RSM Australia Pty Ltd
Level 21, 55 Collins Street Melbourne VIC 3000
PO Box 248 Collins Street West VIC 8007
T +61 (0) 3 9286 8000
F +61 (0) 3 9286 8199
www.rsm.com.au

29 October 2020

CDR Rules team
GPO Box 3131
Canberra ACT 2601

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

Dear Sir or Madam

Submission to the Australian Competition and Consumer Commission (ACCC) on Consumer Data Right (CDR) Rules consultation paper – CDR rules expansion amendments (September 2020)

RSM welcomes the opportunity to comment on the ACCC's proposed CDR Rules expansion amendments.

About RSM

RSM is one of Australia's leading professional services firms, with a national partnership of over 100 Partners and Principals and over 1,200 staff operating out of 30 offices throughout Australia. RSM in Australia is an independent member firm of RSM, the 6th largest professional service accounting and consulting organisation in the world.

As a registered auditing firm (Chartered Accountants Australia & New Zealand), RSM has suitably experienced and qualified individuals who can complete independent assurance reports in accordance with International / Australian Standards on Assurance Engagements (ISAE/ASAE) as lead information security assurance practitioners (including SOC 1/2 reports).

RSM's experience completing CDR information security accreditation assurance reports

RSM has completed independent assurance reports in accordance with ASAE 3150 – Assurance Engagements on Controls for the CDR information security accreditation of two non-ADI Accredited Data Recipient (ADR) applicants. This experience has provided us with valuable insights on the CDR Rules, including defining the boundaries of the CDR data environment, Schedule 2 Part 1 and Part 2. We would therefore like to highlight the following for consideration by the ACCC:

3.3. Restricted level: affiliate restriction

We support the expansion to include sponsor/affiliate relationships. However, self-assessments are renowned for being a poor indicator of adherence to a control framework due to inconsistent skills and knowledge of those completing the assessment.

To ensure the CDR information security requirements are being implemented consistently for all ADR's, we believe that the sponsor should provide reasonable assurance to the ACCC, as part of the certification, that the affiliate meets the CDR information security obligations. The manner for the sponsor obtaining (and subsequently enabling them to provide) reasonable assurance that the affiliate meets the CDR information security obligations could be determined by the sponsor, providing more flexibility on how assurance is

obtained, whilst still providing the rigour required to ensure consumers are confident that their data is being appropriately protected. The sponsor could therefore investigate more innovative reasonable assurance options like automated continuous assurance or more fit for purpose reasonable assurance audit activities based on risk and complexity (for example, an audit performed under the Institute of Internal Auditor International Standards for the Professional Practice of Internal Auditing). This would help to reduce the cost of entry and participation, whilst still providing consumers with a consistent level of assurance that their data is being appropriately secured.

5.2. Disclosure of CDR insights

The data architecture for securing derived CDR data is one of the most costly and restrictive areas for ADRs implementing their CDR data environment. If insights derived from CDR data are allowed to be provided to any person with a consumer's consent, that derived CDR data is no longer secured in line with the CDR information security obligations. Insights derived from CDR data should therefore not be included in the ADR's CDR data environment for the purposes of the information security controls. To have them included in the CDR data environment results in inconsistent controls being applied between ADRs and 'any person' even though the data has the same privacy impact.

Please do not hesitate to contact me to discuss further.

Regards

Darren Booth
Partner, National Head of Cyber Security & Privacy Risk Services
RSM Australia Pty Ltd