NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on *Treasury Laws Amendment (Consumer Data Right) Bill 2018*

7 September 2018

TABLE OF CONTENTS

1. Introduction

NAB welcomes the opportunity to respond to the Department of Treasury consultation on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (Bill) which will enable the establishment of Open Banking in Australia. NAB supports Open Banking being established as part of an economy-wide data sharing framework under the Consumer Data Right (CDR). As a member of the Australian Banking Association (ABA), NAB has also contributed to its submission.

This submission builds on NAB's extensive contribution to the public policy debate on Open Banking, including its:

- March 2018 submission (March 2018) in response to the Review into Open Banking (Open Banking Review); and
- September 2017 submission (September 2017) to the Open Banking Review.

2. Executive Summary

This submission focuses on key issues where NAB believes the Bill needs refinement before being legislated. In some instances, more detail is required so that participants have certainty and clarity regarding the regulatory requirements. In other instances, NAB is concerned that key aspects of the Bill need revision. As NAB has noted before, the implementation of an Open Banking regime in Australia will be a complex and significant change to the Australian financial system.[1]

NAB believes that the data to which the CDR applies (CDR data) should not include derived data and that CDR data should not be allowed to be transferred to non-accredited entities.

NAB also re-iterates its long-standing support for the principle of reciprocity, and argues that holders of equivalent transaction data sets should not be able to become an accredited data recipient until their sector has been designated.

The liability framework should also include the requirement to comply with the data Standards.

Finally, NAB supports the Australian Privacy Principles being 'switched off' and substituted with the proposed privacy safeguards in the Bill and argues that any review of the Bill should be completed by 1 January 2022 at the latest.

NAB looks forward to participating in the upcoming consultation with the Australian Competition and Consumer Competition (ACCC) on the Rules Framework and ongoing engagement with the Data Standards Body (Data61) on the Standards.

[1] See NAB submission March 2018 in response to Open Banking Review, p3.

3. Definition of CDR data – derived data

NAB understands that the legislative instrument containing the designation of the banking sector to the CDR will outline the data sets and data holders to which the CDR will apply. The definition of CDR data in section 56AF of the Bill includes data that is derived from CDR data. The exposure draft explanatory materials (EM) at 1.50 and 1.51 states that CDR data will include 'value-added data which is derived from CDR data' and also that 'CDR data that is derived' from the primary sources of individual transaction data and data that relates to a product.

NAB considers that the expression 'derived data', in the context of the CDR, lacks definition and boundary. Imposing obligations on data holders to share 'derived data' creates uncertainty as to the scope of the CDR and puts data holders at risk of regulatory non-compliance. This outcome is at odds with the concept of legal certainty. Including derived data in the legislative definition also creates ambiguity in expanding the scope of the CDR beyond what NAB understands the intent of Open Banking to be.

NAB has previously stated in response to the Open Banking Review that customer derived data should not be mandated as part of Open Banking.[2] While there is a wide range of data definitions, NAB considers customer derived data to be: information developed by banks based on information provided by customers, such as analytics, and derived insights or information obtained by NAB from a third party under a commercial arrangement – such as credit scores and property valuations.[3] NAB considers this type of data – for example customer segmentation, propensity indexes, or internally derived risk ratings – to be both proprietary and unique to NAB. NAB also believes the definition of 'value-added data' in the Open Banking Review, and supporting examples,[4] should be considered similarly.

As such, NAB believes that the CDR definition in the legislation should <u>not</u> extend to data derived, either directly or indirectly, from CDR data. It should apply only to an individual's transaction data and data that relates to a banking product.

Instead, any further information that is intended to be captured by the CDR (beyond an individual's transaction data and banking product data) should be specified in the data sets as part of the banking legislative designation. This would allow data that should be part of Open Banking to be included under the CDR. An example of this would be account balances from a banking product, which have been derived from the individual transactions on that account.

