1 Margaret St
Sydney NSW 2000

GPO Box 4720
Sydney NSW 2001

TEL (02) 8299 9000
FAX (02) 8299 9600

Cuscal
The complete payments partner

10 May 2019

ACCC Consultation Hub
Australian Competition & Consumer Commission
175 Pitt Street
SYDNEY NSW 2000
Via: ACCC-CDR@accc.gov.au

Submission by Cuscal Limited in response to Consumer Data Rules.

Cuscal Limited (Cuscal) welcomes the opportunity to provide feedback on the Exposure Draft of the Competition and Consumer (Consumer Data) Rules 2019 (Rules).

Cuscal is an end-to-end payments provider that services more than 100 established and challenger brand clients within Australia's financial system and payments landscape, including the majority of the mutual banking sector. We are an Authorised Deposit Taking Institution and also hold an Australian Financial Services Licence and Credit Licence. We are also the founder and owner of 86400 www.86400.com.au who are also submitting similar commentary on the Exposure Draft.

Our services that we provide to our client institutions include: card scheme sponsorship, card issuing, card production services, merchant acquiring, ATM fleet management, digital and mobile banking platforms, and access to the New Payments Platform (NPP). We also act as settlement agent for many of our clients through our Exchange Settlement Account with the Reserve Bank of Australia (RBA). We process approximately 16% of Australia's electronic transactions.

Cuscal also works closely with small and large fintech companies seeking access to the Australian payments ecosystem. We enable their market connectivity so they may provide innovative products, business models, and drive improved customer outcomes.

For further information on services Cuscal provides, please refer to our website at www.cuscalpayments.com.au.

We have set out below our key comments regarding the Exposure Draft.

1. Process for the Data Holder to validate the status of an Accredited Data Recipient.

We would expect that (technically) this would be achieved by the register exposing an API to Data Holders. It may be the intention for this to be included in the Data Standard on "the processes for making product data requests and consumer data requests" but we think it would be useful to include a section within Division 5.3 of the Rules outlining the Registrar's responsibility in this regard.

2. Mechanism for Data Holders to ensure continued accreditation status of Accredited Persons.

The draft Rules provide detailed processes for the suspension and revocation of accreditation but they do not provide a process for communication of register updates to Data Holders. This is significant where customers has provided consent for a period of time. We would expect that the Registrar would need to make available an API or a regular file to Data Holders (at least daily) against which the Data Holder could wash its consents, to ensure that it does not continue to provide data to recipients who are no longer accredited.

We suggest that the Rules include a communication process for updates to the register.

3. Multi Party Disputes

We can envisage scenarios where consumers believe that a data breach of some kind has occurred but it is unclear whether the party responsible is the Data Holder or the Accredited Recipient (or its outsourced provider). In those circumstances there does not appear to be a mechanism to assist with dispute resolution. We would suggest that there be some obligation on participants to assist each other with dispute resolution and perhaps some instruction for consumers on their initial avenue of complaint.

4. Mechanism for Data Recipient to gain access to data from the Data Provider.

Technically each Accredited Data Recipient will need to be allocated authorisation credentials by each Data Provider from which they seek access. The Rules do not currently provide for this and the proposed classes of Standards within Clause 8.1 do not appear to cover this mechanism. We would strongly suggest that the rules should include an appropriate mechanism.

5. Interactions between Parties

We note that proposed S56D of the Act binds all participants to the Data Standards as if they were part of a multilateral contract. We think it appropriate therefore that the Standard provide certain details for the interaction between those parties. In particular:

i) Service Levels:
We note there are references to the Data Standards in respect of responses to customer data requests. We would expect that service levels be established for these responses within the Standards. We think that the Rules should cover the rights of a consumer for a failure to meet those service levels.

ii) Support for enhancement to API's:
We would expect the Data Standards to cover API enhancements and the requirements for Data Holders to support current and recent API versions.

iii) Mechanism for Data Recipient to gain access to data from the Data Provider:
Technically each Accredited Data Recipient will need to be allocated authorisation credentials by each Data Holder from which they seek access. The Rules do not currently provide for this and the proposed classes of Standards within Clause 8.1 do not appear to cover this mechanism.

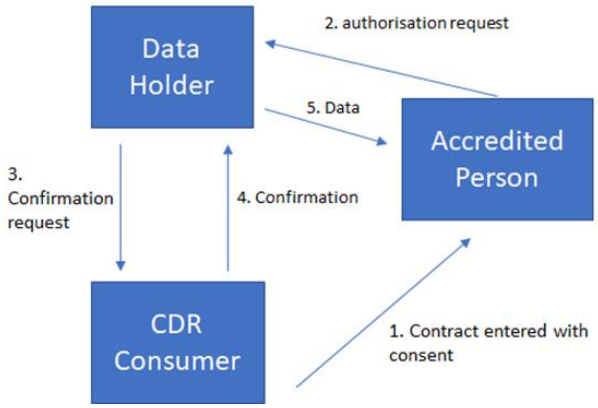
iv) Establishment of different API end points to support CDR:
Data Holders will need to establish different end points for API's depending on whether the Data is Product data or Consumer Data. We would expect the Standards to provide details of these. Product Data may not require any credentials to be passed, while Consumer Data will.

