NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on *Consumer Data Right Rules Framework*

12 October 2018

TABLE OF CONTENTS

1. Introduction

NAB welcomes the opportunity to respond to the Australian Competition and Consumer Commission's (ACCC) consultation on the *Consumer Data Right Rules Framework* (Rules Framework); which addresses rules to be made by the ACCC to implement the Consumer Data Right (CDR).

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

- NAB's September 2017 submission (September 2017) to the Review into Open Banking (the Review);
- NAB's March 2018 submission (March 2018) in response to the Review;
- NAB's September 2018 submission (**September 2018**) in response to the *Treasury Laws Amendment (Consumer Data Right) Bill* 2018 (**CDR Bill**); and
- NAB's October 2018 submission (October 2018) in response to Treasury's further consultation on the CDR Bill.

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

NAB supports the introduction of the CDR and its application to the banking sector via Open Banking. NAB remains very cautious about the proposed timeframe for implementation, given the potential for adverse unintended consequences that could undermine the purpose of CDR and Open Banking. Implementation of this significant initiative must ensure that customers' data and privacy is secure at all times, engendering trust and confidence in the system.

NAB agrees with the ACCC's views on a number of issues, including the proposed approach to former and offline customers, joint accounts, requirements for insurance and restrictions regarding on-selling and direct marketing.

NAB has concerns regarding security implications of some aspects of the framework. This includes the sharing of customer account numbers and payee lists, approach to redundant data, provision of data to consumers via open APIs and transfer of CDR data to non-accredited entities. NAB also has concerns regarding privacy obligations, the approach to consent for minors and the potential requirement for value-added descriptive data to be transferred under the CDR.

Finally, NAB provides factual information regarding how its data is stored, categorised and accessed by customers, which in some instances creates challenges with respect to sharing certain data sets.

3. Who may take advantage of the CDR?

NAB welcomes the ACCC's proposed approach of only including current online customers in the first version of the Rules. There are significant complexities associated with verifying and authenticating former customers and with establishing mechanisms for customers who do not use or have access to internet banking.

4. Data set inclusions and exclusions

NAB raised concerns in its September 2018 submission regarding the definition of 'derived data' and whether this covers 'value-added' data. NAB will provide further feedback on the issue of derived data in its October 2018 submission to Treasury.

NAB is also aware that the ACCC is considering requiring value-added descriptive data associated with CDR data (eg. transaction activity for customers which includes the location or trading name for the merchant) to be transferred under the CDR. NAB acquires this data from third parties at a significant cost and NAB is concerned regarding its compliance with contractual obligations to third parties if the data is required to be disclosed. Furthermore, if this data is required to be provided under the CDR at no cost, it could undermine incentives by third parties to create such data sets in the future. NAB welcomes further information and opportunities to engage with the ACCC on this matter.

The Rules Framework sets out proposed data sets to be included in the Rules. Below are NAB's views on the proposed customer data, transaction data and product data sets.

Customer data

NAB welcomes the decision not to include identity verification assessments in the first version of the Rules. In relation to the types of customer data proposed to be included:

- Authorisations on the account: NAB welcomes further information regarding what data the ACCC intends to capture. NAB recommends that any customer or product data associated with an account be classified and defined as account data.
- Unique identifiers: NAB also seeks further information on what the ACCC considers to be unique identifiers. Accounts have a number of unique identifiers and these may not be standardised across the industry. For example, complications arise if some unique identifiers (such as passport or Medicare numbers) are proposed to be shared as these are often used to verify customer information on independent Government databases.
- Customer account numbers: NAB has security concerns regarding the sharing of customer account numbers given that this is confidential information that may contain Personally Identifiable Information (PII) and may represent sensitive payment data. Customer account numbers for cards are usually the primary account numbers (PANs) (i.e. the number printed on a customer's debit or credit card). Sharing PANs involves sharing a customer's payment facility and has the potential for misuse and subsequent fraud. In addition, sharing of sensitive payment data such as PANs is subject to onerous obligations under PCI-DSS. It is NAB's strong preference that such data be excluded from the CDR. However, if it is to be included, the ACCC / Data61 should require that the data to be masked/tokenised prior to sharing.
- Payee lists: Payee lists include PII and sensitive payment data that belongs to other customers. The transfer of this data would effectively involve transfer of CDR data whereby the individual to whom it relates has not consented to the transfer.
- Direct debit authorisations: It is not technically possible to provide direct debit information as banks do not hold the information because it is originated by the merchant.

