16 October 2022

Rules Unit
Consumer Data and Digital Division
Treasury
Langton Cres
Parkes ACT 2600

Via email to data@treasury.gov.au

Classification Public

Re: Cuscal response to the Consumer Data Right rules – expansion to the telecommunications sector and other operational enhancements.

Cuscal Limited (Cuscal) welcomes the opportunity to respond to the Treasury consultation on the Consumer Data Right rules – expansion to the telecommunications sector and other operational enhancements.

Background to Cuscal

For over 40 years, Cuscal has leveraged our assets, licensing, and connectivity to provide intermediary and principal outsourcing activities on behalf of our clients. We are an end-to-end payments specialist that services more than 100 established ADI and challenger brand clients within Australia's financial system, including the majority of the mutual banking sector and a growing number of FinTech and 'PayTech' enterprises. We enable their market connectivity so they may provide innovative products and business models and drive improved customer outcomes.

We are an Authorised Deposit-taking Institution (ADI), an Australian Financial Services Licence holder, an Australian Credit Licence for Securitisation purposes and an Accredited Data recipient. Cuscal has Board representation with Australian payment plus, NPPA, and Australian Payments Network and participates in numerous industry committees. We are also the founder of 86400 (rebranded to ubank, *https://www.ubank.com.au/*), a fully licenced mobile-led digitised bank acquired by National Australia Bank.

The services that we provide to our client institutions include card scheme sponsorship for issuing and acquiring, payment card issuing, card production services, digital banking applications, access to domestic payment services using direct entry, BPAY, the New Payments Platform (NPP) and Open Banking Data holder services. We also act as a settlement agent for many of our clients through our Exchange Settlement Account with the Reserve Bank of Australia (RBA).

As a fully PCI-DSS accredited ADI, Cuscal is uniquely placed to provide secure and robust capabilities that facilitate access to markets that would otherwise be beyond the reach of some organisations.

Cuscal Role in Open Banking

To help our clients benefit from the CDR while minimising their costs and risks, Cuscal has invested in technology platforms to provide Data holder services and Data recipient services to our clients. This investment will position Cuscal as a CDR intermediary that helps each of the three CDR participants obtain the most out of the CDR:

- Data Holders clients can manage compliance effectively.
- Consumers can share their banking data with best-practice simplicity while remaining in control over the data they consent to share via their bank.

- Data Recipients clients can create better digital services, enabled by the data that consumers consent to share, but minimising the time, cost, and risk of doing it themselves.

Cuscal has attained accreditation as a data recipient and is dedicated to enabling a broad range of services for our CDR participants. For further information on Cuscal and our services, please refer to our website at *www.cuscalpayments.com.au.*

Cuscal supports the draft rules for the telecommunications sector and the phased implementation approach applied across the Banking and Energy sectors. Cuscal's submission concentrates on the proposed operational enhancements in the Treasury consultation and identifies areas that need further discussions and review by Treasury.

- **Business Consumers: [subrule 1.7(1) definitions] :**

  The amending rules aims to bring Business customers into the fold of CDR for data sharing. The CDR consumer is defined in the *Competition and Consumer Act 2010 under section 56AI (3)*. **The term *"person"* also addresses an organisation with specific legal rights.** It appears that the introduction of a CDR business customer is to try and incorporate a new disclosure consent for business customers and increase the duration of consents provided. The need for such amendments is **unclear** from the Exposure draft explanatory materials. The statement that amendments are proposed to support CDR data sharing for small businesses is not well understood. *Phase 3 banking products have been implemented to serve businesses with complex data-sharing capabilities*.

  Furthermore, there are a number of different categorisations already existing within CDR, such as *"large consumer", "large retailer", large CSP"*, etc. **Consistency in terms and definitions is required to maintain simplification in government policies and legislation.** For example, all types of consumers are captured in the broad definition of a CDR consumer under the *Competition and Consumer Act 2010 – Sect 56AI*. Separate subcategories provide further clarity, such as large retailer and large CSP. Similarly, a subcategory, **Business, or non-individual consumer**, is more appropriate than "CDR Business consumer" to avoid ambiguity in the existing legislation. The existing consent adequately captures the use and disclosure of data for Business and non-individual accounts. ***Hence the introduction of a new CDR business consumer disclosure consent and a business consumer statement to support data sharing for a business consumer lacks purpose in the existing provisions of the legislation.***

- **Extension of Consent duration for Business and non-individual Consumers:**

  Cuscal believes that the extension of Consent duration is likely to **bind** a Consumer with a particular CDR participant as there is currently **no avenue to transfer current consents**. The existing approach, where consent is set to expire at the end of 12 months, provides the required flexibility to CDR consumers (individuals and businesses) to re-consider the service provided to them by an entity and agree on extending the service or cancellation and moving to a different provider. ***Such flexibility is required to protect CDR Consumers from locking in extended contracts with entities they may later find difficult to exit due to the volume of information shared and the complexity of moving under such an arrangement.*** The amendment to extend duration is based on instances where consent is not renewed before the 12-month expiry (refer to Point#50 Exposure draft explanatory materials). This is quite evident that such an extension of 7 years for consent could lead to a set-and-forget state that could lead to unintended consequences for a CDR consumer; for example, the business has since changed name and ownership rights.

