ABSIA Australian Business Software Industry Association

217 Flinders Street
Adelaide SA 5000
info@absia.asn.au | www.absia.asn.au

29 October 2020

CDR Rules Team
Australian Competition and Consumer Commission

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

Dear CDR Rules Team,

Re: ABSIA's Submission to CDR rules expansion amendments

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of our members and the software industry. This submission has been prepared with input from ABSIA members and in collaboration with other industry bodies. ABSIA's membership consists of ATO regulated Digital Service Providers (DSPs) and third party add-on/ecosystem software developers operating in the business software application space.

Firstly, ABSIA would like to commend the ACCC on recognising the ATO's DSP Operational Framework. We look forward to the outcome of the ACCC's work with the ATO to produce the required guidance material. ABSIA is more than happy to assist with this process and provide input on behalf of DSPs as needed. Further, we welcome the introduction of the tiered accreditation approach and believe that it will enable greater participation from a range of Accredited Data Recipients (ADRs).

Given ABSIA's position within the industry, we have responded to select questions from the discussion paper. In summary, this submission makes the following points:

- Following the recognition of the ATO's DSP Operational Framework, the ACCC should be recognising industry standards that currently regulate intermediaries and their ecosystems such as the Security Standard for Add-on Marketplaces (SSAM);
- The intention of the CDR regime is to regulate Machine to Machine processes and interactions only. The CDR rules framework should not attempt to control and regulate human interactions;
- We believe that the affiliate accreditation option will not increase participation from DSPs and their affiliates unless the Schedule 2 requirements align with the SSAM which already exists to regulate CDR derived data transfers between ATO accredited DSPs and their third party software products;
- The SSAM will be reviewed by ABSIA and revised upon completion of the ATO's review of the DSP Operational Framework;
- The revised SSAM will be published by ABSIA within 60 days of the finalisation of the Operational Framework security questionnaire or 31 March 2021;

- The ACCC should avoid introducing additional requirements to Part 1 of Schedule 2 as it will add unnecessary costs and work to data transfers that are already secure and working as intended;
- We understand that most DSPs will be providing derived data to their third parties through CDR, which is a level lower than the Level 3 example, and therefore the relationship between a sponsor and affiliate should be taken into consideration. Here, the SSAM is already applied to DSPs and their third party software ecosystems; and
- We wish to once again remind the ACCC about the original intent of Open Banking and consider how these rules are impacting intermediaries, who exist mostly outside of the banking sector, and are having rules intended for banking/finance products applied to them.

Overall, the ACCC should be wary of making the CDR rules too complex for intermediaries to reasonably participate in CDR across current and future applications. This is perhaps the biggest risk to CDR and its overall success.

ABSIA would appreciate the opportunity to engage further on these issues. For further information about this submission, please contact Maggie Leese, ABSIA Marketing and Membership, on .

Yours faithfully,

Chris Howard,
President & Director, ABSIA.

Recognition of the SSAM for Derived Data Sharing

3. We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation.

With the ACCC encouraging greater participation in the CDR regime, there is an increased need to recognise existing industry standards that are already in place to manage intermediaries and their ecosystems.

In our industry, where an ADR is accredited via the ATO Digital Service Providers (DSP) Operational Framework, their ecosystem of affiliates consuming derived data should be able to self assess under the Security Standard for Add-on Marketplaces (SSAM)[1]. ABSIA, in partnership with the ATO and our members, is the custodian of the SSAM industry standard.

The intended recognition of the Operational Framework should come hand in hand with the recognition of the SSAM to create a seamless process for DSPs to encourage participation whilst minimising regulatory burden and administration overheads.

The SSAM is a proven security framework for third parties consuming sensitive data from DSPs via APIs. It is relied upon by multiple DSPs including MYOB, Xero, Intuit and Class among others.

The SSAM applies to third party software products with 1,000 customer connections to Australian business customers of a DSP or those who are connected to the practice client list of an Australian tax or BAS agent. These software products are required to complete and file a security self assessment to the DSPs (ADRs) that they integrate with via APIs once a year.

The DSPs are responsible for monitoring, approving and submitting a list of their connected third parties to the ATO as part of their annual certification process. DSPs are also required to report any known security incidents to the ATO immediately using the Software Developer Portal provided by the ATO's Digital Partnership Office. This reporting mechanism allows DSPs to notify the ATO and other relevant government agencies of any security incidents as they occur. Our members believe this approach has been effective for the past 12 months and should remain in place once the CDR regime is established.

The SSAM will be reviewed by ABSIA and revised following the completion of the ATO's review of the Operational Framework. The revised SSAM will then be published within 60 days of the finalisation of the Operational Framework security questionnaire or 31 March 2021 at the latest.

[1] https://www.absia.asn.au/industry-standards/addon-security-standard/

Please find more information about how the SSAM could apply to the affiliate accreditation tier in our response to the questions below.

10. Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sectors and future CDR sectors.

In comparison to the limited data restriction and data enclave restriction, the affiliate restriction does not create a simpler pathway to CDR accreditation. With the affiliate method still requiring affiliates to meet all of the Part 1 provisions and all but one of the Part 2 provisions under Schedule 2, ABSIA believes that this will create a barrier to entry and therefore limit participation.

For sponsors, ABSIA believes that their obligations are currently too onerous. They should be limited to receiving their affiliate's annual self assessments along with any underlying evidence to support their assessment and sharing this information with the ACCC via the Digital Partnership Office at the ATO when DSPs report this information through their annual review process. This process is currently how DSPs regulate their third parties (as mentioned above) and is covered by the Operational Framework and SSAM working together.