This approach would not preclude the CDR from capturing derived data in other sectors in the future, but would require that these data sets are also detailed in the sector specific legislative designation. NAB believes this also best reflects recommendation 3.3 from the Open Banking Review that value added-added data should not be included in the scope of Open Banking.[5]

---

[2] See NAB submission September 2017 to Open Banking Review, p10. Some of this content is reproduced here.
[3] Ibid, p9.
[4] Review into Open Banking: giving customers choice, convenience and confidence, p33
[5] The Open Banking Review defined value-added customer data as "data that has been enhanced by a data holder to gain insights about a customer".

4. Ability to transfer data to non-accredited parties

The Bill allows CDR consumers to direct their CDR data to be provided in certain circumstances to a non-accredited entity. NAB believes that CDR data should only be shared with accredited entities.

Currently, NAB has several data-sharing arrangements in place, such as sharing banking information relating to small business customers via accounting software provider Xero.[6] NAB small business customers can access this functionality via their internet banking account.

Outside these relationships, NAB has existing processes that permit customers to ask for their financial data to be shared with third parties such as accountants. NAB believes these processes should continue outside the CDR framework, as they allow customer data to be transferred in bespoke formats to people such as accountants.

Allowing CDR data to be transferred to non-accredited entities, however rarely, also risks undermining the customer protection which the accreditation process is designed to provide. Accreditation for data recipients will help ensure the appropriate security and consumer trust in Open Banking and data transfers under the regime. Being required to transfer CDR data to non-accredited entities seems in contrast to this and NAB believes that only accredited entities should be able to receive CDR data.

5. Reciprocity

A guiding principle of the Open Banking Review was that Open Banking promotes competition. In doing so, the system needed to be 'capable of balancing the needs of different participants to ensure that the system is fair to everyone'.[7] NAB considers that reciprocity is a fundamental principle in order to create a level playing field for all participants. Recommendation 3.9 in the Open Banking Review supported reciprocity and data recipients also providing customer data at a customer's direction, including 'any data held by them that is transaction data or that is the equivalent of transaction data.'

An understanding of what constitutes 'equivalent transaction data' for non-authorised deposit-taking institutions (ADIs) is fundamental to reciprocity. NAB considers that an appropriate point to determine 'equivalent transaction data' is at the time a non-ADI seeks to become an accredited data recipient, via the accreditation process.

NAB provided its strong support for the principle of reciprocity in both March 2018 and September 2017. For example, if large global technology companies are eligible to receive customer data from ADIs, they should be required to provide data about customers to an ADI in response to a customer request. In this example, NAB believes ADIs should be able to receive large global technology companies' customer-provided data, or equivalent transaction data, such as search and personal entries, maps and location data. This should occur on a reciprocal basis.

NAB understands that the current framework only mandates the sharing of data after the specific sector has been designated and data sets defined in the instrument of designation. NAB's strong preference is that holders of equivalent transaction data sets are not able to become an accredited data recipient until such time as their sector has been designated.

---

[6] See NAB submission to Productivity Commission Draft Report: Data Availability & Use, p5

[7] Review into Open Banking: giving customers choice, convenience and confidence p.9.

Allowing global technology companies to be an accredited data recipient per the above example, without a requirement to share equivalent data sets until their sector is designated, is not a level playing field. NAB believes this approach could also have unintended consequences for the Australian financial system through the transfer of data from the local banking industry, and its subsequent value, to offshore-based global technology companies.

A way to help prevent this transfer would be a requirement for all CDR participants that CDR data should be held in Australia. It would also require offshore participants in the CDR to invest in Australian data infrastructure in order to participate in the CDR and resultant open data economy.

6. Privacy Protections

NAB considers that the protection of the confidentiality of customer data is critical.[8] With that in mind, NAB supports strong privacy protections so that customers are not put at risk.

The current drafting in the Bill provides that data recipients are generally subject to the privacy safeguards, which provide a more prescriptive approach compared to the Australian Privacy Principles (APPs). Under this model, data holders are subject to the APPs, except where specific privacy safeguards apply. Potential alternative models include drafting the privacy safeguards to build upon the APPs or turning off the APPs and replacing them with the privacy safeguards.

