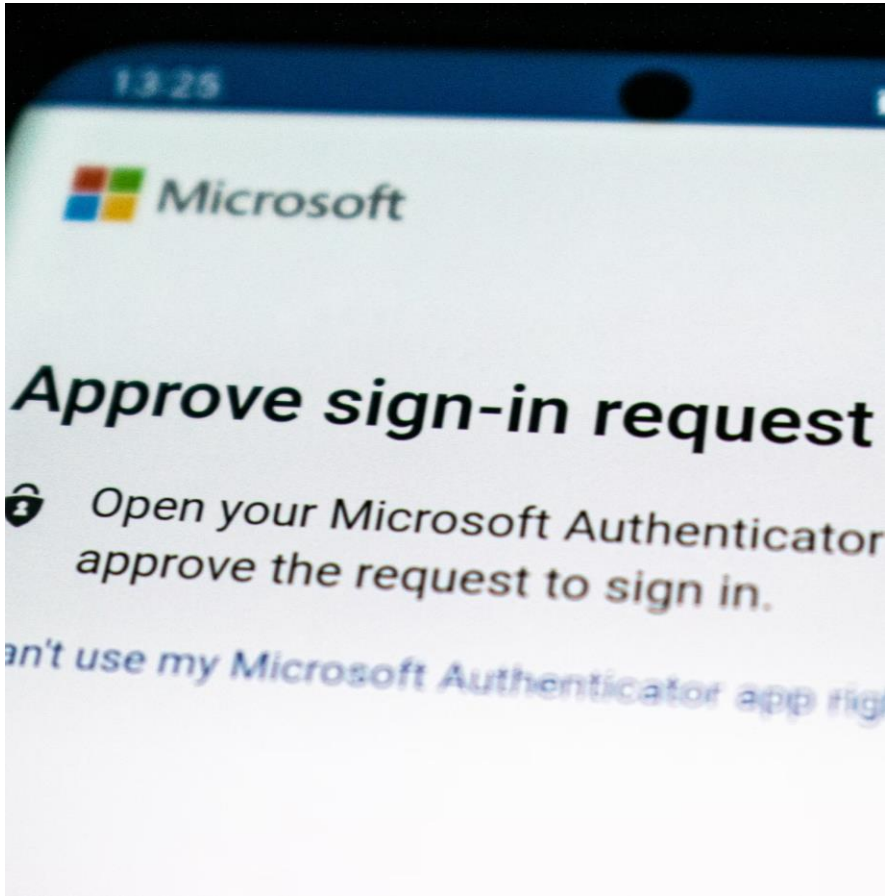
- Consumer participants appreciated extra factors even when they were not expected. Although 2FA was expected for high-risk scenarios, participants appreciated extra factors for actions they deemed less risky.
- Participants did not feel negatively toward increased friction. On the contrary, participants perceived the extra layers of security as the corporation's effort to prioritise data security.
- Extra factors provided participants with a sense of security and comfort. Research indicated that the extra factors or increased friction should be in context and relevant to the use case.



Research Outcomes

Meeting consumer expectations helps to build trust

- The research highlighted the importance of corporate responsibly in order to build trust. Consumers generally only create accounts out of necessity and believe more needs to be done by businesses to protect customer data.
- Participants expect businesses to remain up to date with cybersecurity best practices, never share data with third parties, direct adequate funding to building strong systems and hire talented teams.
- Interestingly, participants inherently placed more trust in larger and more established brands, though they recognised that their data is not guaranteed safety.
- Participants cited Optus, Medibank and Latitude as examples of companies whose recent data breaches have shaken consumer trust.



Research Outcomes

Step-up authentication is perceived as the norm

- The research found that consumer participants expected authentication to adapt and become more rigorous as the sensitivity of their data increased.
- Participants were familiar with risk-based step-up authentication because it is common in industries such as banking.
- Participants generally had a decent understanding of the requirements of step-up authentication, and the friction was considered positive.
- Step-up authentication aligned with participant expectations of security and demonstrates the importance of security measures that are tailored to meet individual user actions.

