Mastercard Australasia
Level 8, 100 Arthur Street
North Sydney, NSW
Australia
Tel: + 61 2 9466 3700
www.mastercard.com.au

Australian Competition and
Consumer Commission
GPO Box 3131
Canberra ACT 2601

Via email: ACCC-CDR@accc.gov.au

17 May 2019

Dear Commissioners

Thank you for the opportunity to comment on the Australian Competition and Consumer Commission's (ACCC) Exposure Draft of the *Competition and Consumer (Consumer Data) Rules 2019*.

As a major participant in the domestic and global payments system, Mastercard is well placed to share insights about using data to drive innovation and greater inclusion in financial services, while protecting the agency and privacy of individual consumers and businesses.

We note that the Treasury Laws Amendment (Consumer Data Right) Bill remains subject to parliamentary review. We are aware of policy concerns from those engaged with the process at the political level, which might mean that there are changes of substance to the Bill assuming it is introduced in the next parliament. As a matter of process the work on the Consumer Data Right has involved several consultations on subordinate rules, at a time when the detail of the enabling legislation is not yet clear. For this reason we can only make comments that are qualified and contingent in nature. And we do not want to make comments that could later inadvertently be misapplied if context changes in the interim.

For these reasons we include in the Annex to this letter a non-exhaustive list of the kinds of issues that we think fall to be considered as the ACCC progresses its work. We hope that the relatively high level approach we take will remain helpful to the ACCC even if there are changes in wider context.

If you would like to discuss Mastercard's position on Open Banking and the Consumer Data Right further, or require additional information, please contact Chris Siorokos, Director Public Policy on [redacted] or via email to [redacted]

Yours sincerely

Andrew Cartwright
Country Manager
Annexure

Data Format

'Human-readable form' and 'machine-readable form' are not explicitly defined, which creates scope for confusion. Under the proposed rules, a data holder can provide CDR consumers with data that is human-readable but not machine-readable, and likewise an accredited person data that is machine-readable but not human readable. This is problematic, for example, in the case of 1.11(3)(a), where product data request service may not be human readable. Moreover, what if the consumer wants to perform his/her own analysis of CDR data, but is only provided with a static image file?

Fees

The document consistently stipulates that "a fee cannot be charged for a CDR consumer making a consumer data request" and "a fee cannot be charged for this disclosure." It is clear this precludes variable fees (e.g., cost per disclosure), but it does not clearly limit platform access, joining, or other fixed fees.

Division 1.3 Interpretation

1.7 Definitions
The 'data minimisation principle' refers to data that is reasonably needed to fulfil a CDR contract. It may be helpful to provide further guidance on what constitutes as "reasonably needed" to assist understanding and the timely discharge of the obligations.

Division 1.4—General provisions relating to data holders and to accredited persons

Subdivision 1.4.2—Services for making requests under these rules
1.12 Consumer data request service (4) (a)
Timeliness should be better defined, as the evolution of Open Banking and customers' expectations means that current-state timeliness may be slower than desirable and therefore not an appropriate baseline.

Subdivision 1.4.3—Services for managing consumer data requests made by accredited persons
1.13(4), 1.14(4)
A disconnect fee has not been expressly excluded. The Rules should explicitly stipulate that the consumer can terminate a contract and/or withdraw without incurring a fee.

Part 4—Consumer data requests made by accredited persons

4.8
The outsourced service provider should be prohibited from using the CDR data for a "prohibited use or disclosure".

Division 4.3 – Consents to collect CDR data
Additional emphasis could be placed on the need for the data minimisation principle to be applied to requests by accredited persons to collect CDR data. Accredited persons should not collect more information than is necessary, and this would help to avoid an undesirable "data maximisation" approach. While this is acknowledged as a note to rule 4.3, elevating the requirement to a rule (similar to rule 4.16(4)) would ensure the principle's prominence and importance in the context of collection.

4.18(1)(a) - Duration of consent to use CDR data
The proposed 12 months may be unnecessarily long (consideration of value-added data services should be taken into account).