Whichever model is chosen, NAB considers that it is important to have clarity as to the circumstances in which the privacy safeguards do and do not apply to data holders. Part of the difficulty is that the same piece of data can be CDR data and personal information at the same time, so for data holders there is a need to specify the circumstances in which that data is subject to the privacy safeguards. NAB considers that any model whereby data is always subject to the privacy safeguards because a consumer has made a CDR request is too restrictive. This is because it would require a higher level of protection that in some instances is not needed or warranted. Certainty regarding when the privacy safeguards do and do not apply will also assist data holders to manage their compliance with regulatory obligations.

NAB's preferred model would involve the APPs being 'turned off' and replaced with the privacy safeguards. This approach has been used in other legislative regimes, for instance it is similar to the present handling of credit information in the Credit Reporting system (Part IIIA of the *Privacy Act* 1988). The benefit of the model is that it is simpler and easier to understand. In addition, the penalties and enforcement process would be simpler, as all penalties would be those under the *Competition and Consumer Act* 2010 (CCA).

In order for a model based on privacy safeguards to work, application of the privacy safeguards to data holders should be limited. This could be either by a general exception (e.g. 'the privacy safeguards only apply to data holders in circumstances where the data holder is disclosing, using, storing or deleting CDR data for the purposes of this Part or the consumer data rules') or in the drafting of specific privacy safeguards.

[8] See NAB submission September 2017 to Open Banking Review, p10.

7. Liability

Section 56GC of the Bill outlines the protection from liability for CDR participants if CDR data is provided in compliance with CCA Part IVD, regulatory framework and consumer data rules. It broadly states that if a party provides data in compliance with these requirements, then it is not liable to action or proceeding in relation to that conduct. NAB supports this approach to liability and has previously argued in both September 2017 and March 2018 that liability for fraud or data misuse caused after the transfer of that data to a third party should fall with that third party. One additional protection NAB believes should be included in section 56G is a requirement to comply with the data Standards. This would ensure that data holders or data recipients who do not collect data in accordance with data Standards are not automatically protected from liability.

Even with this liability framework, the possibility remains that some data recipients may not have sufficient means to reimburse customers in the event of a data breach where they are liable (particularly if it is significant). To prevent this situation where third parties are unable to make payments for which they are liable under the framework, NAB has previously advocated for, and continues to believe, that as part of the accreditation process an insurance requirement for data recipients should be implemented. This is to prevent situations where third parties are unable to make payments for which they are liable under the framework. This is required as if a data breach occurs and an accredited data recipient cannot reimburse customers for their loss, customers may expect data providers, such as a bank, to reimburse customers if the data recipient is unable to do so. This requirement would help prevent customers being uncompensated and foster on-going customer trust in the broader regime.

8. Timeline for review

NAB supports undertaking a future review and has previously argued that Post Implementation Reviews form part of regulatory best practice.[9] The Bill states that the review by an independent reviewer must be completed by 1 January 2023.

NAB notes that the Open Banking Review recommended (in recommendation 6.6) that an assessment of be conducted 'approximately 12 months after the commencement date'. The phased implementation timetable for banking announced by the Government means that Open Banking will be implemented by the four major banks by 1 July 2020, and 1 July 2021 for all other ADIs.

Given this timeline, along with the significant change required to implement Open Banking and speed of technological change in the economy, NAB believes this required review should be brought forward by a minimum of 12 months and be required to be completed by 1 January 2022 at the latest. This review timeline would allow for a full consideration of the four major banks' experience and significant insights from the experience of all other ADIs. It would also be completed after the implementation deadlines for all other ADIs so as not to create uncertainty about their timelines. A review by 1 January 2022 would still capture the experience of other sectors which the CDR will likely to have applied by then.

