SECURELOGIC

**Australian Competition & Consumer Commission
Consumer Data Right Rules Framework
Consultation 2018**

19 October 2018

Australian Competition & Consumer Commission (ACCC)
Consumer Data Right Branch

Email: accc-cdr@accc.gov.au

Secure Logic appreciates the opportunity to provide input into the *ACCC Consumer Data Right – Rules Framework Consultation*.

We wish to express a number of views for your consideration in the specific areas below:
- Section 6. Accreditation
Topic – Tiers of accreditation

- Section 9. Authentication and Authorisation
Topic – Service level standards for the authorisation and authentication processes

Tiers of accreditation

The introduction of multiple accreditation tiers is important to promote a fit-for-purpose audit framework. A singular, rigorous accreditation program would achieve better compliance in exchange for slower industry progress due to the high barrier of entry, narrowing the pool of organisations who can actively participate in the sector. On the other hand, a multi-tier accreditation program can provide a practical solution to strike the right balance between stimulating the proliferation of industry activity and ascertaining secure, responsible practices based on the applicable risk exposure.

Since the Consumer Data Right (CDR) focuses on the banking industry in the first iteration, we would like to draw upon the Payment Card Industry Data Security Standard (PCI DSS) framework as a sample reference for the development of the CDR accreditation tiers. The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data.

PCI DSS differentiates the breadth and rigor of the audit requirements based on the role of the applicant and their annual transaction volume:
- A Merchant would be required to meet relatively less audit scope than a Service Provider
- Organisations who process high volume of transactions annually would be required to fulfil relatively larger audit scope than those with low volume

Secure Logic recommends the role of the applicant as the distinguishing metric upon which the accreditation tiers can be established: data holder, data recipient and data intermediary. Data intermediary should be characterised by their transient relay-only operational scope which does not store consumer data in any persistent storage facility, be it physical or digital.

API transaction volume should not influence the accreditation tiers in order to provide equal protection of consumer rights for every single interaction involving consumer data.

Service level standards for the authorisation and authentication processes

While we agree that the higher fidelity technical details should be provided by the appointed Data Standards Body in alignment with their remit, Secure Logic recommends that ACCC should stipulate that API performance service levels shall be equally provided to all API consumers, and not subject to a tiered model of service levels which attract incremental fees for higher performance.

At least in the first version of the rules framework, this structure encourages greater adoption and innovation in the core banking and fintech space through a more level playing field. It may be reviewed at a later stage when Open Banking has progressed in volume and maturity.

Secure Logic strongly supports Open Banking in Australia and believes that the rules framework will put consumer's data privacy in the forefront of initiative, enabling a secure and rich ecosystem of future fintech innovation.

Kind Regards,

Santosh Devaraj
CEO of Secure Logic