CX GUIDELINES VERSION 0.9.5 AND PHASE 2 NAB FEEDBACK

Summary

- The guidelines are thorough, well communicated, and surface key considerations that are important to individuals.
- Mandatory and recommended requirements are a welcome and appreciated addition.
- There's mixed and unclear messaging on whether or not fine-grained consent is mandatory. The design clearly shows it, but the standards do not support it. NAB is supportive of fine-grained consent.
- De-identification within duration as presented here will not be understood well. This should be explored as a separate step.
- The overall amount of information that's presented to users in the UI is quite overwhelming, particularly on the data recipients' side.
- The research into Consent management and revocation brings up a lot of informative considerations, but there's a lot here that can't be done due to standards not accommodating for it. Next week's workshop can be used to converge thinking and settle on an MVP.

Consumer experience guidelines Feedback

Page, requirement, or prototype, or item	**Feedback**
Generally	
Information quantity	There are quite a lot of steps involved, particularly in the DR consent steps, with playback of a lot of information. **Comprehension testing should be considered.** With the amount of information being played back throughout the end-end flow, how much of it is being usefully retained?
Anonymity and use **pseudonyms**, are not addressed.	It's in the rules but we haven't seen any UX around what that means.
Data Language Standards	
Page 25	**Only data cluster language is included** **Language standards as a broader piece** would help to drive consistency. Additional language that can be included for quick reference purposes.

	Language terms (2.6.1) for the steps, i.e. 'Consent', 'Connect', 'confirm', 'Authorise' Confirming actions e.g. 'I consent', 'I do not consent'. Consent management terminology 'Stop sharing' for revoke. **Authorisation scopes** Need to be updated to reflect the scopes defined in v0.9.5 of the CDS API & InfoSec specification - https://consumerdatastandardsaustralia.github.io/standards/#authorisation-scopes
Pre-consent	
1.1.2 - Product value proposition	**The 'should not' requirements can be clarified.** Examples of what not do would articulate this requirement better. We understand it as 'you cannot ask for consent before this consent step' explore.
p7, #3, De-identification within duration p53 *If the data recipient intends to de-identify CDR data during the sharing period they must receive consumer consent.*	It appears that this consent is only capture by the DR. The DH does not get visibility of this and therefore cannot replay this back during the consent authorisation flow. The DH consent authorisation flow should mimic the permissions and consents obtained on the DR side for customer benefit and consistency.
Consent	
2.3.1 - Trust mark	The trust mark is a recommendation, not a mandatory. by allowing participants to choose whether or not they use the mark the **credibility of the mark becomes a question.** The trust mark can only be a mandatory for it fulfil its intended purpose. 'check our accreditation' as opposed to find out more - **better wording accessibility.** There's a lack of visual distinction of the mark itself, hass there been any thought into creating a logo for recognition purposes? Considerations to ensure that the logo cannot be faked or copied should be key.
2.4.1 - CDR value proposition	The example shown does not reflect the mandatories outlined.

2.4.2 -	Can be split into two different recommendations, Our preference for screen reader accessibility is that should be mandatory.
2.5.2	Some use cases will not lend themselves to be able to share data manually. Is there a way to categorise uses cases that don't make sense to provide manually? For example, a lending application needs to be available a manual process, but it’s unrealistic to expect real-time balance aggregation application to have a manual input flow.
2.7.1 and 2.7.2	Recommendation grammar needs to be reworded. The copy provided gives the impression that you need make a manual request to your bank, customers might be confused thinking that they'll need to go to their bank.
p46 *Greater consumer control may also include actively consenting to the specific uses or allowing consumers to amend the sharing duration both* ***historically (in the past)*** *and into the future*	I don't know what this actually means. How can you amend the sharing duration into the past? What implication does this have of the data to be shared?
p46 *Consultation and research have indicated that fine-grained consent will be needed within the regime*	This is not supported by the CDS API and InfoSec v0.9.5 specification.
p40 *Recommendations: Allow consumer to define the duration of accessing the data history that suits them.*	This is not supported by the CDS API and InfoSec v0.9.5 specification.
2.8.1 - Data request - Data clusters p46, p48 *If data is being requested for multiple uses, the consumer must be able to* ***specify which uses they consent to.***	**This is fine-grained consent; this is not supported by the CDS API and InfoSec v0.9.5 specification.** Data recipients should only be asking the minimum possible data set that will enable them to provide their service. CDR Rules 4.10(3), 4.16(3) state that ADRs 'must allow the CDR consumer to actively select or actively specify which types of CDR data they are consenting to...'

Achieving the above may involve using various consent capture design patterns that allow consumers to opt-in such as checkboxes, toggles, and binary yes/no choices. p49 *The data recipient must allow the consumer to actively* ***select or*** *actively* ***specify those specific uses they are consenting to****.* *The data recipient must allow the consumer to actively* ***select or*** *actively* ***specify*** *the types of data and* ***the uses they consent to****.* *If data is being requested for multiple uses, the consumer must be able to* ***specify which uses they consent to.*** p52 *The data recipient must allow the consumer to actively* ***select or*** *actively* ***specify those specific uses they are consenting to****.*	What's the intent of this design? As a user, should I be selecting a cluster and that I'm okay sharing and if a cluster is not selected, would result in error scenarios saying that all clusters must be selected to be able to consent to data sharing. **Visibility of selection.** How can DH get visibility of this choice? The DH consent authorisation flow should mimic the permissions and consents obtained on the DR side for customer benefit and consistency. **Is this a recommendation for future work, rather than the 0.9.5 standard?**
2.8.1 - Data request - Data clusters - Switches	Is there any rationale that's been given to switches being included in the design? I know this is up to DRs and DHs to decide but the presented switches don't have a very distinct unselected state compared to their selected state. Accessibility standards would not be met with this design choice mainly based on colour contrast.
2.8.1 - Data request - Data clusters - accordions	There's a high density of interaction in a small area, consider moving the show full list accordion below the 'why we need it'.
2.7.1 *The data recipient must ask for the consumer's consent to collect and the selected or specified data. Consent cannot be inferred or implied.*	Recommendation grammar needs to be reworded.

