NATIONAL AUSTRALIA BANK SUBMISSION

Review into Open Banking in Australia

22 September 2017

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

TABLE OF CONTENTS

1. Introduction

National Australia Bank (NAB) welcomes the opportunity to provide a submission to the Open Banking Review. As a member of the Australian Bankers' Association (ABA), NAB has also contributed to and is supportive of its submission.

NAB notes the Government's intention to introduce an open banking regime with the objective to 'provide consumers with greater choice and also support competition'.[1] Similarly, this review's purpose states that 'data sharing will increase price transparency and enable comparison services to accurately assess how much a product would cost a consumer based on their behaviour and recommend the most appropriate products for them'.[2]

NAB welcomes competition that enhances customer outcomes and this submission has been compiled with this objective in mind; particularly granting customers' easier access to banking products and customer data.

NAB's submission also builds on previous comments in relation to open data, including NAB's December 2016 submission to the Productivity Commission (PC) draft report from the *Data Availability & Use* inquiry. NAB is also a member of Data Governance Australia (DGA) and has representation on the DGA Board.

The structure of NAB's response has been guided by the questions posed in the Issues Paper.

[1] See 2017 Federal Budget, Budget Paper 2, p161.
[2] See Inquiry Terms of Reference, Purpose of the review, available at https://treasury.gov.au/review/review-into-open-banking-in-australia/terms-of-reference/

2. Executive Summary

NAB believes a successful open banking regime needs a strong emphasis on customers' interests. When considering the topic of open banking, NAB has adopted a focus on customers; from what types of data will benefit them to the appropriate regulatory framework needed to provide necessary protection from risks that will exist in an open banking regime.

NAB recognises the significant opportunities from data sharing, for both established players and new entrants. For established entities like NAB, key opportunities include:

- The ability to tailor and improve products and services based on a greater pool of data;
- Simplifying Know Your Customer (KYC) processes; and
- Streamlining customer on-boarding processes.

These opportunities are to the benefit of customers and can help support competition in the sector.

Regardless of the approach adopted, the security and safety of customer data is paramount, so the appropriate protocols and security regimes must be adopted. It is also prudent to ensure the incentive to innovate in this area is retained and the cost of introducing such a regime is shared by all parties who participate in the regime.

To best support the Government's objective, NAB believes:

- An open banking regime in Australia should apply to customer collected data and general product data for transaction and deposit accounts.
- A technology neutral approach should be adopted to provide this data, with the banking industry agreeing the most appropriate data format and transfer mechanism.
- A governance framework for open banking in Australia should include an industry working group to agree on implementation, an accreditation entity to authorise third parties to receive the data and regulatory oversight to the regime provided primarily by the ACCC.
- The liability for fraud or data misuse after the transfer of data to a third party at the request of a customer should be the responsibility of that entity.

NAB urges against the adoption of an overly prescriptive, mandatory open banking regime in Australia. An overly prescriptive regime could mean it does not deliver the best customer experience and would curb some of the innovation already occurring in open banking.

3. NAB and data

3.1 NAB's current data sharing activity

NAB currently provides customers with a range of data. Some of these are made available due to regulatory requirements, while others are voluntarily shared to assist customers in understanding their financial positions.

The data below is currently available through Internet Banking:

Category	Type	Form	Purpose of Sharing
Customer Collected Data	Account statements (for loans, cards, savings and transaction accounts). Includes name and address details and account information	PDF	Regulatory requirement.
	Interest statements	CSV	To assist customers with financial management (e.g. preparation of a tax return)
	Transaction data for all card, loan, deposit and transaction accounts.	CSV or specialised formats for various accounting tools such as Quicken, MYOB and Xero.	To assist customers with financial management

3.2 NAB's innovation

NAB and other major banks are proactively pursuing the improved sharing of data through the use of Application Programming Interfaces (APIs). As outlined to the PC, APIs were first implemented as part of the NAB technology infrastructure in 2013. Since then, they have been an important part of NAB's digital infrastructure. NAB's digital assets are currently in the process of being API enabled, for example NAB's update to mobile banking applications on Android and IOS in October and November 2016 respectively was underpinned by APIs.[3] This enablement will provide greater flexibility for sharing data.