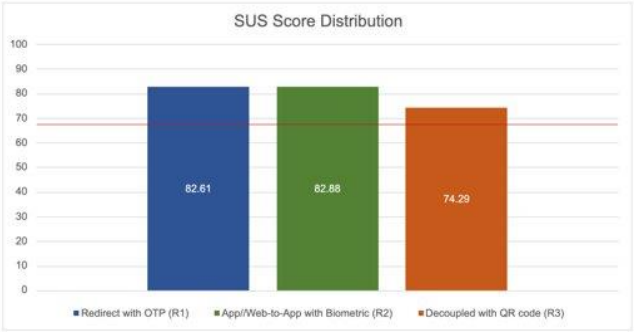
Research Outcomes

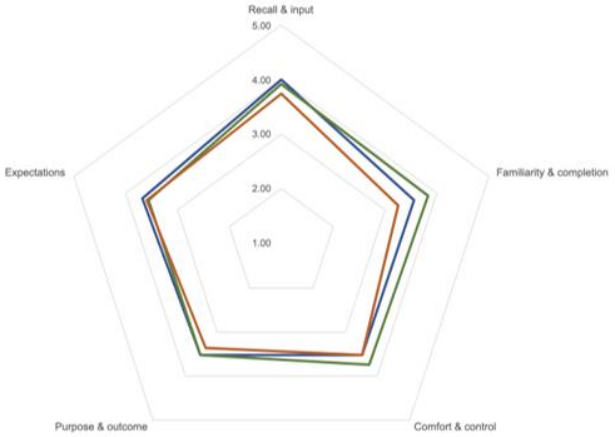
Importance of protecting vulnerable consumers

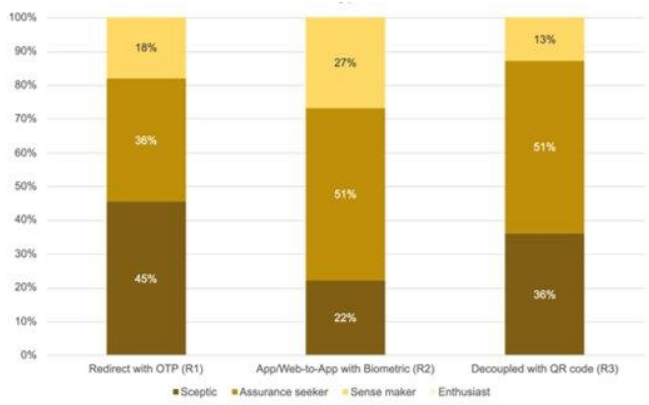
- The research reiterated the importance of accessibility and protecting vulnerable customers.
- Both permanent and temporary disability impact how users prefer – and are able – to authenticate online.
- Further findings included people who cannot read or write, or those with English as a second language may find it hard to comprehend complex information. This reiterates the importance of providing alternative ways to authenticate.
- An alarming finding from the research was the risk malicious intent poses to vulnerable users. Cases are varied in nature, but regularly involve Domestic and Family Violence, or elder abuse.

