NATIONAL AUSTRALIA BANK SUBMISSION

Inquiry into Future Directions for the Consumer Data Right

May 2020

Introduction

NAB welcomes the opportunity to provide a submission to the Inquiry into the Future Directions for the Consumer Data Right (Inquiry). NAB appreciates the extension granted by the Inquiry for written submissions. As a member of the Australian Banking Association (ABA), NAB has also contributed to the ABA submission.

This submission is in addition to past submissions that NAB has made to Treasury and to previous reviews in relation to Open Banking and the Consumer Data Right (CDR) since 2017. NAB has focused its response on the key topics and questions on which the Inquiry has sought feedback.

Executive Summary

NAB supports Open Banking via the CDR as it will give customers greater control over their own data and offers potential new ways for banks to innovate, as well as encourage more competition through new entrants. The CDR therefore presents an opportunity for NAB, as well as our customers. NAB is supportive of extending the CDR to other industries such as energy and telecommunications.

A fundamental overarching principle in considering the future direction of the CDR is the importance of ensuring a level playing field for all participants. Authorised deposit-taking institutions (ADIs) should not be placed at a competitive disadvantage to benefit other industry participants, but instead all participants should be required to compete with others under the same regulatory and legislative framework. Two areas where NAB believes there is potential to improve customer experience within a digital economy are through integrated payment systems and digital identification. NAB believes that the best payment system to be utilised through Open Banking is the New Payments Platform (NPP) and believes there is merit in waiting until key parts of the NPP roadmap are rolled out before integrating this functionality into Open Banking. NAB also believes that there is potential for Digital ID services to support the CDR infrastructure.

NAB believes that any expansion of the scope of Open Banking to areas such as write access should only occur after an assessment of whether the initial Open Banking regime is working as expected. Payment initiation should also remain separate to the other functionalities of write access and each use case should be reviewed independently to assess the different exposures and risks which pertain to them. NAB also supports the establishment of a centralised cyber security capability (distinct from the current internal CDR capability) with the responsibility for coordinating and managing responses to cyber-security incidents, intelligence gathering and other security measures. NAB also makes comment on the increased liability and fraud detection risk which come with write access, as well as the need for higher levels of accreditation if write access were to be permitted.

Where the Issues Paper references leveraging CDR infrastructure, NAB encourages the use of pre-existing standards where possible and developing open standards rather than defined mechanisms to improve the efficiency of the system and to ensure there is room for innovation and competition. Finally, to ensure that vulnerable customers are protected, NAB encourages a sound accreditation

process with potentially higher levels of accreditation for those actively seeking vulnerable customer information.

1. International context

The inquiry invites submissions on how the CDR can be leveraged with international developments of the kinds described above to enhance opportunities for Australian consumers, Australian businesses, and the Australian economy.

NAB believes it is useful to view the developments and implementation of overseas versions of Open Banking, primarily in the UK, to inform the approach being undertaken in Australia, whilst understanding that there is merit in having a uniquely Australian approach to CDR. Of particular interest is the phasing of implementation, and the security and regulatory settings of Open Banking in the UK. Dr. Chris Michael, Chief Technology Officer at the UK Open Banking Implementation Entity (OBIE), has noted that Open Banking should not be viewed in terms of one-off implementation.[1] NAB agrees with this view and believes that there needs to be a resilient and scalable platform implemented prior to extending the CDR across the digital economy, to ensure the safety and security of the platform and its users.

Bain and Co have identified a three-stage evolution of Open Banking in their insights paper 'Open Banking in Australia: An opportunity to regain trust'. The three stages involve a phased approach from establishment to open-data infancy, which includes ensuring certain aspects of the CDR are mature prior to integrating new services such as digital identification and payment initiation, and lastly the final stage where Open Banking becomes pervasive in customers' lives as the CDR is expanded into multiple sectors, thereby creating a digital economy.[2]

The establishment phase is critical to build trust in the infrastructure and requires a pause in the expansion of other features to businesses and consumers, until they have familiarised themselves with the basic services and nature of CDR.

