Mr Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

7 September 2018

Dear Mr McAuliffe

Westpac Group Submission – Treasury Laws Amendment (Consumer Data Right) Bill 2018

The Westpac Group (**Westpac**) welcomes the opportunity to provide a response to the exposure draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (**Bill**) and thanks Treasury for the opportunity to participate in recent roundtables held in Sydney.

In addition, Westpac supports the submission made by the Australian Banking Association (**ABA**).

Introduction

As stated in earlier submissions on Open Banking, Westpac supports the Government's introduction of a Consumer Data Right (**CDR**) regime in Australia. We agree that the application of the CDR to the banking sector, and subsequently to other sectors in the economy, has the potential to transform the competitive landscape by giving individuals greater access to, and the ability to share, their data.

Data, when used safely, effectively, and by trusted users can provide immense value to individuals, industry, the government and society more broadly. Improvements in our collective use of data will ultimately help Australia's global competitiveness through a more innovative and productive economy.

We support the Government's approach to place the value of consumer data in the hands of the consumer so that they are the decision makers in the CDR system and have the ability to direct where it is transferred.

Trust in the CDR regime is integral to its success. We know that customers trust banks with their data and their financial assets.

To retain trust and confidence in the economy, the CDR framework must support the safe transfer and use of customer data, thereby protecting customer privacy and information. In the banking sector, customer information relates to their financial assets, so it is imperative that this information is adequately protected to avoid the introduction of systemic risk into the Australian financial and payments systems.

This submission outlines the key areas of the Bill that we consider require amendment or clarification in order to better align with the intended policy objectives and principles of the

Review into Open Banking: giving customers choice, convenience and confidence (Open Banking Report) [1], namely that:

- Open Banking should be customer focused;
- Open Banking should encourage competition;
- Open Banking should create opportunities; and
- Open Banking should be efficient and fair.

Consumer Data Right regulatory framework

We understand the Government's proposed approach is to implement a consumer data right via a layered regulatory framework with multiple regulators. We understand this framework needs to be flexible enough to accommodate different sectors within the CDR regime and within that structure the ACCC will establish the consumer data rules and Data61 will establish the data, transfer and security standards within the system. We recognise that the draft Bill is therefore necessarily broad.

Westpac supports the layered approach and considers it necessary for there to be flexibility for the ACCC and Data61 to tailor the consumer data rules and technical standards for the very different sectors of the economy that will be subject to the CDR. We note, however, that the ACCC rules and Data61 standards which will sit underneath this broad framework are yet to be developed and will contain much of the detail that Westpac needs in order to identify and mitigate risks ahead of the 1 July 2019 implementation date.

Westpac will continue to work collaboratively with regulators and Data61 through this process in order to safely deliver Open Banking by 1 July 2019.

In terms of the draft Bill, we have identified some key preliminary issues which we consider require clarification including:

- Definition of CDR consumer including corporate customers by 1 July 2019;
- inclusion of value-added/derived/aggregated data in the scope of CDR data;
- reciprocity;
- approach to the privacy safeguards; and
- the liability/penalty regime.

We would also appreciate guidance on a range of ancillary issues, which we have also set out below.

[1] Scott Farrell, *Review into Open Banking: giving customers choice, convenience and confidence*, December 2017 (Open Banking Report)

Key issues

Definition of CDR consumer – corporate customers

We consider that in order to deliver Open Banking safely and securely, the 1 July 2019 start date should not include corporates. That is, the focus as at 1 July 2019 should be on individuals and small businesses. This would enable the vast majority of customers to have increased choice by 1 July 2019. Inclusion of corporate customers will require more time to implement as Banks will need to undertake:

- a large customer engagement program (to recapture consent for the purpose of data sharing arrangements);
- customer education (to ensure the risks associated with data sharing are appropriately understood and accepted and the consent is both informed and explicit); and
- an online workflow authorisation capability (this will require time for design, build and implementation).

The definition of CDR consumer is very broad and includes individuals together with small, medium and large business enterprises.[2] We have set out in our earlier submissions that inclusion of complex accounts (such as those with corporate customers) is challenging as consent models for these customers are far more complex than with an individual customer. A poorly designed corporate consent rule would, for example, give junior employees the ability to share extremely sensitive data.