Over the past three years, in addition to this internal development, NAB has been progressing data sharing partnerships with key organisations to offer innovative customer solutions. For example, NAB has enabled small business customers to more readily transfer transaction data sets to cloud accounting packages, such as Xero and MYOB. This provides customers with better visibility of their financial position. In doing so, NAB is responding to changing customer expectations as to how they wish to use data and is exploring new data sharing use cases with selected partners.

In addition, NAB launched an API Developer Portal in December 2016.[4] NAB is the first Australian bank to launch a Developer Portal, which offers data relating to NAB's branch

[3] See NAB December 2016 submission in response to Productivity Commission draft report: Data Availability & Use, p4.
[4] This portal is available at https://developer.nab.com.au/

and ATM locations and NAB's foreign exchange rates. In the nine months since launch, the Portal has had over 600 individual developer registrations. NAB has also provided keys for production access to six organisations after appropriate certifications and reviews were conducted.

3.3 NAB Ventures

NAB Ventures was established in January 2016 as the venture capital arm of NAB. Through NAB Ventures, NAB holds minority investments in several FinTech companies that help NAB accelerate innovation and deliver better customer products. Relevantly, it has made investments in Data Republic, which is a data sharing platform that enables secure data exchange and governance capabilities. Data Republic allows companies and government entities to securely share their data sets to create innovation across industry sectors in a scalable way.

4. Application of overseas data sharing frameworks

NAB believes it is particularly instructive to note the levels of innovation and development in open banking across different jurisdictions and regulatory regimes.

Some of the most innovative and progressive developments in open banking are occurring in the United States (US). There, Citigroup has launched a global API Developer hub that contains APIs across eight categories including account management and money movement. Separately, Capital One has launched a developer portal named DevExchange, which currently has four open APIs that aim to improve processes such as on-boarding and authentication.[5]

As noted in the Issues Paper[6] this innovation in the US has been driven by market forces rather than government regulation or frameworks.

In contrast, the banking sectors of the United Kingdom (UK) and Europe are more focussed on preparing for the adoption of, and compliance with, upcoming mandated requirements. Most of the nine major banks in the UK have opened APIs only for publicly available information, as required by the Competition and Markets Authority (CMA). NAB understands that these UK banks have fewer resources available to develop innovative data solutions and products for their customers as they seek to comply with these frameworks.

While the European directive, Payment Services Directive 2 (PSD2), is often quoted as a framework for open banking, NAB notes its objective is to create a more integrated and efficient payments market. Likewise, the objective of Europe's General Data Protection Regulation (GDPR) differs to the Australian Government's open banking objective, in that it is focussed on strengthening individuals' rights to personal data and applies to all industries, not just banking.

NAB believes the most informative international framework for the Australian Government's objective of enhancing customer choice and competition is the UK's Open Banking Standards (OBS), which seeks to improve competition and efficiency, and stimulate innovation'.[7]

There are elements of this framework that NAB believes could form appropriate principles for establishing an operating model in Australia:

UK Element	Commentary
Limiting framework to defined data sets: • Reference data, such as branch and ATM location, opening hours. • Product information on personal and business customer transaction accounts and small and medium enterprise (SME) lending. • Transactional data of these accounts	NAB agrees with the approach to define the data in scope and appropriate data sharing rules to reflect the permitted use cases. NAB believes that product information on SME lending should not be included in the scope of data able to be transferred under an open banking regime.

[5] See Citigroup Media Release, available at http://www.citigroup.com/citi/news/2016/161110b.htm
[6] Review into Open Banking in Australia, Issues Paper, August 2017, p3.
[7] The Open Banking Standard, p8.