Transaction data

NAB's specific comments regarding proposed data sets are as follows:

- **Account balances:** NAB does not store a balance prior to and following each transaction. However, NAB can determine a balance for specified periods based on whole days (from midnight). NAB currently reconciles balances at the end of each business day for an account, via batch processing of payments, rather than updating balances intra-day. This ensures that customers' balances reflect all debits and credits throughout the day, avoiding the potential for temporary negative balances due to the sequence and speed of transaction processing. NAB believes only end of day balances should be included in the CDR data sets.
- Identifier for the counter-party to a transaction: The identifier is only available for some transaction types. For instance, for incoming international payments, NAB may not have the ability to provide an identifier for the counter-party. Accordingly, NAB is concerned regarding its ability to provide this data set.
- Metadata: Metadata is a broad term that covers a wide range of data types. NAB considers that there are two types of metadata, being operational metadata and security metadata:
    - Operational metadata: this is discussed in the Rules Framework document, being metadata associated with the execution of the transaction. It may include an IP address, geospatial location and device data fingerprint. This type of metadata is not easily standardised and varies greatly between different users and use cases. NAB's systems are designed to record and manage the "data" of the transaction and the metadata collected at the time of the transaction is not tagged or stored in ledgers. Consequently, NAB does not have the capability to capture this metadata and share it via the CDR.
    - Security metadata: at the time a customer provides consent to share data under the CDR and when CDR data is actually shared between CDR participants, security metadata will be created. Security metadata is the data that is associated with the CDR data exchange process (suggested metadata fields include field data type, technical name, business name, business definition, reference value lists (e.g. ANZSIC code), value constraints, cardinality against other elements, etc). NAB considers that there are security benefits in requiring CDR participants to capture and store this security metadata. Security metadata could be used to inject integrity and non-repudiation controls such as an electronic signature (i.e. crypto hash) containing the data originator and data recipient identifiers. This information would assist forensic investigations in the event of fraud and data leakage.

Product data

NAB understands that the intent of sharing interest rate data is to enhance competition. However, as detailed below, there are challenges to providing interest rate data for a specific customer in relation to some products. Accordingly, NAB considers that a better approach is not to mandate sharing of interest rate data and instead, accredited recipients can receive customer transaction data. By providing customer transaction data, third parties will be able to review the information and see the total picture (ie. transactions, monthly fees, actual interest paid). Third parties will be able to use this data to make compelling offers to customers. Importantly, using actual cashflow data will help ensure that third parties can properly compare products across financial institutions.

In relation to product data that relates to an identifiable or reasonably identifiable person, there are challenges associated with providing interest rate data. For some retail deposit products the tiered or bonus interest rates are disclosed in the product terms and conditions, and the account statement shows the amount of interest paid, not necessarily the interest rate for a particular period. For example, NAB's Reward Saver Account is a savings account which currently pays a variable base interest rate of 0.5%, and then a bonus interest rate of 2.00% if a customer makes at least one deposit before the second last banking day of the month, and no withdrawals. Therefore the interest rate paid on that account is dependent on customer behaviour, and can vary from month to month.