Australia, having legislated an economy-wide data sharing right, has an opportunity to act as an international leader in this area and is therefore well placed to help create a more competitive and innovative digital economy by expanding the CDR into other sectors.

[1] Riley, J (2018), 'Australia's Open Banking Journey', *Innovation Aus,* available at https://www.innovationaus.com/australias-open-banking-journey/

[2] Bain & Co (2019), 'Open Banking in Australia: An Opportunity to Regain Trust', available at https://www.bain.com/insights/open-banking-in-australia-an-opportunity-to-regain-trust/

2. Linkages and interoperability with existing frameworks and infrastructure

The inquiry welcomes input from interested parties on the above, including potential linkages and interoperability with other consumer-directed domestic and international data portability regimes, and accreditation frameworks that focus on data risk management.

NAB agrees with the statement in the Issues Paper that the "CDR regime seeks to build upon and complement the arrangements businesses use and not to displace them". NAB encourages competition and innovation and is committed to ensuring customers, over systems, are the focus when assessing the suitability of frameworks and infrastructures to link in with the CDR. Two areas where NAB believes there is potential to improve customer experience within a digital economy are through integrated payment systems and digital identification.

<u>Payment systems</u>

Payment systems are a critical framework if the CDR were to be extended to write access. Payment systems require user confidence, resilience, trust and security to be stable and sustainable. They also need strong identification of payment initiators, assurance of payment receivers and robust exception and dispute handling to ensure consumer protection.

a) Payment system type

Payment systems should be considered for suitability to ensure that integration with CDR write access is appropriate. NAB does not consider it necessary for the CDR to create a separate, dedicated payment and settlement mechanism for payments or payment initiations. Schemes such as the NPP, which uses ISO20022 standards for messages, are suitable as they ensure appropriate message details, assurance and exception handling. Systems such as Bulk Electronic Clearing System (BECS) carry insufficient data to ensure traceability to support fraud and cybercrime monitoring, so are less suitable for secure Payment Initiations resulting in assured payments.

Whilst acknowledging the CDR will prefer to be payment method agnostic, NAB believes that the best payment system to be utilised through Open Banking is the NPP. The UK implementation, while inclusive of write access, defaults to UK fast payments for payment initiation. NAB considers it would be in the best interest of consumers to wait until the payment initiation and mandated payment service elements of the NPP roadmap are built and tested so a fully functioning and comprehensive payment system can then be integrated with the CDR infrastructure. NAB believes it would be inefficient to use older payment systems such as direct entry, as the trend of migration from BECS to NPP is likely to accelerate in the next few years. Another advantage of aligning to the NPP roadmap is that it will provide a strong model of how key functionality that supports Open Banking (i.e. third-party payments, direct debits and refunds) can be achieved.

The intent of the CDR is to give consumers more access to and control over the use and sharing of their data with appropriate security protections and NAB agrees that this should extend to a consumer's payments. Most payment types (except for cheque and direct debit) are irrevocable, so any model of payment initiation included in the CDR needs to satisfy consumer protection

expectations, including enabling fraud detection, consent verification, unauthorised transaction recovery, and indemnification to the payer institution from the Payment Initiator.

It is also noted that if payment initiation via write access is allowed, financial institutions will lose the ability to monitor and respond to digital malware threats as the user experience layer is no longer delivered and governed by the financial institution, thereby opening up opportunities for criminals. An option is to enable the inclusion of digital malware detection as part of the ecosystem or allow data holders to embed security mechanisms in accredited entities software products. It is also expected that NAB would maintain autonomy outside of the CDR in cases where the CDR Register of Accredited Entities is unavailable.