(excluding data on mortgages and credit cards). • Service quality indicators, i.e. customer recommendation scores. • Use limits (six specified are: current account comparison services, personal financial management, access to credit, affordability checks, online accounting and fraud detection).	
Establishing an 'Implementation Entity', comprising a range stakeholders including representation from industry, regulators, and consumer and business customer representatives to plan, design and deliver future phases of the OBS with input from industry through consultation.	NAB supports an industry working group along the lines of the UK model to agree data sharing standards, technology formats and accreditation requirements.
Regulatory oversight via the CMA.	NAB agrees with the need for regulatory oversight, with the ACCC best placed to be responsible.

However, other elements of the UK framework are less applicable to Australia – particularly given the UK experiences of implementation:

UK element	**Commentary**
Applies to the nine largest retail banks.	NAB believes a framework should apply to all Authorised Deposit-taking Institutions (ADIs) from inception so there is a level playing field across ADIs and customers get a consistent experience regardless of which financial institution they bank with.
Open APIs as the format for data sharing.	NAB believes that a framework should not prescribe technology standards, which has the potential to limit innovation; rather, the most appropriate technology standard should be determined by the industry.
Banks to fund the implementation entity.	NAB believes a 'user-pays' system should be established requiring third parties to pay a fee to obtain accreditation to receive data and ensuring ongoing compliance with standards.

5. What data should be shared and between whom?

5.1. Scope and purpose of data sharing

NAB acknowledges the current manner in which customer data is provided could be done more easily. Informed by our experience, NAB believes that publically available data, via a format such as an API for product and branch data, is the logical first type of data for banking entities to share. As outlined in 3.2 above, NAB is already sharing some of this data via an API available from NAB's Developer Portal. Specifically, this type of data could include:

- Product reference data for transaction and deposit accounts (e.g. product features, terms and rates)
- Service data (including branch and ATM location, opening times, services)

This data could be shared as the first phase of a broader open banking regime. It would help gauge what data is of most interest to customers (based on what data they access and overall demand), and allow the processes for sharing additional data to be refined.

NAB agrees with the Issues Paper that there are a wide range of data definitions in the banking sector. Two key types are:

1. **Customer-collected data**: Based on information provided by customers to the bank, such name, address, date of birth, contact details, or details of customers' banking activity, such as account information, account statements or transaction history.
2. **Customer derived data:** Information developed by banks based on information provided by customers such as analytics and derived insights or information obtained by NAB from a third party under a commercial arrangement such as credit scores and property valuations.

NAB believes that any mandated data sharing requirement under an open banking regime should only apply to 'customer collected' information for the purpose of meeting the Government's objectives of increasing choice and promoting competition.

In all cases, appropriate restrictions on third party access should be in place. These could include:

- That use of data is limited to the approved use case (NAB believes the six use cases specified in the UK – current account comparison services, personal financial management, access to credit, affordability check, online accounting and fraud detection – are appropriate).
- Duration of data (e.g. historic transaction data) is limited to what is necessary to achieve the intended purpose.
- That data is not to be on-sold by the third party (with or without customer consent).

NAB believes that customer collected data under an open banking regime should apply only to personal and small business transaction and deposit accounts. Data related to small business lending, should not be captured. NAB notes significant innovation is currently occurring in small business lending, demonstrated by NAB's QuickBiz loan offering. Launched in May 2016, QuickBiz is a fully digital business lending application offering up $50,000 of unsecured financing for small businesses. It links to data feeds directly from a customers' cloud accounting package, such as Xero or MYOB, to inform

NAB's credit decision process.[8] If SME data was to be included in a subsequent phase, it should be part of a broader requirement applying to providers of SME credit beyond ADIs.

NAB believes customer derived data should not be mandated as part of an open banking regime. This includes externally obtained augmented data, such as credit scores received from credit bureaus and property valuations. This information is provided to NAB under a commercial arrangement from the bureau and customers are able to request their credit score information directly from one of the bureaux.

Similarly NAB believes derived data, such as customer segmentation or behavioural indexes, customer credit worthiness or internally derived risk ratings, should not be shared under an open banking regime. NAB considers this information to be both proprietary and unique to NAB and underpins NAB's credit decisioning processes and commercial practices.