In addition, care needs to be taken to ensure that any interest rate shared as part of CDR is accurate and that calculations are consistent across data holders. It would be undesirable for customers if data providers were required to make assumptions or best estimates regarding interest rates. To this end, NAB welcomes further guidance on specific details of interest rate calculations, including:

- Approach to interest rate calculations where customers have a tailored interest rate due to acquiring a package or bundle of products (e.g. a mortgage and credit card);
- Whether calculation of an effective rate will be required (i.e. incorporating interest rate, fees and value added aspects);
- The temporal element to interest rate calculations, specifically the complexities in calculating rates outside the statement period. Products with a behavioural element in particular would require assumptions to be made to determine the estimated interest rate or fees outside of the statement period. This complexity could create confusion for customers depending on how the third party chooses to present the offer.

For mortgages, every customer is considered individually which often involves a negotiated rate which reflects a range of factors, including the bank's proprietary credit scoring model.

Given NAB's concerns with i) the complexity of calculating some interest rates out of statement cycle for specific customers and ii) disclosure of its competitive offering, NAB recommends following the UK approach. Under the UK Open Banking API specifications interest rates for customer accounts are not exposed. Interest rates in the UK regime are only provided with respect to generic product data. This would ensure simplicity, transparency and consistency across the industry without compromising the ability of third parties to provide compelling offers to customers.

5. Accreditation

NAB supports strong accreditation and auditing requirements for CDR participants. NAB recommends the adoption of well recognised frameworks to govern the entire Open Banking / CDR ecosystem that will host customer sensitive data as ensuring the security and integrity of the system is best for customers. Third-parties must be governed, accredited and audited based on such standards and adopt consistent operational practices to manage their environment.

NAB recommends the adoption of an industry accepted framework for Security Management and auditing rather than creating customised frameworks. If a customised framework was required this would increase compliance costs for both data holders and accredited data recipients.

6. Consent

Who can provide consent?

Joint accounts

NAB supports the ACCC's proposed approach with respect to joint accounts. As noted in its September 2018 submission, NAB believes the most feasible method is for consent on joint accounts held by customers to be based on the authorisation process for accessing the account via internet banking. That is, if a customer is able to login to access a joint account, then they should be required to provide consent for any data sharing arrangements under the account. This may involve each joint account holder being notified of any data transfer arrangements initiated on the accounts and given the ability to readily terminate any data sharing arrangement initiated by other joint account holders.

NAB considers that this approach to consent for joint accounts appropriately recognises the value of CDR data. However, this solution does introduce technological complexity and is likely to impact timeline for delivery. Including single accounts only in Phase 1 may be a technically simpler approach that still provides a large number of customers with the ability to participate in Open Banking. NAB estimates that around 70% of its transaction accounts (Classic, Retirement and Passbook) are single authority.

Complex accounts

As noted in its September 2018 submission, further work is needed for business 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. NAB recommends that sharing on complex accounts is delayed to allow customers and banks to put specific authorities in place.

Minors

NAB considers that accounts held by minors should not be captured as part of the CDR.

The ability for persons under 18 to give their consent under Australian law is a complex topic which is governed under various state based laws. Historically, under Australian contract law, it was deemed that a person under 18 may be unable to understand the full implications of a legal contract and therefore lacks capacity to enter into a legally binding contract. While a consent is a different instrument to a contract, similar considerations apply. For example, where consent must be "informed", a person with a special disability (such as infancy, which is defined as being under age 18), may potentially lack capacity to give an informed consent.

For completeness, we note that certain state based laws deal specifically with minors giving consent in particular situations and contexts.[1]

NAB considers that the preferred approach is for minors to be able to share their data, only where a parent or guardian has provided authority for the transfer. Given the additional complexities involved in implementation of this solution, NAB considers that inclusion of CDR data belonging to minors should be deferred to subsequent versions of the Rules.

[1] *Minors (Property and Contracts) Act 1970 No 60* (NSW); Section 7 of the *Goods Act 1958* (Vic).

Other matters

Redundant data

NAB is concerned about cyber vulnerability and privacy implications for redundant customer data. Accordingly, NAB considers that customer data stored within an accredited data recipient should be destroyed once it becomes redundant.

From a security standpoint, there is a risk that data de-identification processes may fail to fully cleanse customers' confidential information, leading to privacy issues and increasing the risk of data leakage.