b) Payment Initiation and indemnity

In most payment systems with a credit flow where the payer creates the instruction, the payer organisation indemnifies the payee organisation for applying the payment in accordance with the payee details sent in the instruction. In payment systems where the instruction is created by the Payment Initiator (a third party to the payer whether on the payer side or creditor side), the Payment Initiator indemnifies the payer organisation for creating the payment instruction, i.e. liability shifts from the payer organisation to the Payment Initiator. Indemnification in the CDR as it stands is primarily concerned with data breaches and contains an element of 'buyer beware' on the part of the consumer and assumes adequacy of insurance on the part of the accredited data recipient to cover liability. In a write access and Payment Initiation model, Payment Initiators may not be ADIs but will need to be suitably capitalised to ensure they are able to cover claims for unauthorised transactions to ensure customers are protected. Financial institutions acting on Payment Initiations and consequently removing funds from customer accounts will need confidence that Payment Initiations are occurring under payment models or schemes that are robust, resilient and allow the financial institution to meet capital, risk exposure and regulatory requirements.

Digital identification

As the uses of the CDR evolves, NAB expects a greater need for stronger forms of customer authentication. Digital ID is one of many ways of achieving this authentication. NAB believes that there is potential for Digital ID services to support the CDR infrastructure.

Digital ID has broader use cases than just the CDR and therefore the focus should be on creating a level playing field for competition through open standards rather than mandating specific standards or mechanisms. Defined mechanisms risk stifling innovation and acting as a commercial deterrent to building Digital ID capacities. The EU approach to Digital ID involves providing rules and principles but not mandating solutions or technology, thereby preferring open standards over defined mechanisms. Setting open standards would help to future-proof the CDR for emerging technologies.

There is an emerging industry around Digital ID services including the standards set by the Australian Payments Network's TrustID framework and the Digital Transformation Agency's Trusted Digital Identity Framework (TDIF) as well as public and commercial offerings such as Australia Post's Digital ID, MyGovID and pilots through Mastercard and EFTPOS. To illustrate the increasing

momentum of the industry, the Australian Payments Network has had multiple parties express interest in becoming accredited under TrustID. NAB encourages a consultative and integrated approach to developing open standards, which can then be leveraged for use under the CDR.

Other obligations

While supporting CDR interoperability with both digitally enabled payment systems and digital identity and identification, NAB is subject to domestic and international Anti-Money Laundering Counter-Terrorism Financing (AML/CTF) and Sanctions regulatory requirements. This includes requirements for a range of customer actions and authorisations such as payment initiation, and payment execution obligations. Adherence to these requirements is an important part of NAB's prevention of financial crime. Existing financial crime requirements (both domestic with extraterritorial application and international) for Australian ADIs should be explicitly considered when requirements are being developed for the interoperability of the CDR with the payments system. By way of example, limiting the interoperability to domestic payments in Australia (i.e. no payments that cross borders) would reduce the number of requirements that need to be considered. Additionally, any write access model in these domains needs to ensure that customers are not put at an increased risk and that ADIs are not disadvantaged in being able to comply with obligations that may not apply to non-ADIs.

In relation to Know Your Customer (KYC) requirements, as was noted in the 2017 Review into Open Banking, with limited exceptions, the current AML/CTF framework in Australia does not support the reliance on customer identification completed by other parties.[3] If the relevant obligations were changed, data recipients could rely on another entity's assessment. While this may be legally permitted, ADIs would need to assess their own risk appetite in relying on such a process. Without robust benchmarking of standards, ADIs may not be able to validate the authentication and verification standards of the organisation who undertook the assessment. Given this, ADIs may still choose to undertake their own identification and verification actions and possibly even perform further KYC processes on a customer or their proposed agent even if they could legally rely on another entity's KYC assessment. This could particularly apply where the customer or ADI involved had exposure to regulations in other jurisdictions, regardless of the ultimate action occurring in Australia.

[3] See Review into Open Banking, December 2017, p. 39.

3. Write access

The Inquiry is interested in interested parties' views on these issues. In the context of Open Banking, the Inquiry is particularly interested in interested parties' view on how the Consumer Data Right could best enable payment initiation.

