NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on *Competition and Consumer (Consumer Data) Exposure Draft Rules 2019*

10 May 2019

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

TABLE OF CONTENTS

1. Introduction 3
2. Executive Summary 3
3. Accreditation 4
4. Consent 5
5. Definition of CDR data 6
6. Reciprocity 7
7. Privacy 8
8. Timings 8
9. Conclusion 9

1. Introduction

NAB welcomes the opportunity to respond to the Australian Competition and Consumer Commission's (**ACCC**) consultation on the *Competition and Consumer (Consumer Data) Exposure Draft Rules 2019* (**draft Rules**) to implement 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 contributions to the public policy debate on Open Banking. 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; and
- NAB's October 2018 submission in response to the ACCC's consultation on the Consumer Data Right Rules Framework (**Rules Framework**).

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**).

2. Executive Summary

This submission focuses on key issues where NAB believes refinements are necessary. In some instances, more detail is required so that participants have certainty and clarity regarding the regulatory requirements. In other instances, it is difficult to understand how particular provisions will operate as the supporting legislation, Standards and designation instrument are not settled. Finally, NAB considers that some aspects of the draft Rules need revision.

NAB has previously noted that Open Banking is a complex and significant change to the Australian financial system. To that end, NAB welcomes further clarifications regarding the intended operation of the regime, including the Commission's guidance on their approach to enforcement and compliance.

NAB's key concerns with the draft Rules are as follows:

- **Security implications**: NAB considers that the adoption of a customised Security Management framework creates risk as it does not include a mechanism for monitoring or updating the framework to address new security threats. NAB recommends the adoption of an industry accepted framework for Security Management. NAB also requests that clear timelines are included in the draft Rules with respect to notifications for surrender, suspension or a revocation of an accreditation and for withdrawal of consent.

- **Joint accounts:** The approach to joint account consents in the draft Rules significantly differs from the previous approach, adds technical complexity and may lead to customer frustration. NAB considers that joint accounts should be excluded from Phase 1 to allow the technical issues to be considered and for

further consideration of user experience and appropriate customer education with respect to joint accounts.

- **Reciprocity:** The draft Rules do not include a framework for reciprocal obligations as envisaged by the Review. NAB believes reciprocity is critical to the success of the CDR and requests the inclusion of reciprocity in Phase 1, even in a limited form.

- **Privacy**: NAB's preferred model for privacy would involve the Australian Privacy Principles (**APPs**) being 'turned off' and replaced with the Privacy Safeguards. However, if the current approach is to be maintained, NAB requests clear direction in the Rules regarding the transition from the Privacy Safeguards to APPs.

NAB also requests further clarification as soon as possible regarding:

- the Commission's intended approach to disclosure to non-accredited recipients;
- what amounts to derived data and what amounts to materially enhanced data; and
- what is intended to be covered by the requirement to include customer data held 'in a digital form'.

NAB will continue to engage with Treasury, Data61 and the Commission in the development of the CDR framework, in order to make sure we get this right for our customers.

3. Accreditation

Accreditation requirements

In the October 2018 response to the Rules framework, NAB noted the need for strong accreditation and auditing requirements for CDR participants. In particular, NAB recommended the adoption of an industry accepted framework for Security Management and auditing rather than creating customised frameworks.

The draft Rules outline the security controls for the accreditation process and are a customised framework (**Schedule1, Part 2**). NAB has a number of concerns with this approach:

- **Too prescriptive**: The customised framework in the draft Rules is very prescriptive, which may lead to a minimum compliance approach;
- **Need for review:** Security needs are constantly evolving in response to new threats. The Commission will need to invest time in reviewing and updating the framework frequently in order to address new security threats.

NAB is concerned that the static framework for Security Management in the draft Rules may lead to data breaches or other incidents that undermine confidence in the CDR. Ultimately this could lead to delays in the adoption and usage of the CDR, thereby delaying conferral of consumer benefits.

The concerns above could be addressed by adopting an industry accepted framework or mandating a principle based approach. A principle driven framework would have the advantage of continuing to evolve as threats and technology evolve. If a customised framework for security is to be adopted NAB seeks clarity on how the effectiveness of the

framework would be monitored and maintained to ensure that it keeps up with technical developments and threats.

Ability to transfer data to non-accredited parties

The draft Rules note that the Commission is considering rules authorising the disclosure, with the consumer's consent, of a consumer's CDR data by an accredited person to another accredited person (such as an intermediary) or another person (for example, a consumer's accountant, lawyer or financial counsellor).

In its September 2018 submission, NAB raised security concerns regarding sharing CDR data with non-accredited recipients. NAB requests further details regarding the Commission's intended approach to disclosure to non-accredited recipients, including the security measures, identification requirements and the proposed mechanism for transfer.