Division 4.4 – Consent to use CDR data
The ability to withdraw consent for the use of CDR data should be also made available through the channel of the data holder. The reason is that individual consumers, when withdrawing consent, will likely withdraw consent for *both* collection and use at the same time. As such, if consumers approach their bank to withdraw authorisation / consent under rule 4.24, they are likely to make a combined request which covers both collection and use. However, the current rule 4.24 only relates to withdrawal of authorisation of disclosure, and the consumer would have to separately approach the accredited person for withdrawal of consent for *use*. In order to meet consumer expectations, and to reduce consumer frustration, consumers should be able to withdraw consent for use through the data holder as well.

Part 5. Rules relating to accreditation etc.

5.21 and 7.8(2)
Where an accredited person has their accreditation withdrawn, the current process makes them solely responsible for deleting/de-identifying data. There is no third party verification process of this. We see this as a potential weakness particularly where the accreditation is withdrawn on the basis of mishandling of CDR data; effectively the provider has not demonstrated that necessary trust can be placed in them but is then responsible for putting data beyond further use.

5.2(2)(d)
This says that applicants should indicate only what kind of goods and services they propose to offer to CDR Consumers. An alternative is for applicants to be required to talk about how they propose to use the data provided to them as well as to spell out how they propose to commercialise use of that data. We think this alternative is more robust: for fit and proper purposes (and noting that some applicants might have no prior regulatory status) we think it is important for the Data Recipient Accreditor to be given the whole picture.

5.6 and 5.11
In terms of an accreditation that is "unrestricted" (and particularly given that label) we think it is important (1) to make clear that actual use of the data and/or offering any product based on it remains subject to other regulatory processes including AFSL licensing where appropriate (2) if an AFSL or other regulated status is required having regard to the applicants' plans, this is a condition of any authorisation given by the Data Recipient Accreditor.

Where a person in whose favour a person wishes to exercise their CDR already has specific regulatory status, regard should be had to that status in determining whether any application is in fact required and the Data Recipient Accreditor should be empowered and required to give guidance accordingly. At a general level we see the various controls that exist as primarily going to new categories of services providers.

Part 6

Generally we are unclear how the roles of Data Recipient Accreditor and ASIC inter-relate. ASIC's RG165 contemplates an active role for ASIC in assessing External Dispute Resolution schemes for example. We support an approach which keeps the matter at the level of principle but suggest that a focus be co-ordination on when ASIC will and will not have a role in relation to specific matters e.g. where no specific ASIC licensing is required in respect of the applicants' plans."

Part 7—Rules relating to privacy safeguards

Rule 7.2(4)
The wording may suggest that a CDR participant must always have a website and a mobile app. This may be too limiting and restrictive. That is, the references could limit the technology by which the policy is made available, and may not allow for a policy to be made available through a connected TV display or appliance (which is neither a website nor mobile). We suggest that a more technology neutral approach be adopted through updating rule 7.2(4) as follows:

> *"(4) For paragraph 56ED(7)(b) of the Act, a CDR participant must make its CDR policy readily available to CDR consumers.*
>
> *Note: this could be through websites or an application for a mobile device."*

Rule 8.9(4)
This states that "a failure to comply with this rule does not affect the validity or enforceability of a data standard or an amendment to a data standard". In the interest of accountability and transparency, we suggest that this rule be removed.

Schedule 1

The proper management of data breaches by both accredited persons and outsourced service providers is of critical importance in ensuring trust and confidence in the CDR regime, and to minimise harm to consumers. Further, as the

data would be obtained from the data holder, the data holder retains an interest in ensuring that the exposed data is not used to further harm consumers or the data holder (e.g. data is used to perpetuate a fraud on the data holder, or data is used to create realistic phishing emails which appear to come from the data holder).

In that context, in addition to notifying the CDR consumer and the Information Commissioner, we suggest that subclause 1.7 (Step 5 – Manage and report security incidents) of Schedule 1 could be amended to require the outsourced service provider to notify the accredited person, and for the accredited person to notify the data holder of any CDR data security breach. This will ensure that the data holder is provided with relevant information so that appropriate measures can be taken by the data holder to protect consumers and themselves.

Schedule 2

1.3 - Account Data
"Account data" does not specifically call out inbound payments (e.g. payroll into a cheque account, or paydown of a credit card). It stands to reason that this data is no more sensitive than the other data, and it opens opportunity to improve financial behaviours (e.g. encourage credit card pay-down).

3.2(2) (a) - Joint Consent
Not requiring joint account management services to be digital or online may undermine consumers' interest for expedience and ease of use, as the logical outcome is forms that must be manually completed and submitted to a data holder.