Australian Banking Association

Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage)

ABA Submission

16 October 2018

Australian Banking Association

Executive Summary

The ABA welcomes the opportunity to comment on the exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*.

ABA members believe Australia is well positioned to create a strong Consumer Data Right (**"CDR"**) regime that benefits Australians and sparks innovation across the economy.

ABA members welcome the updated draft and believe the proposals strengthen the CDR regime. As Treasury notes, the CDR will give customers the ability to access more information about themselves, and about their use of goods and services, which will enable them to make informed decisions about product and services.

This submission focuses on the principle of reciprocity and the Privacy Safeguards.

The ABA believes that having a well-designed reciprocity mechanism within the CDR is key to ensuring customers reap the full benefits of the data that is held regarding them. Ensuring that all entities wishing to join the CDR are required to enable their customers to share their data is key to fuelling innovation and expanding customer choice. This will mean that entities compete to gain customers using their analytics and insights, and not through their monopoly hold on specific data types.

Another issues that requires further consideration is simplifying the privacy obligations under the CDR. We believe that the dual privacy scheme remains complex and we note specific issues on the application of the Privacy Safeguards.

Australian Banking Association

Table of Contents

Australian Banking Association

1. Reciprocity

ABA members strongly believe that full reciprocity, as outlined in the Farrell Review, should be in place from July 2019. The principle of reciprocity is outlined by Farrell reproduced below.

> ***Farrell Report Recommendation 3.9 – Reciprocal Obligations in Open Banking***
>
> *Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.*

In practice, any entity that is seeking to be accredited to become a data recipient should be subject to an assessment of their data at the accreditation phase. For ADIs, this will mean those entities seeking to join the CDR ahead of their mandated start date would be required to share any data that was within the industry designation's dataset.

With this in mind, the ABA believes that the ACCC should amend the rules for Stage 1 such that any ADI wishing to join the CDR should also be a data holder once they join the CDR. We also believe that non-ADIs with dataset of a similar or identical nature should also be subject to reciprocity when they become accredited.

For those entities outside of the designated industry, the ABA views that the reciprocity principle should also be in place. We recognise that principle of equivalent data is difficult to define and address via rules. However, the ABA notes that equivalent data should be assessed and captured at the accreditation stage based on key principles around core customer data held by the entity seeking to become accredited.

The ABA is developing an accreditation framework that we will circulate shortly to regulators. But we note that equivalent data should focus on customer use cases and what data would be valuable for a customer to share.

An example may be **an online retail website.**

An online retail website collects transaction data on what and when a customer purchases from their site. This data would provide rich insights into a customer's shopping habits. The online shopping website may have entered the CDR looking to offer a new credit product to customers, that draws on their own data and that customer's transaction history held at a bank.

The condition of reciprocity would allow a customer to direct a fintech to access the online shopping data and the bank account transaction data. Coupled together, the fintech could develop a personal financial management tool that helps the customer manage their finances.

2. Interaction of the Privacy Safeguards with the Privacy Act

The ABA appreciates Treasury's clarification on how the dual systems of the Privacy Act's Australian Privacy Principles and the CDR's Privacy Safeguards will work in practice. Particularly, how each system applies to data holders, accredited data recipients and customers.

However, ABA members note that the dual systems remain complex in practice to deliver. Many complexities relate to instances where an ADI is both an accredited data recipient and a data holder, and therefore subject to both the APPs and the Privacy Safeguards on the same data.

Substantive differences between the two systems pose significant practical challenges for banks when using, storing and securing personal information and CDR data, and for internal compliance practices and technical issues like data flows.

The ABA welcomes further discussions with Treasury around the options for institutions that are both data holders and accredited data recipients. These include subjecting them to the APPs only or turning off APPs in some circumstances and having only the Safeguards apply.

2.1 CDR Privacy Safeguard 1 - Open and transparent management of CDR data

ABA members believe PS1 unnecessarily doubles up privacy policies when the APP1 is also in place, and this creates confusion and uncertainty for consumers. Rather existing privacy policies should stay in place and expanded to include the requirements of CDR policy included in relevant circumstances.

Treasury have included a requirement under PS1 that CDR policies be "in a form approved in accordance with the consumer data rules". In practice, this means that when a data holder becomes a data recipient they will be subject to providing both an existing privacy policy under APP1 and would then need to provide that customer with another privacy policy that must meet the CDR rules in an "approved form". It is unclear who approves this policy and why an additional policy would be needed.

ABA members believe that a better alternative would be to update existing privacy policies that meet the APPs with relevant requirements of a CDR policy. There is precedent for this, such as including the requirements of credit reporting policies in the same document as a privacy policy required under the AAPs.

2.2 CDR Privacy Safeguard 2 – Anonymity and pseudonymity

We note that PS2 is inappropriate in a banking context and the ACCC will make consumer data rules which prohibit the use of a pseudonym for this sector. As Treasury notes, consumers are not able to deal with their bank via a pseudonym and it would not be appropriate to enable them to do so within the CDR system.

2.3 CDR Privacy Safeguard 3 – Collecting solicited CDR data

ABA members note that PS3 now reads in a way that requires the consumer to instigate a request for a participant to request their CDR data, but P 4 still uses language implying that it is the role of the participant to seek to collect the information. We believe that consistency in language will improve overall understanding and application of the Safeguards.

2.4 CDR Privacy Safeguard 6 – Use or Disclosure of CDR Data

ABA members believe the amended PS6 places a restrictive scope of permitted disclosure.