NAB acknowledges the possibility of extending the CDR to write access and the potential benefits that this could offer consumers and financial institutions. In terms of when this could occur, and as previously stated, NAB believes that any expansion of the scope of Open Banking to areas such as write access, should only occur after an assessment of whether the initial Open Banking regime is working as expected. This assessment should consider whether the intended outcomes are being achieved and the value that customers are deriving from Open Banking.[4]

As noted above, a fundamental overarching principle to consider is the importance of ensuring a level playing field for all participants under the CDR. ADIs should not be placed at a competitive disadvantage to benefit other industry participants, but instead be required to compete with others under the same regulatory and legislative framework.

Write access incorporates many distinct functions which possess different benefits and risks. NAB believes that each of the use cases in write access should be considered differently. Types of write access use cases include:

- A payment instruction;
- A service request;
- A purchase; and
- Account opening or closure.

Payment initiation should remain separate to other functionalities of write access. Furthermore, within each use case there are different exposures and risks which need to be identified and resolved. NAB recognises that there are potential benefits for consumers and financial institutions from allowing write access.

Benefits/potential use cases for consumers include:

- Bill management and payment
- Personal financial management, including transferring funds and investment management
- Savings propositions by roundup or account sweeping across multiple financial institutions
- Simplified account management such as change of address across multiple institutions and sectors. For example, the CDR could automate the process for changes of address after moving properties by allowing a single consumer direction to update their address with all providers they use within the CDR (such as banking, telecommunications, energy). As noted in the Issues Paper, this could reduce the time that consumers spend on life administration.

Benefits for financial institutions include:

- Opportunities to win customers through differentiation of customer experience

[4] See NAB submission to the Senate Select Committee Inquiry into Financial and Regulatory Technology, December 2019.

- Personalisation of offers with the ability to open and transact immediately
- Operational efficiencies from reduced manual handling

There are also risks for both consumers and financial institutions from write access. These include:
- Consequences of fraud are significantly higher with write access. There needs to be additional protections both at the front end (authorisation/verification) and the back end (liability frameworks)
- Consideration of whether a higher threshold should exist to become an accredited data recipient (ADR) where write access is required.

Enhancements to CDR regime required under write access

NAB believes that the existing governance structure and accreditation requirements for CDR would need to be reconsidered in the context of an extension to write access. To mitigate the significant increase in security and fraud risks because of write access, NAB advocates for a centralised CDR cyber-security capability to be established. This capability should be focussed across the whole CDR ecosystem and be responsible for coordinating and managing responses to cyber-security incidents/data breaches, cyber-security intelligence gathering including intelligence sharing and collaboration with ADRs and data holders. This should be separate to the internal security capability of the CDR Register.

NAB believes that the current consent authorisation authentication requirements for the CDR would not provide sufficient security under write access. Currently, consent authorisation does not extend to the authorisation to act on a customer's behalf for use cases such as payment initiation. If the consent authorisations were not enhanced, NAB believes that CDR activity would face a greater level of cyber security risk.

Liability and fraud detection risk

Liability remains a key concern in relation to write access. NAB currently relies heavily on an in-depth understanding of the user and their device through tools embedded in the way that customers choose to interact with NAB (such as internet banking, mobile applications). This understanding determines the fraud and financial crime risk that a user possesses. If third-party providers can make applications on behalf of a consumer, financial institutions lose this ability. As a result, banks may need to be more conservative in approving applications lodged via Open Banking, which could result in longer processing times and subsequent reduced benefit to consumers. To help prevent this challenge, the data collected and shared with the receiving financial institutions under write access should be expanded to enable more effective fraud controls. Non-ADIs should also be required to share this information with the receiving financial institution to ensure they are competing on a level playing field with ADIs.

Accreditation

The current accreditation process for ADRs would also need to be uplifted if write access were permitted. To respond to this level of potential threat, NAB supports the introduction of a tiered model in accreditation and enhancing the role of the central CDR security function in the

accreditation and audit process of ADRs. Further, a significant re-think of the 'Consumer to Accredited Data Recipient to Data Holder' security authentication and authorisation model needs to be considered, with additional authentication for high value CDR actions, such as payment initiation.