Of note:

- **There is no precedent for a consent framework for corporate customers:** Unlike retail/personal banking, there are no domestic or international examples of a multi-bank entitlement/consent framework to use as a basis for the implementation in Australia. We note that corporates are out of scope of the UK's implementation of Open Banking.
- **Our largest corporate customers are extremely complex**: They have multi-level subsidiary structures, each with different directors and office holders. Entities may have many different bank accounts and facilities and often have authorised staff for payments purposes (often involving multiple authorisations depending upon the amount of the transaction). As a result there may be thousands of individual combinations of people authorised to action aspects of banking services on behalf of a corporate.
- **Existing internet banking solutions contain complex authorisation rules:** In a single organisation, many different individuals may have authority to perform one or more actions on an account. For example, one individual may be authorised to submit payment information, another may be able to authorise payments, and another may be authorised to simply view payments. This separation allows customers to enable staff to operate on an account without providing visibility of sensitive transactions such as payroll information.

[2] Schedule 1, item 1, subsections 56AF(4) and 56AF(5) of the Bill and para 1.53 of the Explanatory Memorandum.

- **Some corporate customer systems are integrated with ours:** Corporate customers have the ability to initiate payments from their own systems in some cases which are subsequently processed by Westpac. For example, if a corporate customer uses an account payables module within an accounting package they can make payments directly within their systems, with Westpac providing the banking channels. In this example, the customer can control the submission and authorisation of payments themselves and Westpac would not have visibility of the real-time controls that are applied by the corporate customer to control either the authorisation of the payment or the visibility of the transactions for those accounts.

Value added/derived data

Under s 56AF of the Bill, CDR data is very broadly defined and includes data which is directly or indirectly derived from information specified in a designation instrument. The Explanatory Memorandum states that this will also include value-added data. As we have not seen the designation instrument for the banking sector, it is difficult to comment fully on this issue. However we note that the inclusion of value-added data is not aligned with the recommendations in the Open Banking Report[3].

The Open Banking Report recommended against the inclusion of value-added data in the scope of Open Banking on the basis that this could be a disincentive for data holders to invest in analysis and transformation and accordingly undermine the objective that open banking encourage competition to generate increased customer choice. The Open Banking Report considered that retaining incentives to make such investments was important to support the creation of an innovative data industry.

We consider that value-added data should not be in scope for Open Banking as it was explicitly recommended for exclusion, and is fundamentally not aligned to one of the four key principles identified by the Open Banking Report; namely that Open Banking should be efficient and fair. The inclusion of value-added data also has the potential to confer an unfair advantage on Westpac's competitors by allowing a customer to share data which Westpac or another entity in the CDR regime has analysed and transformed at its expense. If it is the intention to include value-added data, we consider that more thought needs to be given in how this is defined per sector.

We also seek clarification on the circumstances in which fees will be payable and the rationale for including fees for certain data in the draft Bill.

Reciprocity

Reciprocity was one of the key recommendations of the Open Banking Report, however this is not clearly dealt with in the draft Bill. We consider reciprocity to be an important feature of the Open Banking system and would welcome further clarity on how this would be provided for in the CDR regime. In particular, a fair and balanced regime is dependent upon reciprocity. It is difficult to see how the key principle that open banking be "efficient and fair" [4] would be achieved if data holders were required to provide data to fintechs or non-bank accredited data recipients that were themselves not obliged to share equivalent data in order to support the overall system (which would lead to unintended data leakage).

[3] See Recommendations 3.1 – 3.6 in particular.
[4] As noted in the foreword to the Open Banking Report

In our view (consistent with the Open Banking Report):

- being able to appropriately reciprocate should be a prerequisite to recipient accreditation;
- the ACCC should determine what would constitute "equivalent data" for non ADIs/recipients outside of the banking sector; and
- recipients should only be entitled to participate once they are able to provide "equivalent data" in order to ensure the overall system is supported.

We understand that the implementation, monitoring and enforcement of a reciprocity regime will be challenging. Given this, we note that we are interested and available to work with Treasury and the ACCC on how the regime should be managed.

Privacy

We note that the privacy safeguards in Division 5 of the Bill apply to both data holders and accredited data recipients equally.

Consistent with our previous submissions, Westpac is supportive of appropriate safeguards being in place to ensure customer data is securely and safely handled, particularly for organisations that are not APP entities within the meaning of the *Privacy Act 1988* (**Privacy Act**). In our view, it is not clear however how the Privacy Safeguards are intended to operate with the Australian Privacy Principles (APPs), given the two regimes are not entirely consistent and we do not think it is feasible to have two regimes applying to the same entities at the same time.

We are concerned a two tiered regime will not only create operational complexity but also will either introduce significant cost or curtail the existing use of data and associated innovation. Our view is that data holders that would ordinarily be subject to the Privacy Act should continue to be subject to that Act and not be subject to multiple overlapping regimes, which would be difficult to implement operationally but also very confusing for the consumer e.g. in terms of the different rights a consumer has under each regime. Specifically our recommendations are as follows.

