ANZ welcomes the opportunity to provide feedback on Decision Proposal #327, focusing on the first phase of the authentication uplift for the Consumer Data Right (CDR).

ANZ is broadly supportive of many of the recommendations outlined in this Decision Proposal, however suggests that more focused working groups are established given the complexity of the recommendations proposed.

ANZ is not supportive of requiring LoA3 or above. This requirement conflicts with the requirement for "Data Holders may only support authenticators commensurate to their existing digital channels to ensure there is consistency across channels". To require LoA3 or above has the potential to introduce friction in the Customer Experience as it may cause misalignment across a Data Holders' channels.

Our recommendation is to support option 2, requiring LoA2 or above for Phase 1, which would unblock the existing limitations on Data Holders' ability to roll out authentication controls that are aligned with their existing digital channels and aligned to their strategic objectives.

Consultation Questions

1. Are there any reasons, or scenarios, when MFA must be required?

ANZ are not supportive of mandating when MFA must be required, particularly under Phase 1 of the uplift. We are supportive of changes which encourage the use of MFA and are supportive of Data Holders implementing authentication controls that are aligned with their strategic objectives and risk appetite.

2. Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?

ANZ prefers the Data Standards align with global NIST standards.

3. Where retention of TDIF is supported, are there any clauses in the TDIF role requirements that should not or must not apply to the Data Standards?

As above, ANZ does not support retaining TDIF references.

4. Are there any specific accessibility requirements that should be considered in addition to the success criteria 3.3.8 and 3.3.9 of the WCAG 2.2?

ANZ believes further consideration is required on the potential impacts and requirements around accessibility (eg. Fallback options when biometrics cannot be utilised).

5. What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why?

ANZ supports how this is currently represented in the standards, and otherwise should be left to Data Holders to align with their other digital channels.

6. Should email-based OTP delivery be classified as a Restricted Credential list in accordance with NIST guidance for either or both online and offline customers?

ANZ is not supportive of this as it may limit a Data Holder's ability to authenticate customers in a way that is aligned with their existing digital experience.

7. Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?

ANZ is not supportive of this as it may limit a Data Holder's ability to authenticate customers in a way that is aligned with their existing digital experience.

8. How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?

As above, ANZ does not support retaining TDIF references.

9. Should the Redirect with OTP flow require a second factor of authentication, including for offline customers?

ANZ is not supportive of this being considered for Phase 1. Consideration of this would better align with Phase 3.

10. Should OTPs be only delivered to a channel the customer has already established to receive authentication secrets?

ANZ is supportive of this.

11. Is it reasonable to require Data Holders to support preferred interaction flows, such as App2App, where the Data Holder is dealing with an online customer who has the DH app installed?

ANZ believes it is not reasonable to require Data Holders to support this under Phase 1. This requirement would be based on feature assumptions with Data Holders that may not exist, and may not be consistent with their approach to customer authentication. Similar to the approach for the recommendation in 5.1, ANZ believes this should not be a restrictive requirement but made available as an option.

12. Are the dates proposed for Phase 1 achievable?

ANZ believes that the dates proposed are not reasonable when taking into account the complexity of these changes, and the significant consultation still required prior to any build work being able to be commenced.

13. Do you propose any other enhancements to the uplift of authentication for the CDR?

None.

14. Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?

ANZ is not supportive of NFRs being defined in this context. These would be dependent on the authentication methods being used by different Data Holders, and may not provide any meaningful benefit when weighed against the security uplift being sought. Further consultation is required to ensure any proposed NFRs achieved their purpose.

15. Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?

ANZ believes further consultation on any proposed service level agreements is undertaken to ensure they achieve the purpose for which they are defined.