A review offers an opportunity to assess if the CDR is working as expected, the level of consumer uptake, and whether the intended outcomes are being achieved. A review could also consider the value customers are deriving from CDR and the speed at which

[9] See National Australia Bank, 'A Plan for Deregulation, April 2014, p13.

other sectors have or should be designated. NAB encourages the legislation to specify areas, such as these, which the review should be required to examine and report on. These would act as the minimum scope of the review, which could be augmented or further expanded by terms of reference for the review published by the relevant Minister at the time.

9. Conclusion

The establishment of the CDR, and subsequent designation of the banking sector, is a significant development in the Australian financial services industry. Open Banking has the potential to improve the speed of decision-making and offers opportunities to enhance customers' experience. It also offers the potential to increase competition in the banking sector and NAB welcomes competition that enhances customer outcomes.

The implementation of Open Banking remains complex and challenging. NAB looks forward to further and ongoing engagement with the Department of Treasury, the ACCC and Data61 on implementation.

Appendix

In order to implement Open Banking by the Government-announced timeline NAB requires certainty regarding fundamental aspects of the framework, which are not yet determined. NAB is hoping many of these issues will be promptly resolved through the upcoming rule-making process being undertaken by the ACCC.

Set out below are the key issues that need to be resolved which are:

1. **Consent for joint accounts**: It is unclear what the consent requirements will be for sharing CDR data for joint accounts. Most of the products within scope for Open Banking allow joint accounts.

   NAB has previously advocated for the authorisation of data transfer for joint accounts to reflect the arrangements on accounts which apply for money transfers. Upon further consideration of this issue and the required implementation timelines, NAB believes the most feasible method is that consent for joint accounts held by consumer customers be based on the authorisation process for accessing the account via internet banking. That is, if a customer is able to login into access a joint account, then they should be required to provide consent for any data sharing arrangements under the account. Any transaction history transferred should be tagged to the correct joint account holder name to ensure it is correctly attributed. This approach would align to the current situation whereby a joint account holder can share data about that account via a third party, for example via a CSV file.

   Further work is needed for business customer accounts in identifying who in a business, particularly in larger businesses, has the ability to direct that the businesses data be transferred to an accredited party.

   The ability to terminate a data sharing arrangement should follow the same principles as the establishment.

2. **Workflow:** From a technical perspective, the mechanism for consent and then transfer of data, noting the Open Banking Review recommendation 4.5 that consent be 'informed [and] explicit', needs to be resolved.[10]

[10] Review into Open Banking: giving customers choice, convenience and confidence, pIX

3. **Accreditation**: Certainty is needed regarding the framework for accreditation, including the proposal for the register of accredited entities and the technical process for checking accreditation (e.g. via an API call to a dynamic registration which provides a certificate, or by another means) and whether or not the accreditation list is updated in real time. Of particular interest is the notification process of data providers for when a previously accredited party is de-accredited. This notification needs to occur in real time to customers and data providers. Otherwise, there is a risk that customers will request their data be transferred to an entity which may have lost their accreditation, something the data provider could be unaware of. Even a short delay in notifying data providers or customers of de-accreditation creates unacceptable levels of risk. A further concern is whether there will be requirements to notify the accreditation entity if a participant is concerned about a data recipient's accreditation, and how this would interact with NAB's existing regulatory requirements (e.g. under the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 NAB must not disclose to any person that it formed a suspicion about an individual as this would constitute 'tipping off').
4. **Requirements for participants to share data acquired under the CDR:** It is currently unclear whether a CDR participant will be required to transfer (at a customer's request) CDR data it has acquired from a data holder to another accredited data recipient. A data recipient should not be required to on-share customer data which it has acquired via the CDR system (e.g. NAB should not be required to share a customer's NAB and Commonwealth Bank of Australia data with Westpac).
5. **Non-CDR data (product information):** Clarity is needed on the scope of the requirement to provide non-CDR data; in particular, the product types and specification that need to be provided. NAB considers that the requirement to share product price and feature information should only relate to products for which this information is already publicly available.