- That the Privacy Safeguards apply from the time of the CDR Consumer request until the CDR Data has been disclosed by the data holder to the Accredited Data Recipient.
- If a data holder receives CDR Data that relates to a CDR Consumer (being information provided by the customer or customer transaction data), the APPs apply to that CDR Data from time of receipt. The APPs should apply in the same way that they apply to personal information received via other means for example information received via an online application or in a branch. It is impractical to have two regimes applying to the same customer's data dependent upon how that data was received. In our view, requiring this dual standard is unnecessary with respect to data holders that have existing compliance processes in place to manage and protect this information today, securely and in accordance with their current responsibilities under the Privacy Act. We note data holders should still be required to ensure that they collect the CDR Data pursuant to a valid request/consent from a CDR consumer. Separately, we note that Privacy Safeguard 8, with respect to

requiring all offshore recipients of CDR Data be accredited, is impractical for organisations with existing outsourcing arrangements with service providers with offshore operations and we consider APPs 8 and 11 adequately protect this information.

- For non-personal information that is CDR data, for example information relating to a business or corporate, neither the Privacy Act nor Privacy Safeguards are appropriate safeguards and our existing confidentiality obligations which apply to banks generally as trusted institutions [5] provide both sufficient and suitable protection.

Liability

Westpac is broadly supportive of the provisions that have been included in the Bill in relation to "protection from liability" and liability of data holders to data recipients.

In relation to penalties for a failure to comply with the Privacy Safeguards are concerned:

- any penalties under the Bill should be aligned with, and no more onerous than, existing penalties under the *Privacy Act* (**existing penalties**) to ensure proportionate consistency between the two regimes; and
- it is not the policy intent for the penalties under the Bill to be greater than the existing penalties – which would appear to be the unintended consequence of the drafting in the Bill. For example, there could be a single customer affected by multiple Privacy Safeguard breaches or a single CDR incident that affects multiple customers. In each case, the civil penalty provisions, as drafted could result in multiple penalties being applied (which would be extremely high in aggregate[6]) and which far exceed the current maximum penalties under the Privacy Act[7].

This is not aligned with the Open Banking Report.

We presume the Standards will address matters covered by Privacy Safeguard 10 (in relation to requirements for accuracy, currency and completeness). In addition, as a practical matter, we do not think the requirement to advise customers should be triggered where we would "reasonably be expected to be aware" of incorrect CDR Data[8] and instead consider that the obligation should be triggered by a CDR Participant's actual awareness.

Geographical application

We consider that the geographical application of the draft Bill is unclear and broadly drafted. For example, we do not believe it is the intention to cover banking customers in other countries (that have their relationship directly with a legal entity in that country but which entity is related to an ADI even if the ADI collects that data, for example, Westpac New Zealand in our case).

[5] Banks have a common law duty of confidentiality which is also acknowledged in the Code of Banking Practice.
[6] In the 10s of millions.
[7] $2.1m for companies
[8] 56EM(2)

Drafting

Currently, the definition of "CDR Consumer" could also include Westpac with respect to CDR Data that Westpac discloses as a data holder given that Westpac could be identifiable from the supplied CDR Data which we do not believe is the intent. In addition, the breadth of the "CDR Consumer" definition would appear to cover individuals or businesses with whom we do not necessarily have a banking relationship which we believe is not the intention. We recommend reviewing this definition to ensure it works as intended.

Other Issues

Other areas of the Bill that we are seeking clarity include: how a customer should be able to obtain their CDR data; and the right for data holders not to honour data requests.

How customers can access their data

We note that the draft Bill empowers the ACCC to make rules that could allow a CDR consumer to request that their CDR data be disclosed directly to them, rather than to an accredited recipient. In order to ensure the safe transfer of customer data, data holders should be given the flexibility to determine how to provide data to consumers in these circumstances. For example, customers already have access to their transaction data through online banking as well as through transaction statements. We consider that it should be open to a bank to determine how it will provide data to a customer when it receives such a customer request.

Data destruction

We consider that under APP4, as a practical matter, Privacy Safeguard 4 should permit de-identification as an alternative.

Right to refuse data requests in limited circumstances

Westpac is also seeking clarity on limited circumstances in which a data holder may exercise discretion to refuse a CDR data request, including for example in the case of suspected fraud or AML/CTF issues. That is, what an appropriate standard of evidence would be before a data holder could exercise the discretion, what an appropriate safe harbor might be and potential penalties for failing to, for example, exercise it reasonably.

We welcome the opportunity to discuss the issues raised in this submission. Please do not hesitate to contact Roza Lozusic at roza.lozusic@westpac.com.au or 0466 424 324 if you would like any further information or wish to discuss.

Yours sincerely,

Michael Choueifate

Head of Government Affairs