On-selling and direct marketing

NAB agrees that customer data acquired via CDR should not to be on-sold by data recipients or used for direct marketing. There is a risk that on-selling such data will facilitate data leakage, fraud and reputational damage to the entire CDR scheme which would impact consumer confidence in the scheme.

7. Authorisation and authentication processes

Some aspects of the authorisation and authentication process outlined in the Rules Framework raise concerns from a security perspective. Some key issues include:

- Service level standards: In relation to service level standards, NAB considers that they should be addressed in both the Rules and Standards, with consistent definitions across the documents. The Rules should specify high level principles and provide some input to service levels. The Standards should be much more granular and provided detailed requirements as needed.
- Management of consent authorisation and revocation via a single portal: NAB proposes that revocation of authorisation is performed on the same channel where authorisation was granted in the first place. That is, on the data holders' consumer dashboard. From a security perspective, this provides a consistent approach to the consumer and assurance that the consent is truly terminated (at the origin where it was originally granted). In addition, it eliminates the need for data holders to expose an API with right/delete access for consent revocation, improving security by reducing the landscape for vulnerabilities.
- Suspension of access: NAB considers that data holders should be empowered to suspend a recipient's access in limited circumstances. Data holders will be the first targets of cyber-attacks on exposed APIs. Accordingly, NAB's view is that attacks must be mitigated in real-time to ensure the security of the CDR. This would involve a data holder temporarily suspending access in circumstances where an incoming cyber-attack is detected. Options to do so would include by blocking network traffic and/or suspending credentials / tokens while a security incident response is conducted, involving the relevant regulator and the accredited data recipient. The technical working groups could work to define specific abuse-cases that can be manually or automatically triggered once specific events occur or thresholds are exceeded.

8. Providing data to consumers

NAB has no concerns with providing customers with copies of their own CDR data. Today, NAB customers can collect their transactional data via their internet banking portal (as CSV files) or share it directly with accounting software providers such as Xero or MYOB. NAB has a data-sharing arrangement in place with Xero whereby small business customers can share their banking information directly with Xero via their internet banking account.

However, NAB considers that providing data to consumers via API access creates a major security risk. NAB is concerned this may lead to creating of non-authorised API based apps which will capture and store customer secrets (tokens/password/API keys) and collect and withdraw customer data.

9. Use of data

NAB has significant concerns regarding the security implications of sharing CDR data with non-accredited entities. NAB provided further detail regarding this issue in its September 2018 submission to Treasury.

Allowing CDR data to be transferred to non-accredited entities, however rarely, 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 contradiction to this and NAB believes that only accredited entities should be able to receive CDR data. As noted at **Section 2** above, security of customer data is fundamental to the success of the CDR.

10. Reciprocity

NAB strongly supports the principle of reciprocity. NAB provided detailed feedback regarding the issue of reciprocity in its October 2018 response to Treasury's further consultation. NAB also previously addressed reciprocity in its September 2017, March 2018 and September 2018 submissions.

11. Privacy Protections

NAB has consistently stated that the protection of the confidentiality of customer data is critical to the success of the CDR regime (see discussion at **Sections 2**, 5 and **9** above).

While the proposed amendments to the CDR Bill aim to reduce the complexity of the privacy framework, NAB considers that the approach remains overly complicated and creates uncertainty and duplication. Further information is provided in NAB's September 2018 submission.

12. Conclusion

The CDR is a significant initiative for the Australian economy. It will encourage a new data economy which better recognises the value of data and empowers consumers to make use of their data in a safe environment. Open Banking in particular has the potential to increase competition and enhance customer outcomes. However, these benefits will only be realised if Open Banking is implemented at the "speed of safe" and the unnecessary complexity described in this submission is avoided.

The development of the framework for the CDR and the regulation of Open Banking remains complex and challenging. NAB looks forward to further and ongoing engagement with the Department of Treasury, the ACCC and Data61.