NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on how best to facilitate participation of third party service providers

3 February 2020

National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686

Introduction

NAB welcomes the opportunity to respond to the Australian Competition and Consumer Commission's (**ACCC**) consultation on how best to facilitate participation of third party service providers.

This submission builds on NAB's extensive contributions to the public policy debate on Open Banking and the Consumer Data Right. These include:

- NAB's September 2017 submission to the Review into Open Banking (**the Review**);
- NAB's March 2018 submission in response to the Review;
- NAB's September 2018 submission in response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (**CDR Bill**);
- NAB's October 2018 submission in response to a further Department of Treasury (Treasury) consultation on the CDR Bill;
- NAB's October 2018 submission in response to the ACCC's consultation on the Consumer Data Right Rules Framework (**Rules Framework**);
- NAB's May 2019 submission in response to the ACCC's consultation on the Consumer Data Right Exposure Draft Rules; and
- NAB's November 2019 submission in response to the Office of the Australian Information Commissioner's consultation on the draft CDR Privacy Safeguard Guidelines.

NAB has also been an active participant in the ACCC and Treasury's consultation processes and the Data Standards Body's (Data61) development of the Consumer Data Standards (**Standards**).

Overview

NAB supports the introduction of the CDR and its application to the banking sector via Open Banking. The CDR will give consumers greater control over their own data, spark innovation and drive more competition in financial services.

As noted in NAB's previous submissions, the success of the CDR is dependent on consumers having trust and confidence in the system. Accordingly, we believe that strong security measures, together with privacy protections are fundamental to the success of the CDR.

NAB sees intermediaries as a necessary element of the CDR, supported by a tiered accreditation model. However, the CDR ecosystem is only as strong as its weakest link. Accordingly, NAB believes that the security requirements for any lower tiers of accreditation should be directly linked to the sensitivity of the data the party will receive and the functions the party will perform on behalf of consumers.

NAB is not supportive of transfer of CDR data to non-accredited entities. NAB considers that under the CDR, consumers should reasonably expect that anyone who receives their data is accredited (and this should be transparent to consumers). Accreditation for data recipients provides security protection and ensures that CDR data is subject to stringent privacy protections under the privacy safeguards. NAB is concerned that transfer of CDR data to non-accredited entities increases the risk of data breaches. In addition, transfer of CDR data to non-accredited entities is at odds with the original design of the CDR via the

Review into Open Banking. Including transfer of CDR data to non-accredited recipients also provides minimal upside to consumers given that other mechanisms exist to share data with third parties outside the CDR.

Intermediaries

As noted in NAB's response to the Senate Select Committee on Financial Technology and Regulatory Technology (December 2019), a competitive and innovative financial services industry is critical to ensure good customer outcomes and growth of the economy more broadly, with opportunities for new businesses and business models. To that end, NAB recognises that introducing tiered levels of accreditation will allow for innovative models to emerge and lower barriers to entry.

The growth of the CDR and the data economy more generally is predicated on consumers being motivated to participate. Lowering barriers to entry in the CDR will allow more companies to participate, providing greater scope for innovation and the development of novel applications that help consumers.

To enable an effective tiered accreditation model, care must be taken to ensure that appropriate obligations are placed on participants with a lower tier of accreditation. NAB believes that the obligations should be commensurate to the sensitivity of data that the recipient will receive and linked to the functions that the recipient will perform on behalf of the consumer (as appropriate). For instance, in the future the CDR may be expanded to include write-access and high risk actions include updating personal information (as this may lead to identity takeover by changing a physical address or lead to high volume fraudulent transactions if a mobile phone number used for second factor authentication is changed). Similarly, if the CDR is expanded in the future to include payments, it is important that ADRs that perform these functions are subject to stringent security obligations.

In addition, it will be important that consumers are aware at the time they consent to the provision of their CDR data that it is to be shared with multiple parties (ie. the intermediary and the party with a lower level of accreditation). NAB recognises that it may be challenging to clearly explain to consumers the flow of data between third parties, particularly in the context of providing consent within an App. Nonetheless, in order to ensure consumer trust and confidence the process must be transparent and knowledge of the parties who will access their data is crucial for the provision of informed consent as per Rule 4.9.

Non-accredited entities

Transfer of data to non-accredited entities was previously considered by Treasury in its consultation on the CDR Bill in September 2018. NAB maintains its previous position that CDR data should only be shared with accredited entities.

Allowing CDR data to be transferred to non-accredited entities undermines the customer protection which the accreditation process is designed to provide. Non-accredited entities are not subject to the stringent privacy safeguards and depending on their status, may not be subject to the APPs. Non-accredited entities may not be legally required to report a data breach or equipped to cooperate effectively and within reasonable time frames with incident response or fraud investigation teams. This could lead to very poor

consumer outcomes. In addition, the CDR provides a clear definition of liability for data breaches. Where non-accredited entities receive CDR data under the CDR it is unclear who the consumer would have recourse to in the event of a data breach.

NAB has significant concerns regarding the security implications of sharing CDR data with non-accredited entities. From a technical perspective, in the absence of accreditation or a registry that whitelists participants, it is challenging for Data Holders to be confident that a third party making an API call is who they say they are. Accordingly, NAB is concerned that transfer to non-accredited participants increases the potential for fraud risk and compromise of customer data.

Existing mechanisms operate to facilitate the transfer of data from consumers to third parties, therefore introducing non-accredited entities to the CDR arguably places consumers' data at risk for minimal gain. Currently, NAB has several data-sharing arrangements in place, such as sharing banking information related to small business customers via accounting software provider Xero. NAB small business customers can access this functionality via their internet banking account. Where NAB has data-sharing arrangements in place with third parties those parties have satisfied rigorous security obligations.

Outside these relationships, NAB has existing processes that permit customers to request 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 shared in bespoke formats.

NAB believes that utilising either these existing processes or data-sharing arrangements with third parties is a better way of managing the security risks and challenges involved in this activity rather than allowing CDR data to be transferred to non-accredited entities.