## Decision Proposal 327 – Authentication Uplift Approach

CBA welcomes the opportunity to provide feedback on Decision Proposal 327 (DP327).

CBA's view is that several the proposals made in this Decision Proposal extend beyond the scope of the Consumer Data Right (CDR) Legislation. For example, where there are gaps between the DSB's proposed CDR identity assurance requirements and existing bank practices, this may require data holders to re-verify the identity information of existing customers (i.e. KYC) outside of the CDR. The Data Standards should instead defer to existing legislation and business practices.

Further, given separate legislation is being proposed to regulate Digital Identity systems, CBA understands the intent of the Australian Government is to maintain Trusted Digital Identity (TDI) and the CDR under separate regimes. Key concepts regulating the operation of a viable digital identity ecosystem, such as identity proofing levels and the roles of attribute provider (as opposed to identity provider), which are currently absent from the CDR rules and standards, would require significant redesign and build to incorporate these concepts into the CDR, at a high ecosystem cost. Further, Identity Proofing and verification are broader industry practices, for example for customer due-diligence assessments conducted under the Anti-Money Laundering Counter-Terrorism Funding (AML/CTF) Act and international frameworks such as NIST. Consequently, the CDR is not the appropriate regime to regulate these practices and related technical standards.

Given the broader policy and regulatory implications of the proposed changes to the Data Standards, CBA recommends these issues should be tabled at a policy level by Treasury and the ACCC and undergo formal consultation.

### Section 5.1 Levels of Assurance

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

The use of MFA and/or 'step-up' authentication should be at the discretion of data holders and commensurate with other risk-based controls implemented by data holders in their primary digital channels.

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

CBA recommends alignment of the Consumer Data Standards to the NIST Authentication Assurance Levels (AALs), as it allows greater flexibility in implementation, given banking data holders operate within a tightly regulated environment.

CBA opposes reference or alignment to TDIF Credential Levels in the CDR Data Standards. The CDR Data Standards should not impose Identity Proofing standards on data holders. Identity Proofing levels and requirements under TDIF are specifically designed for Digital Identity services.

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?*

CBA does not support the inclusion of TDIF role requirements in the CDR Data Standards. Introducing TDIF role requirements, e.g. identity proofing and credential management, directly into CDR standards adds unnecessary regulatory burden on top of existing and emerging banking sector regulatory obligations (i.e. AML/CTF, TDIF).

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

Based on CBA's current assessment, no additional accessibility requirements need to be considered at this time.

## Section 5.2 Restricted Credentials

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

Customer authentication is an existing customer process and, in the banking sector, is regulated via principles based, outcome focused standards and guidance from APRA, specifically CPS234 and CPG234. Authentication standards should not be regulated within CDR, particularly in a prescriptive manner. CDR specific constraints on authenticators and authentication channels may require data holders to deploy authentication methods across existing channels and other instances of authentication for non-CDR activities, which will increase cost and complexity across the ecosystem. CBA recommends that authentication requirements not be prescribed within the CDR and instead defer to industry standards.

In CBA's view, based on current technology, the 'x2App' authentication method provides the most secure consent flow, addressing the regulators aim of reducing drop-out rates. CBA recommends that a 'x2Web' redirect to a single factor web login page not be enabled due to the greater risk of fraud (phishing). Instead, CBA recommends that the existing One Time Password (OTP) authentication method be preserved for customers who do not use data holder digital apps.

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. Which options outlined in this paper do you support?*

CBA is supportive of email-based OTP delivery being classified as a Restricted Credential list in accordance with NIST guidance for both online and offline customers, based on the assumption that OTP is retained for customers who do not use data holder digital apps, per our response to Question 5.

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

CBA is supportive of SMS-based OTP delivery being classified as a Restricted Credential list in accordance with NIST guidance for both online and offline customers, based on the assumption that OTP is retained for customers who do not use data holder digital apps, per our answer to Question 5.

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

The use of Restricted Credentials must be limited to 'read only' consent flows. CBA supports all four of the requirements referenced in the question. However, CBA recommends the standards directly reference the upstream NIST Special Publication, SP 800-63B rather than section 4.3.9 Restricted Credentials of TDIF.

## Section 5.3 Uplift the 'Redirect with OTP' flow

9. *Should the Redirect with OTP flow require a second factor of authentication, including for offline customers? An example may be introducing an additional PIN code secret that is established for CDR data sharing purposes.*

CBA supports maintaining the existing OTP flow for customers who do not use banking apps and does not believe that additional friction is currently needed for read access use cases. The Redirect with OTP flow should be re-assessed in the context of action initiation at which juncture CBA recommends that all CDR consumers be required to leverage an x2App flow.

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

CBA supports delivering OTPs to an authenticated, protected channel as defined in NIST SP800-63B Digital Identity Guidelines.

## Section 5.4 X2App (Web2App and App2App) Interaction Flows

11. *Is it reasonable to require Data Holders to support preferred interaction flows, such as x2App, where the Data Holder is dealing with an online customer who has the DH app installed?*

CBA is supportive of the decision flow proposed in Figure 2 on the assumption that the fall-back to an OTP web redirect will only support non-app customer consent flows. Further to our response to Question 1, CBA recommends a principles-based approach allowing data holders to leverage processes and controls for 'step-up' authentication methods in line with broader business practices.

## Section 5.5 Transition Roadmap: phasing in of authentication uplift obligation

12. *Are the dates proposed for Phase 1 achievable?*

CBA suggests an obligation date of 18 months from the date of endorsement of the CDR Data Standards by the DSB Chair for Phase 1. The proposed compliance date of 11 November 2024 for Phase 1 is not achievable given the existing pipeline of ongoing CDR compliance and change delivery.

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

To support consumer trust and safety in the CDR ecosystem given the extent and nature of data shared by consumers, commensurate authentication uplifts should be implemented on ADR platforms.

## Section 5.6 Transition Roadmap: phasing in of authentication uplift obligation

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

Further to our previous responses, it is not pragmatic to prescribe authentication methods and associated performance requirements within the CDR given the scale of non-CDR banking services and customer expectations of their existing digital banking authentication experiences.

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

Based on our current assessment, CBA believes that the existing service level agreements (SLAs) for CDR services remain appropriate. It is not necessary for separate SLAs to be defined for authentication methods, particularly in circumstances where authentication flows for CDR and a data holder's digital channel are the same.

In conclusion, CBA submits our feedback on DP327 Authentication uplift Phase 1 for consideration by the DSB. We look forward to further engagement and consultation as identified in our responses. Thank you for the opportunity to provide feedback.