NAB's View

- Product reference data for transaction and deposit accounts and service data could be shared as the first phase of a broader open banking regime.
- Mandated data sharing under an open banking regime should only apply to customer-collected data relating to personal and small business transaction and deposit accounts.
- Customer derived data should not be mandated for sharing as it is either obtained from a third party or proprietary to NAB.

5.2 Principles on who should receive the data

NAB believes requirements should be established on the types and sizes of third parties which are able to receive data under the regime. While NAB believes the exact requirements for third parties should be agreed by the industry and administered by the accreditation entity, principles of these requirements should be:

- Third party recipients should only be provided data for the express purposes of providing competition in the financial services sector, such as price and product comparison. Again, NAB believes the five other categories of use cases specified in the UK – personal financial management, access to credit, affordability check, online accounting and fraud detection – are appropriate for adoption in Australia;
- Consideration should be given to whether all companies, regardless of their size, should be permitted to receive data from ADIs. NAB believes there could be unintended consequences if data sharing requirements are the same for all third party data recipients. Priority should be given to providing data to smaller, Australian operated firms which offer competition in the local market. A way of doing this could be to impose an upper limit on the size of firms which can be accredited as a third party recipient, so that large global technology organisations are not captured under an open banking regime.
- If large global technology organisations were permitted as third parties to receive data from banks at the request of customers, customers should be able to request data held about them by these organisations is transferred to ADIs under the

[8] For the latest product offerings via QuickBiz, see 'New unsecured $50,000 financing to help Australian small businesses grow faster', 31 July 2017, http://news.nab.com.au/new-unsecured-50000-financing-to-help-australian-small-businesses-grow-faster/.

principle of reciprocity. For example, access to customers' transaction search data could allow ADIs to offer customers more targeted digital products and services which better meet their needs.

6. How should data be shared?

Based on the experience of overseas jurisdictions and the UK in particular, NAB believes there are a number of issues to be worked through in order to balance the Government's objectives with appropriate consumer protection. NAB's preliminary view of these issues is set out below.

6.1 Technology solution

NAB believes a technology neutral or agnostic approach should be adopted for open banking in Australia, with no specific technology prescribed. Legislating prescriptive technical solutions could become out-dated as technology changes. NAB supports the banking industry agreeing to the data format and common standards on how data can be transferred.

Based on current technology available, NAB believes that APIs would likely be the best technology to transfer data to customers and third parties in a standardised format. NAB does not though support API technology, or any other form of technology, being mandated as the mechanism for sharing data.

NAB also believes that different customer types will have different needs and uses for their data, allowing banks to vary the way this could be made available.[9] A mandated data format may limit NAB's ability to provide data in bespoke forms to best meet the needs of those customers.

NAB's View

- A technology neutral approach should be adopted in Australia. Currently, APIs would likely be the best technology but this, or any other form of technology, should not be prescribed.

6.2 Data security

The security of customers' data is paramount. Breaches of customer data in the sharing process under an open banking regime could significantly impact on the trust and confidence that customers have when dealing with NAB, regardless of when the breach occurs.

Obtaining the consent of customers to transfer data to third parties is critical. No data could be transferred without that consent. Providing consent though does not alleviate all security concerns. It will also be important that in gaining such consent, further education is provided to remind customers of the risk they are accepting, and to ensure they are confident in the third party recipient managing their data. Consent should also be limited to a specified period of time, and not be in perpetuity.

[9] See NAB December 2016 submission in response to Productivity Commission draft report: Data Availability & Use, p5.

A way to ensure the veracity of consent is to require customers to provide it directly to a bank. Customers could do so when accessing their account via internet banking. Logging onto an internet banking account means that customers will already be operating in an authenticated environment before they consent to transferring data to third parties. Within their account, a list of third parties who have been authorised by the accreditation entity would be available for customers to select. Providing consent directly to a bank would utilise the existing security and protection afforded to customers.