Supporting Metrics

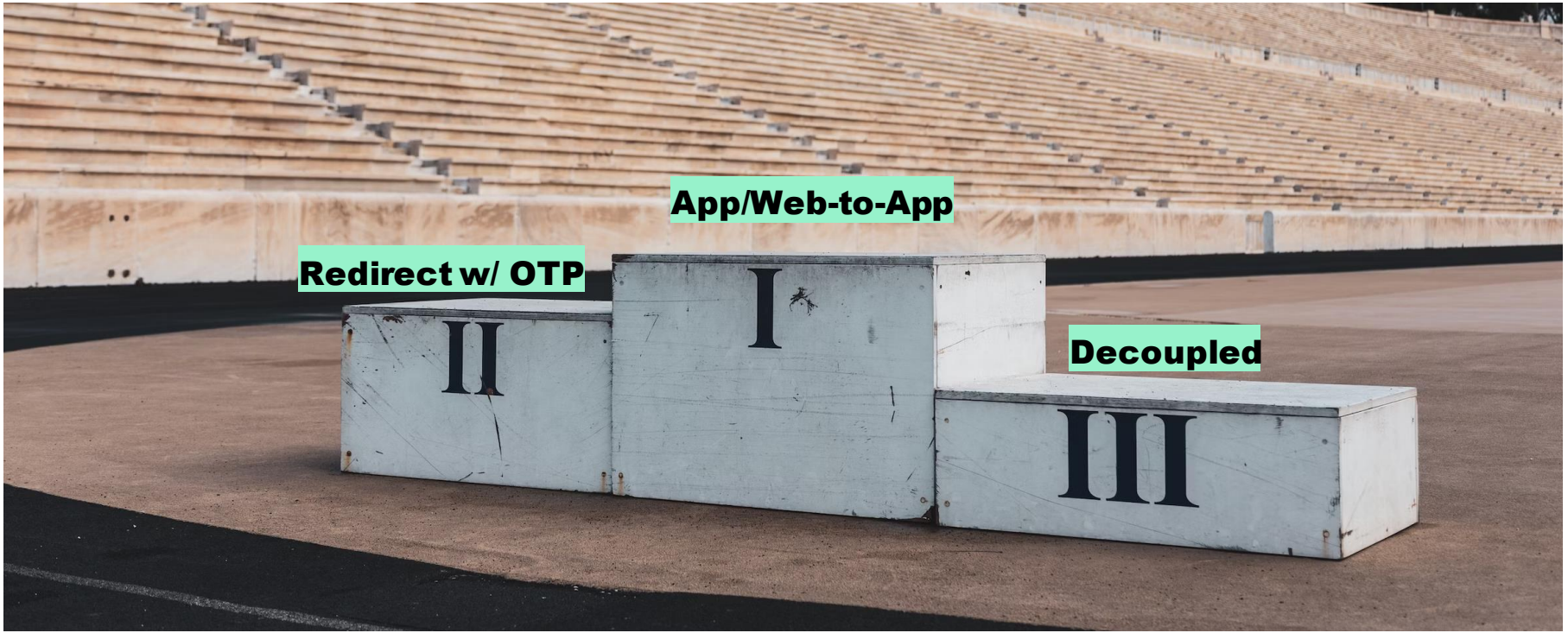
	ONE TIME PASSWORD			APP/WEB 2 APP			DECOUPLED		
	Moderated	Unmoderated	Combined	Moderated	Unmoderated	Combined	Moderated	Unmoderated	Combined
Recall & input	3.93	4.08	4.01	4.02	3.83	3.93	3.88	3.63	3.75
Familiarity & completion	3.73	3.39	3.56	3.95	3.72	3.84	3.52	2.98	3.25
Comfort & control	3.97	3.08	3.53	3.54	3.94	3.74	3.48	3.56	3.52
Purpose & outcome	3.97	3.08	3.53	3.46	3.60	3.53	3.39	3.33	3.36
Expectations	4.10	3.25	3.68	3.35	3.77	3.56	3.62	3.58	3.60







Outcomes



Uplift Approach

Where to from here?

Opportunities Identified

We are consulting on how to introduce support for the following:

Harden the OTP redirection flow	Introduce the App2App flow with LoA2 authentication method support	Support Decoupled Authentication flows with LoA2 and MFA	LoA3 authentication method support / FIDO standardisation / Step-Up authentication / Risk based control framework

We are proposing an initial focus on OTP Redirection and App2App, followed by Decoupled w/ LoA2 and MFA along with LoA3, FIDO, Step-Up, and eventually a risk-based framework.

We want to consult on phasing approach and options within phasing – *how we get there and what we're defining at each stage.*

Thank you

The DSB welcome any questions from the community.

Data Standards Body

Website	consumerdatastandards.gov.au
Zendesk	cdr-support.zendesk.com/
Github	github.com/ConsumerDataStandardsAustralia

DATA STANDARDS BODY