2.7.2 *'Selecting "I consent" won't give us access to your data, you **will need to ask your bank to share your data with us**' That's the next step.*	The copy provided gives the impression that you need make a manual request to your bank, customers might be confused thinking that they'll need to go to their bank.
p52 *The data recipient **must** outline how often data is expected to be collected over that period.* p74 *The data holder **must** state how often the data will be disclosed over the specific period.*	Does this mean DHs need to know if DRs will be accessing data in response to consumer's directly using the DR's service (e.g. attended traffic), which is different to DRs accessing data in the background / batch (e.g. unattended traffic)? If so, then this is not supported by the CDS API and InfoSec v0.9.5 specification.
2.12.1 - De-identification within duration	This concept is very hard to understand, and we believe it would confuse user more than they are already confused. Look at software installation flows, this is similar to asking for users to participate in helping to improve the product through collection of data on how to he software is used. **It's contradictory to requirement 1.1.2 -** 'The data recipient must not bundle consent with unrelated purposes.' The use of de-identified data being used for analytics or other undefined purposes other than would fall under that Linking off to documentation around defining de-identified data is also **contradictory** to **CDR rule 4.16(2)(c)**. *'When asking a CDR consumer to give their consent for the purposes of paragraph 4.3(1)(b), an accredited person: must not include other documents, or references to other documents, that reduce comprehensibility'*
Authenticate	
3.1.1 - Forgotten password link	Messaging is not reflective of examples, forgotten password links shouldn't exist as there is no password input, it might be a recovery flow for forgotten Customer IDs.
3.1.2 - Mandatory ADR not asking for passwords	This can be more prominent; disclaimer text is naturally dismissed.

3.3.2 - One Time Password instructions	'ADRs will never request your password' messaging should be on the first step of authentication. before OTP validation. it's a double up of messaging on the previous step,
3.3.3 - OTP code must expire	Shown is an example of a countdown timer in the UI, Is this a recommendation? The time limit proposed is 10:00 minutes, that is traditionally far too long. Can there be an example that is more aligned with the InfoSec stream.
p67, OTP Guidelines	Will there be any other guidelines around the number of incorrect attempts allowed for OTP authentication? What about the number of times the OTP can be requested to be resent? The following is probably for DH to decide: Can resent OTPs have the same code or different codes? Are all codes received valid?
Authorise	
4. Authorise steps - Account selection - then Confirmation	There is no rational for the order of the steps, is the order a mandatory or requirement?
4.1.2 - Trust mark	See 2.2.1 feedback
4.2.1 - Select accounts from which they will share data.	This should be a mandatory requirement if account data is being shared.
p71 *Data holders should provide exemptions for vulnerable consumers with joint accounts that can be triggered at the account selection stage. Such exemptions should prevent other joint account holders from being notified when a vulnerable consumer shares their own data.* *Data holders should allow consumers to notify the data holder if they are vulnerable and/or at-risk **during the authorisation flow**.*	Is this saying that someone can share a joint account data without all joint holders agreeing to it, in situations where the initiating joint holder is a vulnerable customer? How do we stop abuse of this? Perhaps all sharing under this flow would be manually reviewed by the data holder?

4.4.4 - how your data will be shared	Labelled in description as a single collection, but the diagram is for ongoing collection
4.5.1 - Where to review this arrangement also applies to 2.14	The language of 'arrangement' is introduced, can this be a word that has been used before to simplify and be consistent. e.g. you can review this 'consent'. **We should minimise introducing language as much as possible.**
4.6.1 - Final affirmative action	It's recommended that the final affirmative action redirects users back to the data recipient, but there's no indication this will happen at this point.

Manage and Revoke

Page, requirement, or prototype, or item	Feedback
Engagement, output, and expectations going forward. p.2	The research piece was intended to inform early implementations of the CDR framework. The considerations very informative and forward thinking, How much the recommendations can we expect to actually translate into UX and standards that can be implemented?
'Your data' dashboard - Data holder dashboard	DRs can have multiple consents to one DH relationships, as demonstrated in the research, **they key information is not the account that's shared - it's the capability/feature that it enables.** listing out the account that is shared is not realistically informative. features can be have multiple accounts to one consent relationship (A list of 100 accounts shared is not realistic or informative to display) **Consider labelling the feature the consent enables as a more informative identifier.**
'Data I'm sharing' - Data holder dashboard	This is not supported by the CDS API and InfoSec v0.9.5 specification.
Recommendations for Centralised Consent management	Outline this for future phases.
Revoke consent language	There's inconsistent language, align with recommendations.

Revoke consent flow	**It's 6 steps to stop sharing my data**. This feels like unnecessarily long and a way to increase dropouts or prevent revocation of data. This might be fine for DRs, but DHs should make it as easy as possible to revoke consent.
Supporting Third parties	DHs will have no visibility of this. Redirection to revoke from a DR is unnecessary.
History of data access	We've seen mentions of an access history or log type feature, we haven't seen any concept work for it what that look like.
Raising disputes and who to contact	We would like to see what kind of workflows need to be thought about from an end-to-end experience.

Authenticate notify & reauthorise feedback

Page, requirement, or prototype, or item	Feedback
p40 *Recommendations: Allow consumer to define the duration of accessing the data history that suits them.*	This is not supported by the CDS API and InfoSec v0.9.5 specification.