NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on *CDR rules expansion amendments*

29 October 2020

TABLE OF CONTENTS

1. Introduction

NAB welcomes the opportunity to respond to the Australian Competition and Consumer Commission's (**ACCC**) consultation on the expansion of the Consumer Data Right (**CDR**) Rules. NAB supports Open Banking being established as part of an economy-wide data sharing framework. As a member of the Australian Banking Association (**ABA**), NAB has also contributed to its submission.

This submission is in addition to past submissions that NAB has made to Treasury and the ACCC to previous reviews in relation to Open Banking and the CDR since 2017. NAB has focused its response on the key topics and questions on which the ACCC has sought feedback. NAB welcomes the opportunity to provide further detailed feedback prior to the Rules changes being made.

2. Executive Summary

This consultation canvasses significant changes to the framework of the CDR. NAB believes the following guiding principles should be considered for each proposed change: technical assessment, timelines for delivery, privacy and security impact and customer experience.

NAB is concerned that some of the proposed Rules add complexity to the regime when customer data sharing has only recently commenced. Some participants have already voiced concerns that the regime is too complex and that smaller ADIs may struggle to navigate their regulatory obligations. Similarly, if consumers do not understand the consent process, their rights and the role of participants in the CDR this may reduce consumer uptake and ultimately the success of the regime.

NAB is supportive of a phased approach to implementation. The technical assessment should drive the delivery timelines and rhythm for delivery, rather than pre-defined delivery dates. NAB recommends that the roadmap for the CDR is based on clear stage gates that tie finalisation of milestones to delivery dates

NAB agrees with the proposed extension of the CDR to additional participants and sectors supported by the use of a tiered accreditation model. NAB is supportive of the limited data restriction model proposed. However, while NAB supports lower levels of accreditation for access to lower risk data, we continue to hold the view that all banking data sits at the high risk level. Therefore the limited data restriction model likely has greater application in lowering barriers to entry for other sectors.

NAB is supportive of developing a model to safely facilitate access for brokers to CDR data. NAB is happy to engage with the ACCC and the broker industry to develop a suitable approach.

NAB considers that the proposed affiliate model is unlikely to reduce barriers to entry for new participants due to the challenges of reaching commercial agreement with sponsors. This type of arrangement could be covered through modifications to the existing CAP arrangements rather than creating a new structure.

The protection of the confidentiality of customer data is critical and therefore strong security and privacy protections are paramount to the CDR. Accordingly, NAB is not supportive of ADR to ADR transfers or the extension of the CDR to non-accredited entities.

3. Complexity of the proposed changes to the Rules

NAB supports strong privacy protections so that customers are not put at risk. In update 2 to the Privacy Impact Assessment (**PIA**), Maddocks raises a number of risks with the proposed changes to the CDR Rules.

NAB agrees with the risks raised by the PIA in relation to the complexity introduced by the changes to the Rules. The CDR regime is already extremely complex to navigate and the proposed changes are significant – including additional categories of consent, complex information flows, new frameworks for participation and new definitions. CDR participants have previously raised concerns regarding ascertaining and understanding compliance obligations. NAB is concerned that the additional complexity will lead to consumer confusion, compliance challenges for small ADIs and uncertainty for ADRs.

We consider that the different categories of consent add more complexity to the regime and it is not clear how this will assist consumers and whether this change has been informed by consumer testing. Rule 1.10A defines specific types of consents and the category of consents. While the descriptions have specific meanings under CDR, they are generic terms and the intent could be lost on consumers. There is a risk that the approach will simply add to 'information overload' during the early stages as consumers learn how the CDR works which could in turn make consumers less likely to participate in the CDR.

Whilst we are supportive of the recommendation in the PIA that detailed and comprehensive guidance be issued in relation to the intended application and operation of the new Rules, we also query the underlying basis and necessity for adding more complexity to this legislative framework in the first place.

4. Roadmap

NAB is supportive of a phased approach to implementation that allows incremental development of capability and ensures participants have time to troubleshoot and refine their approach before adding further complexity. The development of the CDR ecosystem to date has been complex and challenging. NAB recommends that the roadmap for the CDR is based on clear stage gates rather than arbitrarily set compliance dates. We would recommend that the ACCC and Treasury, working with the Data Standards Body (**DSB**), establish a cadence whereby there is a long term roadmap that includes a series of milestones with associated lead times:

- Rules establishment – 12 months minimum prior to implementation;
- Standards finalisation – 9 months minimum prior to implementation;
- Conformance testing uplift – 6 months prior to implementation.

NAB has supported the need for at least 12 months between the finalisation of the Rules and implementation since March 2018.[1] Tying finalisation of the above milestones to implementation is important so that any delays in their finalisation is reflected in the implementation date, rather than delays creating insufficient time to comply with a pre-defined date.