From a regulatory architecture perspective, it would be prudent for APRA to have greater involvement in the accreditation process, particularly if the CDR were extended to write access as the ACCC may not be the most appropriate body to consider liability flows in payments when undertaking the accreditation process.

4. Leveraging CDR infrastructure

The Inquiry welcomes views on the above as well as any broader role that other aspects of the Consumer Data Right regime could play in supporting productivity and data security in the digital economy.

The infrastructure being developed for CDR and other initiatives, such as Digital Identity and the NPP, offers the potential to be transformative for Australia. Innovative technology infrastructure should be considered holistically to ensure that ongoing investment is made in areas that will deliver enhanced outcomes for customers and promote the development of an innovation ecosystem.[5]

NAB believes there are multiple elements to the above question. Firstly, determining which elements of CDR are mature enough to be leveraged and secondly, which elements still require maturity. NAB encourages the leveraging of pre-existing standards where possible and developing open standards rather than defined mechanisms to improve the efficiency of the system and to ensure there is room for innovation and competition. The Issues Paper makes specific reference to the Data Standards Body, information security standards, and accreditation as areas in which the CDR have established solutions and or frameworks which can be leveraged to enhance other elements of the digital economy.

NAB believes that there is still further work required on areas such as joint accounts, complex accounts, security standards and accreditation processes. The Government could also consider governance consolidation to ensure that new and pre-existing standards are linked. To promote the role of CDR in the digital economy, greater governance consolidation should be addressed to ensure synchronicity not only in accreditation but in other standards such as security too.

[5] See NAB submission to the Senate Select Committee Inquiry into Financial and Regulatory Technology, December 2019.

5. Consumer protection

The Inquiry invites submissions from interested parties on how to ensure that, as the Consumer Data Right develops, it does so in a manner that is ethical and fair, as well as inclusive of the needs and choices of all consumers. This includes ways to encourage socially beneficial uses for the Consumer Data Right.

NAB believes that consumer protection is of the utmost importance, particularly in a CDR construct where data sharing becomes easier. To mitigate any risk that vulnerable customer data falls into the wrong hands, NAB sees the importance of a sound accreditation process, and potentially a higher level of accreditation for third-party providers who seek specific access to use vulnerable customer data.

Banks, which are subject to the highest levels of accreditation by attaining an ADI license, have relatively new obligations to manage vulnerable customers and their data differently, through changes to the Banking Code of Practice. Similar lines of thinking should be considered for other recipients of this data to ensure that a collective responsibility is recognised where appropriate for those working with customers experiencing vulnerability.

Further, within a CDR structure it is expected that the Data Holder will not be managing the digital front end of the customer experience, which is where dynamic authentication controls are implemented. At this point, NAB is usually able to employ Step-Up Authentication as a method of elevating assurance in NAB's interaction with the right customer, particularly for sensitive actions such as personal details changes, updating security configurations, payment flows and for vulnerable customers. NAB would expect that this method of consumer protection be maintained, allowed and provisioned for in the CDR rules.

Additionally, NAB notes the many benefits and uses of CDR in promoting consumer protection. For example, consumers facing hardship would be able to flag this centrally through the CDR which would result in consumer benefits such as time savings and reduced need to report sensitive information repeatedly across different sectors such as banking, telecommunications and energy.

6. Conclusion

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. NAB realises and supports the potential for a burgeoning digital economy to be established under the CDR. However, NAB encourages a careful approach to implementation of an expanded CDR, particularly to write access, to ensure a strong, safe and scalable platform is built with a firm focus on customer protection. NAB supports the adoption of open standards over defined mechanisms where practicable, not only to foster innovation but to future proof the CDR. NAB believes that the existence of appropriate governance structures, accreditation processes and security capabilities are critical to ensure consumer confidence in the CDR system.

NAB looks forward to engaging further with the Inquiry over the coming months and being of any assistance to the process.