ADIs could also negotiate specific agreements with third parties, allowing customers to provide their consent on that third party's platform. These third parties would be verified through the existing processes banks adopt when entering partnerships with third parties.

NAB believes that in addition to customer consent and a proposed system of third party accreditation, the security of data transferred under an open banking regime could be ensured by encryption in the transfer process. It could also be supported by requiring the auditing and logging of data requests by individuals or transfer requests for third parties. This would allow for traceability and auditability in the event of a breach. In the instance where multiple parties are involved and a data breach occurs, identifying the exact party where the breach occurred can be challenging.

6.3 Customer privacy

Customer data, as well as the information created as part of bank records, is confidential; it needs to be handled appropriately. Ensuring that this confidentiality is secured is critical for banks in maintaining the trust of customers. Banks must constantly assess how customer data is treated, who is permitted to gain access to systems or records, and how compliance and risk appetite is maintained; however, in doing so, they must also remain flexible enough to engage in new technologies and encourage innovation in products and services.

Accordingly, NAB believes that in creating an open banking regime, the privacy of the information must be maintained so that customers are not put at risk. NAB believes an open banking regime will need to consider:

- Its interaction with existing legal rights of customers to access their personal and credit eligibility information.
- The handling of joint accounts. This is particularly important along with what occurs when these accounts are separated (e.g. after a relationship breakdown).
- Ensuring any disclosures to third parties are made on instructions of verified customers.
- Assurances that third parties will be subject to equivalent privacy obligations (noting that the Privacy Act has a small business exemption).
- How the regime will interact with the trans-border data provisions of the Privacy Act.

These issues could first be discussed at the proposed industry working group, outlined in the next section.

7. Governance of third party access to data

NAB believes that third party access under an open banking regime should be aligned with an economy-wide data sharing regulatory framework. The PC recommended the creation of a 'Comprehensive Right' to access and use digital data. If implemented, this would allow consumers to request their data be transferred in a machine-readable form to an individual or a nominated third party. As noted in the Issues Paper, the Government is currently developing its response to the PC report, including the recommendation to establish a comprehensive right.

In NAB's preliminary view, a governance framework for open banking in Australia comprises:

- An industry working group, responsible for determining standards and rules for data sharing, technology formats and security requirements.
- An accreditation entity, responsible for overseeing the accreditation process, monitoring compliance, and conducting audits.
- A regulatory body responsible for enforcing the data sharing regime, investigating breaches, and overseeing the Comprehensive Right as part of the economy-wide data sharing framework.

7.1 Industry working group

NAB believes that an industry working group is best placed to agree on implementation matters such as standards for data sharing technology and formats, and minimum security requirements. These standards would form the basis of accreditation for third parties to access the regime.

The industry working group would include three components, broadly in line with the UK model:

- **A steering group** as the decision making body, with representatives from each of the major and regional banks, two customer representatives (one consumer, and one small business) and six regulatory observers (the ACCC, Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, the Office of the Australian Information Commissioner, the Department of Treasury and the Reserve Bank of Australia).
- **Specialist working groups** who support and report into the steering group. These groups would look at areas such as customer outcomes; data (scope, formats, standards, duration and use cases); security; legal considerations and liability.
- **Advisory groups** for all interested parties, such as FinTechs and data aggregators, to contribute to the standards being developed. These would report to the steering group.

A more detailed proposal on the structure of the industry working group is available in the ABA's submission to this review.

NAB's View

- Establish an industry working group, responsible for determining standards and rules for areas such as data sharing, formats and security requirements.

7.2 Accreditation entity

NAB believes any requirements for transferring data to third parties needs to be supported by a system of accreditation or authorisation for the third parties, undertaken by a new body. This would ensure that third parties have been verified as having the appropriate security measures and capability to protect the data that is being supplied them. Without such a system, NAB would be unaware of a third party's data management standards and practices. Only third parties who can demonstrate robust data security processes should be allowed to receive or access data.

An accreditation entity offers a productivity benefit of third parties only having to receive a single accreditation, rather than needing re-certification from each bank.