The roadmap outlined includes items that are in varying degrees of readiness before they could be properly contemplated by participants as compliance obligations. Now the

[1] See NAB submission to Treasury on 'Consultation on Open Banking Review Final Report', March 2018.

system is up and running, the potential for these changes to have impact to the ecosystem increases and must be managed more closely. In particular:

- Proposed compliance dates from December 2020 through to July 2021 should be reconsidered due to the impact to Data Holders (**DH**). During that period there is significant work already established for both the major banks who have sub-brands and all other ADI's facing their first major compliance date.
- There has been no assessment of the priority of each change as to its importance on system stability, user experience or consumer adoption.
- The earliest change window that should be contemplated would be February 2022, and this date should be preserved to high priority changes.
- Given the change windows between now and February 2022 would then be filled by current compliance and roadmap items, NAB believes that the most suitable next window for the introduction of the proposed changes to support business customers is July 2022.

5. Increasing the number and types of businesses that can participate in the CDR

NAB is supportive of the proposed extension of the CDR to additional participants. As more participants join there will be greater scope for innovation and for the development of applications that help consumers. This has positive network effects and can lead to the establishment of a vibrant and creative data industry.

As noted in submissions to ACCC dated 3 February 2020 and 24 July 2020, NAB supports a tiered accreditation model, subject to strong security requirements commensurate with the sensitivity of the data the party will receive and the functions the party will perform on behalf of consumers.

The proposed rules include three types of restricted accreditation – separate affiliate, data enclave or limited data restrictions. These methods are in addition to the CAP arrangements which were codified in version 2 of the Rules (dated 2 October 2020).

These models introduce complexity which may lead to consumer confusion as well as potential for participants not to fully understand their regulatory obligations. The framework could be simplified, with the restricted levels split into two parts – limited data and sponsored (via data enclave or affiliate). The existing CAP arrangements could be extended to cover the 'sponsored' arrangements. NAB believes that further consultation is required to refine the tiering framework before the Rules are updated.

Further comments regarding the different models are set out below.

Restricted level: limited data restriction

NAB supports the tiering of accreditation where an ADR has a lower level of accreditation and is able to access limited data clusters. From a policy perspective, this supports the intent to open the CDR to a larger number of participants by lowering barriers to entry. This is consistent with the Review into Open Banking (December 2017), which set out that the object of the CDR was to enable a safe and secure data economy.

While NAB supports lower levels of accreditation for access to lower risk data, there are challenges in determining appropriate risk levels for each designated sector. The preliminary assessment of risks associated with data sets included in the consultation paper includes an indicative risk level, although this measure has not been defined. NAB believes that the risk levels need to be clearly defined in the Rules. The Data Standards can then be applied based upon agreed criteria. As a consequence, the DSB will be in a

position to set appropriate levels and categorise APIs based upon the sensitivity of the information they contain. Derived data should also utilise this criteria, as some insights are more sensitive than the underlying data.

We continue to hold the view that all banking data sits at the high risk level. Defining the criteria will allow for uniform application across industries depending on the risk level of the data.

In banking, care must be taken to protect customers and consequently a rigorous risk assessment must occur prior to banking data being shared with participants with lower levels of accreditation. Malicious actors will target the most vulnerable aspects of any system in order to exploit these weaknesses for gain. In banking, that translates to the traumatic customer experience of identity takeover and payment fraud.

Restricted level: data enclave restriction

Under this model a person accredited at the restricted level (principal) has a relationship with an unrestricted ADR that has established a data 'enclave' (the enclave provider). The data enclave approach may enable a party with a lower security posture to use data without materially increasing the risk of data loss. This could benefit ADRs by lowering barriers to entry.

It is proposed that the principal would not be able to access data outside the enclave or download local copies of the data to another environment. NAB is supportive of this approach but we note that this may be technically complex to implement correctly. For example a provider could state they have met the enclave requirement by presenting data to the agent via a web browser and through the use of javascript disable selecting and then copying the text. However this type of protection can easily be defeated (for example directly calling API endpoints, modifying javascript on the page). As such, technical guidance should be provided to ensure solutions are implemented that truly prevent outside access and downloads. This guidance could stipulate that data be rendered within the enclave and then displayed remotely.

In order to support the data enclave restricted accreditation, the parties would be required to use a CAP arrangement. NAB is concerned that by combining CAP arrangements and the data enclave restriction the structures become too complex. As a consequence, recipients and consumers may be confused regarding the accreditation and tiering structure which could impact on the level of consumer participation in the CDR.

In addition, the CAP arrangements were only codified in October 2020 and have not yet been properly exercised. The introduction of the CAP arrangement framework could naturally allow for a similar approach to the enclave structure and varying overlaps between provider and principal.

Restricted level: affiliate restriction

This model involves a commercial relationship between a person at an unrestricted level (known as a sponsor) and a third party who is accredited (affiliate), but can only access CDR data collected by the sponsor. The proposed rules acknowledge that an affiliate may collect data from their sponsor via a CAP arrangement or ADR to ADR transfers. In NAB's view introducing the affiliate restriction adds unnecessary complexity to the framework.

It is difficult to conceptualise how the introduction of the affiliate restriction will assist to increase uptake of ADRs into the CDR, in circumstances where it is largely similar to the already existing CAP arrangement. The main difference between the two is that the affiliate restriction requires the sponsor to play a significant role in oversight and assurance of its affiliates. This role and functionality could be created via further changes to the CAP arrangements rather than creating a new type of restriction.

