

21 May 2020

Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Mr Farrell,

RE: Inquiry into Future Directions for the Consumer Data Right

The Australian Business Software Industry Association (ABSIA), welcomes the opportunity to submit to the *Inquiry into Future Directions for the Consumer Data Right*.

ABSIA actively represents the interests of the Australian business software industry working with key government departments and software providers to develop innovative solutions and progress Australia's digital economy.

ABSIA recognises the importance of the Consumer Data Right (CDR) in promoting innovation within the consumer services sector. This submission takes into account member feedback and is summarised by the following key views:

- CDR should create a single access mechanism;
- CDR should provide a low-cost and robust identity verification capability;
- ABSIA supports the extension of CDR into the superannuation sector and notes its potential to provide opportunities for innovation alongside Open Banking;
- Current and future CDR implementations should be consumer focused rather than sector focused;
- ABSIA commends CDR's approach to leveraging existing frameworks to lower the costs and fast-track implementation; and
- ABSIA broadly supports the introduction of 'write' access.

For more information about this submission, please contact: Ian Gibson, ABSIA Non-Executive Director, ian.gibson@absia.asn.au.

Yours faithfully,

Chris Howard
President, Australian Business Software Industry Association.

**Australian Business Software Industry Association's response to the
Inquiry into Future Directions for the Consumer Data Right**

Issues Paper Questions

Question 1 - We invite interested parties to make submissions on any or all issues raised by this Issues Paper of Terms of Reference. This includes views on potential developments and expansions in Consumer Data Right functionality, including their benefit and priority.

With CDR expected to expand into more sectors, CDR should consider creating a single access mechanism for those wishing to provide CDR capabilities. Each implementation of CDR currently has or appears to be adopting tailored access mechanisms, two examples being Open Banking using APIs and Open Energy using the AEMO model. Each access mechanism creates additional costs, both to implement and support, as well as introducing greater complexity and increasing the difficulty of leveraging data from a combination of Open "X" implementations. As CDR expands, this will only become more challenging.

Similarly, CDR should provide a low-cost and robust identity verification capability. This would help small to medium solution developers significantly while also providing consumer confidence about the integrity of CDR-based services. This becomes critical in an environment which incorporates 'write' access capabilities as it will assist in mitigating the potential negative impacts of identity theft or impersonation.

Question 2 - The Inquiry invites submission on the future roles that could be performed by the Consumer Data Right, the future outcomes which could be achieved, and what is needed for this to happen.

ABSIA supports the expansion of CDR into the superannuation sector in the form of Open Super. Open Super data, when combined with Open Banking data, will cover the majority of an individual's financial position (given superannuation often includes insurance coverage). This will provide a multitude of opportunities for innovative products that service both individual consumers and advisers.

Further, this combination of rich and comprehensive data could be leveraged to power an automated financial advice capability. This is perhaps the best solution to fill the gap between Australia's large retiring population needing quality financial advice and the decreasing number of qualified advisers.

Question 3 - The Inquiry invites submissions on how the Consumer Data Right can be leveraged with international developments of the kinds described above to enhance opportunities for Australian consumers, Australian businesses and the Australian economy.

No comment.

Australian Business Software Industry Association's response to the Inquiry into Future Directions for the Consumer Data Right

Question 4 - The Inquiry invites submissions on how the Consumer Data Right could be used to overcome behavioural and regulatory barriers to safe, convenient and efficient switching between products and providers, whether those barriers are sector-specific or common across industries.

One of the four key principles of CDR is to be consumer focused, however CDR is currently being adopted with sector specific solutions, which not only make it complex and expensive for developers, it also has the potential to be confusing for consumers as CDR expands into new sectors. In overcoming barriers to switching, CDR could adopt an individual consumer centric approach rather than an industry sector centric approach. Having sector specific solutions also makes it harder to generate a consolidated consumer view that could assist in maximising switching propensity.

If CDR were to develop a “whole of consumer” view it would enable consumers to access this data from a central location and allow them to truly benefit from CDR. An even better outcome would be to take a consumer oriented view and adopt a single identity verification regime and an access and consent management mechanism across all CDR areas. We have mentioned this in our answer to the question above.

Consumers need to be more educated on what CDR is and therefore what the potential benefits of CDR are. Research released at the end of 2019¹ found that 12 percent of respondents knew about Open Banking but they did not actually know what it entailed. Similarly in the 2019 EY FinTech Australia Census², an interviewee shared their concern about the low consumer awareness of Open Banking and questioned its success and value without this awareness.

Empowering and educating consumers to increase their trust in CDR and therefore their likelihood of participating in a CDR-based service needs to be a priority moving forward.

Question 5 - The Inquiry welcomes input from interested parties on these topics - including their benefits and costs - as well as other ‘read’ access functionality that the Inquiry should consider.

Keeping track of and managing a consumer's various consents for read and write access functionalities is already available in most software provider's applications. Here, a consumer has the ability to revoke access to any third party applications currently connected to their software. Adding multi-factor authentication (MFA) across these requests is an additional step that ABSIA recommends CDR to consider.

1

<https://which-50.com/open-banking-will-give-consumers-control-of-their-data-but-most-australians-still-havent-heard-of-it/>

2

<https://fintechauscensus.ey.com/2019/Documents/EY%20FinTech%20Australia%20Census%202019.pdf>

Australian Business Software Industry Association's response to the Inquiry into Future Directions for the Consumer Data Right

However, a consumer needs to manage third party access to each and every one of the applications that they are using. In terms of CDR, it would be beneficial for a consumer to be able to control third party access to each of their software solutions from a central location or service.