6. Consent Expiry and Renewal (Rule 4.12)

Under Rule 4.12 consumer consents expire after a maximum of 12 months. There is no mechanism in the Rules for the renewal of consents, so that a renewal would need to follow the original consent process. We do not think that is an efficient or desirable outcome for customers in the context of a continuing service which the customer has requested (e.g. the display of aggregated transaction details).

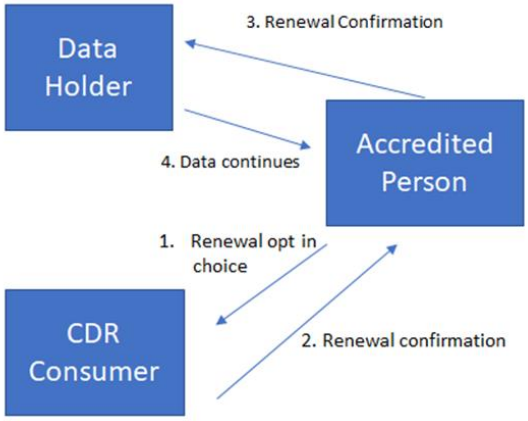
Figure 1 below illustrates the initial proposed consent process.

Figure 1 . Initial consent process (per exposure draft)



While we accept the reasoning for customers to update their consent, we believe that such updates are more efficiently transacted by the customer directing their service provider (or Accredited Recipient) to confirm their consent with the Data Holder. This overcomes the need for another interchange between the consumer and the Data Holder. This proposed alternative is depicted in **figure 2** below.

Figure 2 . Suggested consent renewal process



The consumer will have provided their initial consent directly to the Data Holder, so when the Data Holder receives the renewal request it can still be satisfied that it is a legitimate renewal instruction from its previously identified customer.

Given that the Accredited Recipient is subject to stringent accreditation requirements, we think it reasonable that they be trusted to accurately pass on an individual's renewal of consent without the Data Holder having to reconfirm that consent.

We note that the consumer will be able to view their consents on both the Accredited Person and Data Holder dashboards and be able to withdraw consent any time.

7. Notification of current consent each 90 days (Rule 4.14)

We think that the Rules could specify what is meant by customer notification. For example, where a customer is a regular user of an account aggregation service, we believe it is intrusive for the service provider to have to remind the individual by email or SMS of their consent each 90 days. We think notification for an ongoing consent should be satisfied by:

i) the Accredited Person displaying the user's consent status as "current" on a home page or access point for the service; and

ii) Notifying the user by SMS or email if the user has not used the service for 90 days.

8. Joint Accounts (Part 3)

In relation to joint accounts, we would note the following extract from *Review into Open Banking* (December 2017, page 82) which was aimed at providing customers choice, convenience and confidence,

> **Recommendation 4.7 – joint accounts**
>
> Authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from the joint account. Each joint account holder should be notified of any data transfer arrangements initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

We think that the draft rules covering joint accounts are confusing and potentially conflicting and, if our interpretation of them is correct, will not provide a desirable outcome for consumers, as indicated in the Review report.

3.1 (1) of the draft Rules (page 89) gives each joint account holder the ability to make data requests and provide or revoke authorisations. Rule 3.2 allows the Data Holder to provide the functionality for joint account holders to perform those items together. We cannot see why a Data Holder would provide that functionality when they are always required to act on the instructions of a single joint account holder.

In our view the rules governing joint account holders should be consistent with the authority which the account holders have provided the Data Holder to operate their account (Authority to Operate). Typically, ADI's will designate accounts as "both to operate" if the Authority to Operate requires both parties to initiate or authorise a transaction or "either to operate" if either party can initiate or authorise a transaction.

We think that a "both to operate" instruction reflects the intention of the consumers to require both of them to be involved in important decisions involving their account. We submit this should extend to CDR requests and authorities, however either party should be permitted to revoke an authorisation.

We recognise that this alternative could make implementation of a CDR consent management solution quite onerous and consideration may need to be given for "both to operate" joint accounts to be excluded from the definition of "required consumer data". That exclusion would affect a minority of joint accounts.

We hope that these comments have been useful and would be happy to provide further explanation if that would assist the ACCC, please feel free to contact me [redacted] or [redacted].

Yours Sincerely
Cuscal Limited,

Kieran McKenna
Chief Risk Officer.