Submission to Australian Consumer and Competition Commission on Competition and Consumer (Consumer Data) Rules 2019

Exposure Draft dated 29 March 2019

Response by SISS Data Services Pty Limited

Contents

About SISS Data Services

Since 2011, SISS Data Services (SDS) has been providing driving innovation via our direct feed (not screen scraping), and API based data feeds under contract from Australia's largest Banks to both local and international FinTech's.

At present SDS provides over 250,000 data feeds covering 300,000 Australians from a range of Data sources, including Banking, Stock Broking, Manage Funds/Wraps.

Our core experience is Data Source Connectivity, Managing Consumer Consent, API connectivity, Developer Sandbox Access and Third Party (Data Recipient) Accreditation.

Within the current Consumer Data Right (CDR) framework, SDS would fit into the category of an 'intermediary'

Third Party Access (rule 4.8)

SDS request the ACCC provides more clarity around Third Party Access (TPA).

For example, where accredited Data Recipient is an Accounting Software Provider (ASP), and the ASP has its own 'Add-On' environment where Third Party Apps can obtain access to data held by the ASP. When should these Add-Ons be accredited under CDR?

Ideally the accreditation should consider that the Add-On App has obtained explicit consent to access data from the Consumer, and the data they access may include CDR related data.

Intermediaries

While it is noted that the roles of an 'intermediary' are still being formulated by the ACCC, it important to understand the current role of Data Aggregators in providing data to Consumer.

SDS estimates current 'intermediaries' in a pre-CDR/Open Banking environment share data for over 400,000+ accounts. These intermediaries are typically characterised by formal relationships between Data Holder, Intermediary and Data Recipients and provides consumers with a trusted and secure way to share data.

This trusted relationship should continue in the CDR environment.

Should Intermediaries not be included in the accreditation from the launch of CDR, Consumers will be disadvantaged. For example, under Open Banking:

- Consumers pay more under existing Data Feed agreements (average fee is $38 per year) compared to Open Banking ($nil)

- The Open Banking consent framework provides for clearly define, easily revocable and traceable consent. Existing Data feed arrangements are typically paper based and do not provide these functionalities.
- The Under Open Banking, the liability framework for Data Holders, Data Recipients are clearly defined. In the current environment, the liability and who is responsible is not clear to the Consumer.

Intermediary Role within CDR

The role on an Intermediary within CDR is to provides Data Recipients with the services *e.g. Consent process* and Consumers with a disclosed party they can trust to share their consented data.

An Intermediary role is to *fill the gap(s)* where the Data Recipient does not have the expertise, technical skill or legal knowledge to connect to, and comply with CDR. The infrastructure provided by an intermediary can reduce compliance costs for Data Recipients and provide them with the speed to market for the product or service.

An intermediary Role can include, but is not limited to:

1. Provide access to CDR Data for Unrestricted Data Recipients
2. Provide access to CDR Data for Restricted Data Recipients
3. Compliance with the Minimum Information Security Controls E.g. Vulnerability Management

Functionality of Intermediary

The key functionality of an intermediary is listed below:

1. Consent Management
2. Consumer Dashboard
3. Data Standardization
4. Bulk data collection across many data holders and consumers
5. Data cleansing, validation and value adding
6. Compliance & Data Security *e.g. Vulnerability Management*
7. Customer Dispute Resolution
8. Data Minimisation

Disclosure of use of the Intermediaries

In line with the philosophy of the CDR, we believe the use of an intermediary by an Accredited Data Recipient must be disclosed to the Consumer during the Consent process, but ***not as an additional consent screen***. An additional consent screen specifically for an intermediary will cause more friction for the Consumer during the consent process, and the intermediary can be easily and effectively disclosed in the existing consent framework.

The disclosure of an intermediary is process already used in pre-CDR consent process with success. SISS can provide documentation and evidence of the process to the ACCC upon request.

Accreditation

General Comments

1. We note the accreditation level for unrestricted accreditation is adequate for those who want full access to CDR data and/or utilise an Intermediary.
2. The ACCC will need to provide further guidance on the external audit requirements of the Minimum Information Security Controls.
3. The current unrestricted accreditation level may not be attainable for smaller FinTech's, due to cost and/or complexity, which may stifle innovation and limit the benefits of CDR.
4. SDS recommends the Data Recipient Accreditation process recognises existing security accreditation(s) e.g. ISO 27001 when Data Recipients or an Intermediary apply for accreditation under CDR.

Accreditation of Intermediaries

SDS recommend the ACCC provide for a formal accreditation for Intermediaries.

All Intermediaries will be responsible for the access to, and transfer of Consumer Data. SDS recommends an intermediary attain the highest level of accreditation (unrestricted).

Unrestricted Level of Accreditation

SDS agrees with the Minimum Information Security Controls for the Unrestricted level of Accreditation.

SDS seeks clarification on the external Auditor requirements and the ability for the ACCC to scope the Vulnerability Management.

Restricted Level of Accreditation

SDS proposes that ACCC permit a restricted level of accreditation for Data Recipient (via Intermediaries).

The restricted level of accreditation should be based on limiting the Authorisation Scope the Data Recipient can access. This would align with what data can be shared in the pre-CDR environment today.

For example, to ensure the continuity of data supply for existing (pre-CDR) Accounting and Personal Finance Software Data Recipients the Authorisation Scope could be reduced as follows:

	Unrestricted Accreditation	Restricted Accreditation
Authorisation Scope	**All**	**Restricted**
Basic Bank Account Data	Yes	Yes
Detailed Bank Account Data	Yes	No
Bank Transaction Data	Yes	Yes
Bank Payee Data	Yes	No
Bank Regular Payments	Yes	No
Basic Customer Data	Yes	No
Detailed Customer Data	Yes	No
Public	Yes	Yes

Should the Authorisation Scope be restricted as outlined above, and given the additional oversight provided by an Intermediary, the Minimum Information Security Controls could also be reviewed to reflect the reduced risk.

In line with the above example, the Minimum Information Security Controls could be reduced as per the following table which matches what is typically required by banks today in the pre-CDR environment, for sharing BAI2 type bank data files.

	Unrestricted Accreditation	Restricted Accreditation
Penetration Testing	Externally Audited	Externally Audited
Vulnerability Management	Externally Audited	Externally Audited
Information Security Management System	Externally Audited	Evidenced Based

Accredited person and Accredited Data Recipient

SDS seeks clarification from the ACCC on the terms “accredited data recipient” and “accredited person” as they appear to be interchangeable in the rules.

End of Submission