4. Consent

Minors

NAB raised concerns regarding the inclusion of minors in its October 2018 submission regarding the Rules Framework. NAB welcomes the decision to exclude minors from the operation of the CDR by excluding persons under 18 from the definition of required consumer data (**Schedule 2, R2.2**).

Joint accounts

The framework outlined in the draft Rules differs from that in the Rules Outline.

Under the draft Rules the data holder must provide a joint account management service which allows joint account holders to individually be able to make consumer data requests, and give and revoke authorisations in relation to the information that relates to joint accounts (**Schedule 1, R3.2(1)**). Data holders can also offer the functionality for joint account holders to elect that both joint account holders can make consumer data requests, and give and revoke authorisations together. Where joint account holders have not made an election prior to sharing data via the joint account management service, the data holder must refuse to disclose data (**Schedule 1, R3.3(2), R3.5(2)**). In practice, this means that a joint account holder may believe they have consented to sharing their joint account data but if the joint account management service was not used first, the data holder must reject the request. This would be a poor experience for customers.

In contrast, the Rules Outline envisaged a joint account management service but included a concept of a 'default position' whereby either joint account holder can provide consent that is subsequently subject to authorisation by the other holder.

In the October 2018 response to the Rules Framework, NAB raised concerns regarding the technical complexity associated with the previous approach to consent for joint accounts. The approach to joint account consents in the draft Rules significantly differs from the previous approach. The lack of certainty means it will be difficult for data holders to build a solution that meets the requirements.

Accordingly, NAB considers that joint accounts should be excluded from Phase 1 of the CDR. Delaying the introduction of joint accounts allows the technical issues to be considered as well as more work to be done on user experience and customer education with respect to joint accounts.

Withdrawal of consent

R4.24 provides that a CDR consumer who gave an authorisation to an accredited person may withdraw that authorisation at any time by communicating the withdrawal to the data holder in writing. NAB considers that this Rule is overly prescriptive, will create additional compliance burdens for data holders and creates a risk that revocation may not be executed in a timely manner.

NAB recommends the inclusion of a Rule that requires data holders to offer a process for offline withdrawal of consents but leaves it open to data holders to operationalise. This would allow data holders to enable withdrawal of consent through existing customer communication channels and support processes, for example the call centre and in the branch. From a security standpoint, this allows data holders to ensure that authentication and authorisation controls are enforced and that withdrawals of consent are actioned promptly.

Renewal / reauthorisation

The Rules outline noted that the Standards may provide for a simplified process for the renewal of consent/authorisation (at **[7.27**]). NAB notes that the draft Rules do not cover a process for reauthorisation or renewal of consent authorisation. NAB considers a Rule should be included mandating the Chair of the Data Standards Body to make Standards regarding the process to be followed where consent expires.

5. Definition of CDR data

Derived data

NAB has consistently raised concerns regarding unintended consequences should derived data be included in the CDR. NAB appreciates the clarification in the draft Rules that 'Required consumer data' does not include derived data.[1] As noted in the October 2018 submission, NAB considers that the expression 'derived data', in the context of the CDR, lacks definition and boundary. Further details are needed to provide certainty regarding the limits of derived data and what amounts to materially enhanced data.

The Bill defined CDR data as including information 'wholly or partly derived' from a class of information specified in the designation instrument. We understand that the definition of CDR data in the Bill intended to provide scope for transformed or value-added data to fall within the CDR regime at a later time. In the Rules Framework the Commission accepted that the terms 'transformed' or 'value-added' can encompass a

1 This is consistent with the Explanatory Memorandum to the CDR Bill which noted that for data that relates to a CDR consumer, the requirement is limited to data that is specified in the instrument and does not include derived data.

spectrum of activities and referred to the concept of data that results from 'material enhancement' as contemplated by the Review.[2]

NAB understands that Treasury intends to amend the designation instrument to provide further clarity regarding what amounts to material enhancement. NAB welcomes the release of the updated designation instrument as soon as Treasury is able to do so.

Clearly defining the limits of derived data and what amounts to materially enhanced data will be crucial for the success of the CDR as a whole. In particular, we note that the draft Rules currently state that fees cannot be charged for the disclosure of required consumer data. However, no concept is currently included for voluntary consumer data or materially enhanced data that may be subject to a fee.

Customer data

The definition of customer data in relation to a particular person means any information that the person provided at the time of acquiring a particular product and relates to their eligibility to acquire a product (**Schedule 2, R1.3**). The definition of required consumer data includes customer data that is held in digital form (**Schedule 2, R2.2(1)(c)**). NAB requests further detail regarding the data sets intended to be covered by this definition, such as whether this includes scanned copies of application forms, payslips or other supporting documentation.