- **Disclosure of CDR data to Outsourced Service Providers [Rule 1.10 and 1.10AA (3)]**

  The amending rules propose allowing ADRs to disclose CDR data to a CDR representative to disclose CDR data to a direct or indirect Outsourced service provider of the CDR representative. The objective of amending the CDR model rules is unclear at this stage for below reasons:

  - The disclosure of CDR data to an outsourced service provider is currently applicable under a sponsor/affiliate model. Hence, the current proposal to amend rules for the CDR principal /CDR representative model **makes the sponsorship/affiliate model less attractive, given the levels of security and assurance currently placed on CDR affiliates**. The CDR representatives do not have compliance placed directly on them by a regulator. Any compliance issue will only result in a breach of contract terms with a CDR Principal.

    > *"55. ADRs (and now CDR representatives) may engage multiple OSPs via different CDR outsourcing arrangements. The Amending Rules allow an ADR or CDR representative in multiple CDR outsourcing arrangements to authorise their OSPs to disclose CDR data directly to one another, which is more efficient than requiring the CDR data to be disclosed back to the ADR or CDR representative by one OSP to be on-disclosed to the second OSP."*

  *The above scenario from Treasury's Exposure draft indicates CDR participants are **unclear about the existing CDR models** and how they should be constructed for consumer benefit.* Such arrangements are available under a CDR sponsorship model, and the CDR representative model is **inappropriate** for sharing data with Outsourced service providers.

  - The CDR representative is not permitted to enter another CDR representative arrangement [rule 1.10 and subrule 1.10AA (3)]. And the CDR Principal is held liable for non-adherence to regulatory and compliance requirements. *With multiple CDR representative arrangements and the inclusion of multiple direct/indirect outsourced service providers handling CDR data under a contractual agreement, the proposed model is set to **fail** as it will have a cascading effect should one entity fail to meet contract terms.* For managing high liability in a regulated ecosystem, **the financial viability of CDR principals** must be assessed to ensure consumers can be compensated in the event of data loss similar to the one we have seen in recent Cyber-attacks in Australia. In Cuscal's view, the government should exercise caution in removing all barriers to entering the CDR ecosystem, as it could lead to **inadequate consumer protections** in a data economy that is continually faced with cyber threats.

  - Cuscal agrees to extend the Privacy safeguards to entities handling CDR data (including outsourced service providers). In addition, the **Privacy Act 1988 do not apply to most small businesses**, and as such, there are **no safeguards** for consumers concerning such sharing arrangements where third parties are involved.

  - The issue raised by Treasury under point#69 of the Exposure draft explanatory materials:

    > *"a similar requirement to the one set out in paragraph 65 above should apply to an accredited person if one or more of their CDR representatives is likely to disclose CDR data to a direct or indirect OSP based overseas and is not itself an accredited person. If this change is not made, the information will be available in an ADR's CDR policy concerning their own OSPs but not about the OSPs of their CDR representative(s) (noting*

that CDR representatives do not have their own CDR policy but are required to provide CDR consumers with the link to their ADR's CDR policy)."

The proposed rules amendment is **not required** as the current CDR sponsor/affiliate model already caters for sharing with an outsourced service provider and **has required regulatory protections** with respect to consumer data privacy and safety. The proposed model to allow disclosing CDR data by an unaccredited CDR representative to direct/indirect Outsourced service providers within/outside Australia is **not balanced** and **undermines** the regulatory protection available under other CDR data sharing models.

- **1.15 Consumer Dashboard – Data holder – inclusion of additional feature:**

Rule 1.15 Consumer Dashboard – subsection (2AA) refers that the consumer dashboard may also include functionality that allows a CDR consumer to request to disclose corrected CDR data. The current flow of data in CDR is **not aligned** with this specific requirement and will add **unnecessary technical complexity** to a complex ecosystem.

- The data flow commences with a CDR consumer providing valid consent to an accredited data recipient for the collection of CDR data. The above requirement for a data holder indicates that a CDR consumer should be able to initiate corrected CDR data to an accredited data recipient. This request has **no associated consent**, so reconciliation at the accredited data recipient end will be challenging.
- The process could create duplicate transaction records for an accredited data recipient as there is no corresponding data collection request.

In Cuscal's view, the logical approach will be for an accredited data recipient to request sharing of corrected CDR data under rule 1.14 (2A) and for the data holder to respond with the corrected CDR data.

- **Point #102 Record keeping of Complaints data:**

Cuscal agrees with including the Complaint data as part of record keeping and accessible to consumers. Furthermore, the current record-keeping requirements are for a period of 6 years. **Cuscal recommends increasing the duration of record keeping from 6 to 7 years aligned with financial record-keeping requirements under ASIC, AUSTRAC, and APRA**. This will support alignment with other legislative requirements and frameworks as CDR expands into other sectors and considers action initiation.

We trust that our above responses help Treasury finalise the draft amendment rules and ensure the regulatory standards are superior in the CDR ecosystem.

Yours sincerely,

Kieran McKenna
Chief Risk Officer