In addition, the liability framework may make the affiliate restriction commercially unviable. Under the regime, the sponsor is subject to additional liability and potential civil penalty provisions if the sponsor fails to take reasonable steps to ensure compliance of its affiliates. In practice, liability would be subject to commercial negotiation of indemnities between the parties. However, for an affiliate, in addition to likely providing indemnities for its conduct to the sponsor, the affiliate is also an accredited person and therefore liable for misuse of data or failing to meet other obligations in its own right.

6. ADR to ADR transfer

NAB is concerned around the additional complexities and risks associated with ADR to ADR transfers.

In order to prove informed consent, consumers would need to understand the transfer of their data between ADRs. From a user experience perspective, consumers would require an explanation of the arrangement within a consent flow in order to provide this consent. Further, there are challenges in the event the consumer withdraws consent or where there is a data breach. As the DH is no longer party to the sharing of data, in the event of a data breach by an ADR, the DH will be unable to trace whether that consumer's data has been compromised. In order to manage data breaches, OAIC and ACCC would need to perform analysis to enable DHs to trace compromised identities so that appropriate controls can be put in place to protect consumers.

7. Sharing CDR data to non-accredited persons

The consultation proposes Rules that would allow ADRs to disclose CDR data to 'trusted advisors' and limited insights to nominated persons, with the consumer's consent. The potential for CDR data to be shared to non-accredited persons has been previously debated, including in relation to the original Treasury Laws Amendment (Consumer Data Right) Bill 2018.[2] NAB believes that CDR data should only be shared with accredited entities.

As noted in previous submissions, allowing CDR data to be transferred to non-accredited entities risks undermining the customer protection which the accreditation process is designed to provide. Accreditation for data recipients ensures the appropriate security standards and privacy protections (including the privacy safeguards) operate to protect consumers. Non-accredited persons are not subject to the stringent privacy safeguards and may not be subject to the privacy legislation. As a consequence, non-accredited entities may not have requirements to notify DHs of a data breach. This means that a DH may not be made aware of a data breach that compromises their customer's data and presents a fraud risk.

NAB considers there are alternative methods (such as tiering of accreditation) that can reduce barriers to entry and ensure greater participation in the regime rather than permit the sharing of CDR data to non-accredited entities. Privacy and security standards should not be reduced in order to encourage additional participation as the success of the CDR is dependent on consumer trust and confidence in the regime.

[2] See NAB submission to Treasury on 'Treasury Laws Amendment (Consumer Data Right) Bill 2018' (September 2018).

Disclosure to trusted advisors

NAB does not consider that the CDR needs to include the concept of sharing to 'trusted advisors' due to concerns for privacy and security. In NAB's view, current arrangements work to share data with these types of individuals already.

NAB is concerned that the effective supervision of 'trusted advisors' is dependent on the current regulatory oversight that exists outside of the CDR. As noted above, there may be gaps in oversight such as the possibility that individuals are not subject to privacy law. In addition, it is unclear how a person or organisation would qualify for data to be shared with them. Clear directions are needed on how to confirm that the individual holds the relevant qualification.

For many advisors, existing arrangements work well to allow customer data sharing outside the CDR. Further information is at section eight below regarding access to CDR data by brokers.

Currently, NAB has several data-sharing arrangements in place, such as sharing banking information relating to small business customers via accounting software provider Xero. 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.

Disclosure of CDR insights

NAB is concerned about potential for consumer detriment if CDR insights are provided to non-accredited persons. Data insights can have the potential to be more sensitive information that the raw data. For example, detailed transaction history can be used to identify a person's daily movement habits, health status and location.

8. Role of brokers and aggregators

Brokers play an essential role in enhancing competition and enabling access to credit for many Australians. Allowing participation by the Broker Industry is an important part of the CDR and would allow consumers to easily share financial data that is crucial to lending origination. Brokers also enable consumers by assisting with acquiring new lending or switching lenders where data provision is difficult to obtain, collect and move securely. Brokers do so through aggregator business. Aggregators provide platforms and access to client relationship management and lodgement systems in order to assist brokers comply with regulatory obligations and in the application of loans to lenders in the market. NAB is both a lender and the owner of three aggregator businesses, PLAN Australia (**PLAN**), Choice Aggregation Services (**Choice**), and FAST.

NAB recognises that the intention of including brokers in the definition of 'trusted advisors' is to simplify their access to the CDR. However, NAB does not consider that extending the CDR to non-accredited entities in this way will operate to assist brokers in practice.

NAB welcomes further engagement with ACCC and the broker industry to explore how the value chain could be accommodated within CDR. The key will be designing a model for broker access to the CDR that retains privacy and security measures while enabling brokers to participate.

9. Conclusion

The proposed changes to the Rules involve significant amendments to the structure and operation of the CDR. NAB considers that there is risk in adding additional complexity to the regime when it is in its infancy.

Further consultation with participants as well as CX testing should occur prior to the Rule changes being finalised. NAB would be pleased to participate in these discussions.