Developing a safe and efficient ecosystem of participants could be accelerated by re-using or remodelling existing networks. We would like to reiterate and share the importance of three frameworks used by the business software industry:

1. Superannuation Transaction Network (STN);
2. Digital Service Provider (DSP) Operational Framework; and
3. Security Standard for Add-on Marketplaces (SSAM).

STN

The STN, which is operated and maintained by the Gateway Network Governance Body (GNGB), assists employers and superannuation funds in meeting their obligations under the mandatory Data and Payments Standards³. The STN could form the basis for a common access mechanism across all CDR implementations given that this network connects the majority of businesses in Australia with hundreds of super funds and thousands of SMSFs including banks and the ATO.

DSP Operational Framework

The ATO's DSP Operational Framework outlines the security requirements for all the Digital Service Providers (DSPs), Sending Service Providers (SSPs) and Gateway Operators (GOs) that send personal, financial, payroll and superannuation data to the ATO. It requires them to undergo re-assessment each year and the framework itself is also reviewed annually and changes are enacted to reflect the risks present in evolving digital environments. The DSP Operational Framework essentially covers the applications that wish to connect directly to the ATO via API and therefore the first tier of this digital ecosystem.

Security Standard for Add-on Marketplaces (SSAM)

With DSPs operating their own APIs and allowing further third parties to connect and transact data, there was scope for the ATO to secure this broader range of ecosystem participants. Together with the ATO and software developers, ABSIA developed the SSAM as a baseline security standard for third parties connecting to DSPs via API. This protects both the DSPs and the ATO. The SSAM ensures the integrity of third party providers that participate in this DSP ecosystem but they do not connect directly to the ATO.

³ <https://www.gngb.com.au/superannuation-transaction-network/>

Australian Business Software Industry Association's response to the Inquiry into Future Directions for the Consumer Data Right

Question 6 - The Inquiry is interested in interested parties' views on these issues. In the context of Open Banking, the Inquiry is particularly interested in interested parties' views on how the Consumer Data Right could best enable payment initiation.

ABSIA broadly supports the enabling of 'write' access.

At the moment, from a software provider's perspective, making payments to employees and suppliers is a cumbersome process for a consumer. With the introduction of write access, consumers can use their accounting software to initiate transactions or make payments to third parties without having to leave their software. This reduces the risks with no more ABA files and less human error involved. At the same time, it also increases operational efficiencies for consumers and their businesses. For software providers, there are minimal regulatory barriers, compliance costs or risks involved as they already use APIs and enforce the robust authentication that is required for write access to work securely. The adoption of e-invoicing could also assist here as it provides the ability to electronically verify senders and receivers.

However, when it comes to establishing who bears the responsibility and where in payment transactions, there are a number of things to consider from a software provider's perspective. Such considerations include:

- Is the sender authorised to access this account?
- Is the business software authorised to connect to the institution's API and make the request?
- Has the financial institution verified these parties?

What is clear from the above questions is that the risk and responsibility cannot be definitively placed on one party. Instead, a framework should be established that takes into account a number of checks and balances that would help determine who should bear the responsibility if a mistake were to happen in a payment transaction.

ABSIA, at this point in time, does not support the extension of write access to enable third parties to change the details used to identify customers. At the moment, without the correct security measures in place, it would be very hard to manage the security risks to the third parties, consumers and the Open "X" service in question. ABSIA would support this extension if CDR were to develop an identity verification capability that could provide absolute confidence in the identity of the consumer before details can then be amended.

Question 7 - The Inquiry welcomes input from interested parties on the above including potential linkages and interoperability with other consumer-directed and international data portability regimes, and accreditation frameworks that focus on data risk management.

ABSIA commends CDR's approach to re-using and innovating off current services (where applicable) rather than starting from scratch when building their own frameworks and infrastructure. We encourage this approach moving forward.

Australian Business Software Industry Association's response to the Inquiry into Future Directions for the Consumer Data Right

There are a number of standards currently emerging across different sectors and it is now becoming difficult for software providers to adhere to multiple rules frameworks without negatively impacting how their software operates. This is why ABSIA commends CDR's approach. In particular we suggest evaluating the STN, DSP Operational Framework and SSAM as we have mentioned in our response to question 5.

ABSIA suggesting liaising with the following bodies regarding each of these frameworks:

- GNGB for the STN
- ATO for the DSP Operational Framework
- ABSIA for the SSAM

ABSIA also recommends evaluating the Trusted Digital Identity Framework (TDIF) as a mechanism for identity verification, on the basis that the TDIF could be extended to being used by certified third party service providers.

Question 8 - The Inquiry welcomes views on the above as well as any broader role that other aspects of the Consumer Data Right regime could play in supporting productivity and data security in the digital economy.

Despite the fact that the work on the national API standards⁴ is focused on creating a standard for government APIs, there may be scope to take this framework into consideration once it is completed. The CDR could use this to create their own API standard for third party providers to use or they could point to the national API standard as best practice for developers. It is also worth mentioning OWASP's API security project here⁵.

In line with previous comments, CDR should continue their re-use attitude towards building future CDR frameworks and capabilities.

Question 9 - The Inquiry Invites submission from interested parties on how to ensure that, as the Consumer Data Right develops, it does so in a manner that is ethical and fair, as well as inclusive of the needs and choices of all consumers. This includes ways to encourage socially beneficial uses for the Consumer Data Right.

No comment.

⁴ https://api.gov.au/standards/national_api_standards/

⁵ <https://owasp.org/www-project-api-security/>