An accreditation or authorisation system for third parties should occur at inception, and then on an ongoing basis. Third parties should be required to participate in periodic certification process to maintain their accreditation. This would ensure security safeguards are maintained and necessary upgrades to protect against new security threats are made. Various levels of accreditation could be created depending on what type of data a third party is seeking to receive and how the third party intends to use the data.

An independent entity is one structural option to perform this accreditation or authorisation process. Another option is to create an entity which operates at arm's length, owned by the banks, to utilise the collective knowledge and expertise of security experts working in the banking sector.

Regardless of the structure, once established, consideration could be given to the entity in time being utilised by other industries as part of the economy-wide data sharing framework (proposed under the Comprehensive Right), after receiving the appropriate regulatory approval. This would allow the considerable security expertise of the banking sector to be utilised by other sectors and streamline the accreditation process for third parties accessing data from various industries.

The entity should be funded via a user-pays system, with third parties applying for such accreditation required to pay a fee to obtain the appropriate accreditation.

NAB believes a new entity is most appropriate given the technical, and specialised, nature of the work it would be required to conduct.

NAB's View

- An accreditation entity established to verify third parties as being appropriate to receive data from customers with their consent.
- Accreditation granted only for a defined period of time with third parties required to renew their certification periodically.

7.3 Regulatory oversight

The appropriate regulatory framework and oversight of an open banking regime in Australia is of vital importance to customers and industry participants. NAB believes the ACCC is best placed to administer, enforce and have primary regulatory oversight of the regime. This would have several benefits:

- Ensures an open banking regime is aligned with an economy-wide data sharing regulatory framework, in line with the PC's recommendation that the ACCC be responsible for the oversight of the economy-wide Comprehensive Right.
- Assists the scheme in achieving the Government's stated objectives of increasing customer choice and supporting competition given the ACCC's remit.
- Aligns with the regulatory oversight adopted in the UK by the CMA, allowing Australia to learn directly from the UK regulatory experience.

NAB acknowledges that some further regulatory oversight may be needed by other regulators on areas of the open banking regime the ACCC may not be best placed to oversee, such as an external dispute resolution function to resolve individual customer disputes arising from data sharing.

NAB's View

- The ACCC is best placed to administer and have primary regulatory oversight of the open banking regime

7.4 Other governance issues to be considered

- **Ability to restrict for demonstrated poor practice:** NAB recommends that banks be able to restrict access to third parties accessing data if that third party has suffered a data breach within a recent period of time.
- **Clear standards for data integrity and quality management:** The sharing of data requires both sharing the actual data and also the characteristics or quality and integrity level of the data provided. How this is delivered needs to be consistent so data can be appropriately understood. NAB recommends that key standards are agreed to as part of an open banking regime.
- **Clear framework for the data exchanged:** A key consideration in the provision of data to third parties is the liability of any data about the customer that they have not handled directly. If the customer is not involved in the exchange, it needs to be clear that the provision is on the specific instruction of the customer who attests that the information is accurate and current.

7.5. Liability framework

An effective liability framework is also critical to the success of an open banking regime. NAB supports a core principle that the customer should not be at loss in the event of a data breach.

At present, the bank is ultimately liable for reimbursing a customer in the event of loss for which they are not responsible; however, once a customer's data is transferred to a third party, at the request of that customer, the bank is no longer in control of that data.

NAB believes that liability for fraud or data misuse caused after the transfer of data to a third party should fall with that third party. Where a third party is responsible for a data breach, that party would assume liability for the breach and reimbursing customers for any loses. NAB believes the adoption of an accreditation entity to authorise third party

data recipients should help reduce the risk of data breaches by ensuring robust and ongoing vetting of data recipients. Even with such an entity, NAB acknowledges the possibility remains that some third party data recipients may not have sufficient means to reimburse customers (particularly if the data breach is significant).

An option to address this possibility and to prevent customers being out of pocket is an insurance requirement for third party data recipients as part of the accreditation process.