Depending on the definition of 'digital form' this may add significant complexity for data holders, who may not store application forms/other documentation in readily accessible locations. There is potential for this drafting to significantly increase the scope of data to be provided in the CDR and accordingly, NAB welcomes clarification as soon as possible.

NAB also notes that the definition of customer data still includes details such as phone numbers. NAB has previously raised security concerns regarding sharing customer Personally Identifiable Information (**PII**) via API,[3] particularly given that phone numbers are often used for second factor authentication for security purposes.

6. Reciprocity

NAB has previously noted that it considers reciprocity is a fundamental principle in order to create a level playing field for all participants. Recommendation 3.9 in the Review supported reciprocity via 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.'

NAB welcomes the inclusion of **R5.2(e)** which requires persons applying for accreditation to indicate whether it is or expects to be the data holder of any CDR data that is specified in a designation instrument. This Rule provides a platform for inclusion of a limited form of reciprocity at a later date.

---

2 See Recommendation 3.3 of the Open Banking Review.
3 See NAB's response to Decision Proposal 26 of the Consumer Data Standards: https://github.com/ConsumerDataStandardsAustralia/standards/issues/26#issuecomment-431314876.

However, as noted in NAB's October 2018, March 2018 and September 2017 submissions, NAB considers that reciprocity should be broader and encompass that which was intended in the Review. NAB considers that reciprocity necessarily involves 'equivalent transaction data' being shared by non-authorised deposit-taking institutions (**ADIs**) who choose to participate in Open Banking.

NAB believes the inclusion of a more expansive definition of reciprocity will give consumers more choice and opportunity to participate in the CDR and support the growth of the data economy. Not addressing reciprocity in phase 1 would allow non-ADIs to receive data from ADIs at the request of customers, but have no ability for customers to request that comparable data be transferred to other entities until a later, unknown date. This would not be a level playing field.

NAB acknowledges the complexity associated with inclusion of full reciprocal obligations as envisaged by the Review. However, given the limited form of reciprocity currently contemplated NAB considers this should operate from the Phase 1 commencement of Open Banking.

7. Privacy

NAB provided detailed feedback in its September 2018 submission regarding the privacy framework in the CDR Bill. NAB maintains its concern that the current regime is too complex and imposes a significant compliance burden on data holders and accredited data recipients to determine whether the customised Privacy Safeguards or the APPs apply to a particular disclosure.

For instance, we note that credit providers have obligations under Part IIIA of the *Privacy* Act 1988 in relation to the correction of credit related personal information and related notification requirements. Part IIIA sets out where the APPs apply and where the Part IIIA provisions apply. The draft Rules and CDR Bill also include Privacy Safeguards that apply in relation to the correction of CDR data. As a consequence, there is significant complexity when considering how to comply with requirements in relation to correction of CDR data that is credit related personal information.

NAB's preferred model would involve the APPs being 'turned off' and replaced with the privacy safeguards. However, if the current approach is to be maintained, NAB requests clear direction in the Rules regarding the transition from the Privacy Safeguards to APPs.

8. Timings

In a number of instances, timing for critical matters is not defined in the Rules. For instance:

- **Withdrawal of consent:** if a consent to collect particular CDR data is withdrawn, the accredited person must notify the data holder of the withdrawal, however no timeframe is specified (**R4.11**). While **R8.**11 provides that Standards can be made regarding these matters, these are not yet defined in the data standards.

- **Revocation / surrender of accreditation:** Similarly, **R4.25** provides that if an accredited person's accreditation is revoked or surrendered, all authorisations for a data holder to disclose expired when the data holder is notified. However, no timeframe for notification is included.

- **Notifying Accreditation Registrar of surrender/suspension/revocation: R5.20** provides that the Data Recipient Accreditor must notify the Accreditation Registrar of a surrender, suspension or a revocation of an accreditation 'as soon as practicable'. NAB believes it is critical that this notification occurs in real time given the security implications of data holders providing data to recipients who no longer hold accreditation.[4]

NAB raised concerns regarding timely provision of updated accreditation information in its September 2018 submission. In particular, NAB noted that notification needs to occur in real time to customers and data providers. NAB considers that clear timelines should be mandated for these matters, given the potential for data leakage or other security incidents.

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 the potential for enhanced customer outcomes.

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

[4] NAB also notes the importance of dynamic registration in the directory design (see comments in response to the Consumer Data Standards https://github.com/ConsumerDataStandardsAustralia/infosec/issues/63#issuecomment-483948040).