Recognising the SSAM would make this a much easier process for DSPs and their broader ecosystem of software developers. The evidence requirements and exact specifics of how the SSAM should be revised to accommodate the CDR rules should be undertaken by ABSIA members in close consultations with the DSPs, ATO and ACCC.

Here, we would like to note that this regulation is extending well beyond the banking sector in a way that is unintended by the Designation Instrument. Without recognising existing frameworks and standards that already cover similar data sharing processes, there are additional costs and regulatory burdens imposed on DSPs and it leaves them with few benefits. Aligning the sponsor-affiliate regulatory relationship with the Operational Framework and SSAM will make CDR much more attractive for DSPs and their third parties to participate in. Failure to do so may result in a stunted, fragmented or failed ecosystem similar to what has been seen following the introduction of the New Payments Platform (NPP).

11. Should there be additional requirements under Part 1 of Schedule 2 for sponsors?
No. ABSIA believes that these requirements are sufficient enough for now. If the SSAM is recognised for sponsors managing their affiliates, there should be no need to introduce additional requirements under Part 1 of Schedule 2. Adding further requirements here would just add unnecessary measures to data transfers that are already secure and working as intended.

Fundamentally, there are established working processes and protocols that facilitate API based data exchanges between DSPs (who will be Accredited Data Recipients (ADRs) under the CDR framework) and a wide ranging ecosystem of third party software applications. To realise the

innovative potential of the CDR, this ecosystem must be respected and allowed to continue to develop with minimal disruption.

13. The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.

Example level 1: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems.

Example level 2: affiliate is able to access all data sets, but uses some of the sponsor's systems and applications to access or manage the data.

Example level 3: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor's systems and applications to access or manage the data.

Many DSPs are not expected to share raw CDR data with third party software products via their APIs. As a result, our members believe that data shared by DSPs via APIs will almost always be considered to be CDR derived data. This kind of data sharing is at a level lower than what is considered in the example of Level 3 and therefore there is a case for considering the relationships between sponsors and their affiliates.

With the SSAM already being applied, CDR regulation should not be applied to DSPs and their third parties with the industry specific SSAM and Operational Framework being recognised instead. The SSAM is already fit for purpose and working as intended to ensure the safe transfer of permissioned data. The ATO recognises this framework and moving forward, the SSAM will continue to be aligned with the Operational Framework.

The ACCC should take the opportunity to align the CDR accreditation process with the Operational Framework and SSAM to make it much easier for DSPs and to avoid the duplication of these standards and the work required to meet them.

The SSAM will be reviewed by ABSIA and revised following the completion of the ATO's review of the Operational Framework. The revised SSAM will be published within 60 days of the finalisation of the Operational Framework security questionnaire or 31 March 2021 at the latest.

18. Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding 'raw' CDR data as disclosed by the data holder)?

As mentioned earlier, most ABSIA members expect to exclusively share limited or derived CDR data with their third parties alongside any other data that they normally share through existing processes. As DSPs will generally only share derived data, these insights could be limited to derived data. However, this may not hold true for other data interactions or other designated sectors such as telecommunications and energy.

With the definition of derived data currently being quite broad, the ACCC should be wary of the unintended consequences of capturing derived data that was not meant to be included in CDR.

Consumer Dashboards

14. We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.

As principals have these relationships, it makes sense that they are the ones providing these dashboards to consumers. However, with all these different types of ADRs needing to create their own dashboards, the result will be the creation of hundreds of different dashboards which may be confusing for consumers. The fact that we are only considering Open Banking here means that as CDR expands into other sectors, more and more dashboards will need to be created by ADRs with the potential of further confusing consumers.

To avoid confusion amongst consumers, we recommend that the ACCC takes a consumer-centric focus rather than a sector-specific focus to current and future CDR implementations.

General Feedback

Accredited Entities vs. Non-Accredited Entities

The ACCC should consider the unintended consequences of putting extra regulatory burdens on accountants and bookkeepers by regulating them as “non-accredited” entities. ABSIA believes that CDR should be regulating the machine to machine processes and interactions only and that the rules framework should not attempt to control and regulate these human interactions.

In this approach to only regulating machine to machine interactions, we do understand that this will be a difficult process as there will be machine to machine interactions that should not be included as a part of CDR.

Original Intent of CDR in Open Banking

From our last submission, we would once again like to note the original intent of Open Banking which was to, “revolutionise the financial services sector, transform the way Australians interact

with the banking system by giving consumers the right to safely share their data with other banks, other institutions and innovative FinTechs and get themselves a better deal."[2]

As Open Banking has expanded, intermediaries (and their customers) have been caught up as collateral. This was not the original intent and in some cases this has resulted in rules that are meant to apply to banking and financial products, being applied to accounting products.

Further, intermediaries were not a part of the Open Banking conversation until the *CDR consultation paper - participation of third party service providers*[3] which wrapped up in February this year. There has been a very short amount of time in between the introduction of intermediaries to CDR and the rules for intermediaries being created and with no official consultation process (like the two year consultation process that occurred with the banking sector), an opportunity has been missed to better understand the different types of intermediaries and how they share data.

This lack of consideration has the potential to create negative flow on effects to intermediaries and their consumers. As CDR expands and intermediaries are considered within those industries, it is important to consider such effects as intermediaries will have different levels of interaction with their own third parties and data holders across different sectors.

2 https://ministers.treasury.gov.au/ministers/scott-morrison-2015/media-releases/review-open-banking-giving-consumers-choice

3 https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-facilitating-participation-of-intermediaries-in-the-cdr-regime