NAB does not believe that the banking industry should be ultimately responsible for bearing the cost of a data breach by a third party; this cost should be met by the third party. In this way, liability is a critical issue to be resolved prior to implementing an open banking regime.

If the banking industry was required to be liable for data breaches by third parties, then the security and data standards would need to be even more significant than they would otherwise have been. For example, individual banks would likely seek to retain control of the accreditation process and individually approve each third party seeking to receive data. This could limit the number of third party entities able to receive the data, in turn reducing the competition benefits of the open banking regime. A change such as this would be needed to accommodate the additional liability risk which banks would incur. While difficult to quantify without details of the open banking regime being confirmed, this liability risk could be significant and even unlimited, without a cap being adopted on the amount banks were liable for.

NAB's View

- Liability for fraud or data misuse caused after the transfer of data to a third party should fall with that entity.
- An insurance requirement would prevent third parties having insufficient means to reimburse customers following a data breach.

7.6 Commercial model

If specific data sets are mandated to be shared under an open banking regime, NAB believes data providers should be able to charge a fee to access this data, as part of a cost recovery model. It is not commercially sustainable or equitable in the long term for the entire cost of implementing an open banking regime to be borne by the incumbent banking sector.

This cost could be agreed by the industry, with appropriate regulatory approval, to ensure it was standard across the sector and that customers were not charged different amounts to receive the same type of information from different financial institutions.

8. Implementation timelines, roadmap and costs

Having regard to the experience in the UK, and the features of the Australian market, NAB believes that the key driver of an implementation timeline is the need to define an operating model that balances the objectives of open banking in Australia with appropriate consumer protections, including regulatory oversight, the establishment of an accreditation entity and an effective liability framework. This framework is critical for the sharing of customer data; however is less necessary for sharing general product data. As such, NAB agrees with the ABA position that the industry would be in a position to share general product data for transaction and deposit accounts in 12 months, once the appropriate product information is standardised and a data format is agreed by the industry working group.

The establishment of a sustainable operating model for the sharing of customer data is likely to require material time and effort to develop. NAB also agrees with ABA's commitment of in principle support for sharing elements of customer transaction data within two years once the underpinning regulatory framework issues are confirmed.

NAB strongly supports a phased implementation for the creation of an open banking regime in Australia, regardless of the exact model adopted. Such an approach would allow Australia to:

1. **Gauge the level of customer interest:** Phasing implementation allows industry participants to assess the level of interest from customers and third parties, and demand for the provision of data. Operationally, having an indication of the demand for initial data types could help inform the approach and technology requirements for sharing data.
2. **Learn from overseas experience:** NAB agrees with the issues paper that a phased implementation will enable Australia to learn valuable lessons from the implementation and initial operation of open banking in other jurisdictions.[10]
3. **Costs:** A longer time to implement will also assist in reducing implementation costs. As previously outlined to the PC, NAB believes the key costs will be in identifying, collating, verifying and aggregating the data, the development of technology systems and infrastructure to complete this work, and the ongoing costs of data reporting and system maintenance. It is difficult to estimate the specific costs without a proposed approach, data format and commencement date being identified.[11]
4. **Managing Risks:** A phased implementation would help to manage the risks associated with security, liability and privacy by progressing in a careful and considered manner. It also offers the ability to recalibrate the approach to minimise risks and guard against unintended consequences through the implementation period.

As a general comment, the more prescriptive an open banking regime is the longer implementation will likely take.

[10] Review into Open Banking in Australia, Issues Paper, August 2017, p5.
[11] See NAB December 2016 submission in response to Productivity Commission draft report: Data Availability & Use, p5.

9. Conclusion

The introduction of an open banking regime is a significant development in the Australian financial services sector. Implemented successfully, open banking has the ability to achieve the Government's policy objectives to support competition and benefit customers.

The experience of overseas jurisdictions is useful, but ultimately Australia should adopt an open banking regime that is bespoke for Australia's banking system and existing legal and regulatory framework.

NAB appreciates the engagement to date with the Open Banking Review and looks forward to further discussions in the coming months on this important topic.