2.4.1 Consent

The ABA believes requiring consent is an important principle of the CDR, but there may be circumstances where the consent requirement could be captured under "bundled consent". For example, if an entity is using a cloud service provider, this will result in ongoing disclosures of CDR

data. It would be unworkable for a bank to seek consent from a customer each time the data is disclosed.

PS6 permits an entity to disclose CDR data only if permitted by the Rules, even if the consumer has provided a valid consent. Limiting the use of CDR data to where such specific active consent has been obtained will effectively require banks to build and maintain separate structures to hold and maintain data.

2.4.2 Restrictions on non-accredited data recipients

Under the ACCC's current draft of the CDR Rules Framework, the ACCC has enabled CDR data to be disclosed to non-accredited persons provided that consent has been given. We note that providing CDR data to non-accredited persons may jeopardise the integrity and security of the CDR regime.

Data arrangements exist outside of the CDR that are subject to bilateral agreements such as feeds to accounting software. These arrangements should the given third parties such as accountants who would not be accredited entities under the CDR regime can already obtain read-only account access in practice now, we think it might be difficult to suggest such non-accredited entities be blocked entirely on the basis of jeopardising the integrity and security of the CDR regime.

2.5 CDR Privacy Safeguard 7 – Direct Marketing by accredited data recipients

The ABA believes that Privacy Safeguard 7 should be amended to remove what is likely to be an unintended discrepancy with APP7. That is, to recognise the Spam Act (2003) and Do Not Call Register (2006).

PS7 outlined in Treasury's exposure draft enables the use of CDR data for direct marketing only when permitted by the Rules and where a valid consent has been provided in accordance with the Rules. However, the ACCC state that direct marketing is prohibited under the Rules. We note that this is stricter than APP7, which allows for direct marketing, provided the customer is given an opportunity to opt-out of their data being used for marketing.

2.6 CDR Privacy Safeguard 8 – Cross-border disclosure of CDR data by accredited data recipients

PS8 (Cross-border disclosure) will apply to restrict an accredited data recipient from disclosing CDR data outside Australia unless the new recipient is an accredited person or permitted under the consumer data Rules.

In practice, banks and fintechs use outsourced service providers for storage and/or processing of data. Requiring all CDR data recipients to be accredited, as outlined in PS8, poses issues for those banks that use outsourced service providers, including those that are domestically based but with offshore support. ABA support the ACCC's requirements that outsourced providers be subject to minimum safeguards and we believe this is sufficient to capture this common arrangement.

2.7 CDR Privacy Safeguard 9 – Adoption or disclosure of government related identifiers by accredited data recipients

The ABA would note that PS9 should be simplified by just noting that APP9 applies to all persons.

As it stands, it is unclear what section (2) of PS9 is trying to achieve. That is, is it to prevent further disclosure of government identifiers via subsequent disclosures? Or is it to allow CDR disclosures to disclose government identifiers freely as it's just the transfer of data the customer wants to another party? If so, the ABA believes consideration should be given to data recipients not necessarily being authorised Tax File Number recipients.

2.8 CDR Privacy Safeguard 11 – Quality of CDR data

We note that practically it may be difficult to keep CDR data accurate where the CDR data is derived (or is a result of a chain of derivations).

2.9 CDR Privacy Safeguard 12 – Security of CDR data held by accredited data recipients

In the case of a data holder that is also an accredited data recipient, the requirement to destroy or de-identify CDR data that it no longer needs for the purposes under the consumer data Rules may not be practical. This also goes beyond the requirement of the APPs.

2.10 CDR Privacy Safeguard 13 – Correction of CDR data

The requirement to correct CDR data applies to both data holders and accredited data recipients. This is in addition to APP 11 as it applies to data holders to ensure the quality of personal information they hold.

ABA members believe that it will be difficult to correct CDR information in instances where information has been de-identified or aggregated. In this scenario, it is not possible to ensure that the data as it related to a CDR customer can be updated as part of an aggregated dataset.

3. Other proposals

3.1 Proposal 1 – Derived Data

ABA members support clarification that the CDR is intended to follow the Farrell Review. As a general rule "data that results from material enhancement by the application of insight, analysis or transformation" should not be included in scope, but that "there can be exceptions to, or qualification of, this broad principle."

We support changes to the exposure draft that means the Minister will hold the power to determine what data is included via the industry designation instrument, rather than at the discretion of the rule-making power. This will provide stakeholders with greater level of transparency over datasets from an earlier stage and will ensure that datasets are subject to parliamentary oversight. This will also ensure that data holders have greater certainty over their intellectual property and will continue to invest and innovate in analytics.

3.2 Proposal 4 – Process for designation and rule-making

The ABA supports the transparent minimum consultation requirements outlined in the exposure draft. We also support limiting the circumstances in which emergency Rules may be made to when the ACCC views emergency Rules are necessary to avoid imminent risk of serious harm to the efficiency, integrity and stability of the Australian economy, or to consumers.

3.3 Proposal 5 – Framework for charges for and access to a CDR dataset

The ABA supports Treasury's proposal that the designation instrument for datasets should identify whether a data set is fee free or the data holder can impose charges for access and use (a chargeable data set). We also support that where fees may be imposed, market-based pricing is the initial pricing approach. The ACCC would have powers to determine a reasonable price for access if data holders impose excessive fees taking account of a range of factors, similar to current access regimes.

Australian Banking Association

About the ABA

With the active participation of 24 member banks in Australia, the Australian Bankers' Association provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.