

23 March 2018

The Treasury
Langton Crescent
PARKES ACT 2600

Via email: data@treasury.gov.au

Achieving a sustainable Open Banking framework

The Commonwealth Bank welcomes the opportunity to contribute to Treasury's consultation on the Review into Open Banking in Australia – Final Report (the "Farrell Report"). The Commonwealth Bank has reviewed and is broadly supportive of the Open Banking system outlined in the Farrell Report.

The Commonwealth Bank re-affirms its view that for Open Banking to deliver positive outcomes and increase benefits to consumers, regulations and the implementation approach must prioritise security standards and customer privacy rights. Accordingly, the Commonwealth Bank proposes following refinements to the findings in the Farrell Report to ensure that Open Banking is sustainable.

Recommendation 1 – Phased implementation. Implementation of Open Banking should be phased, starting with the product and account types most likely to bring benefit to the broadest range of customers. Implementation of data sharing capabilities should commence only once technical standards and Open Banking Rules have been designed and set.

Recommendation 2 – Secure authentication models. Participants should be free to adopt secure authentication technology that protects customer security and promotes safe online behaviour. In particular, a 'low friction decoupled model' should be the preferred method of access and authentication.

Recommendation 3 – Clear fundamental 'without charge' offering. There should be clarity regarding the types of transaction data that participants (including but not limited to banks) must provide without charge, and also the service levels under which that data should be made available. This will provide the economy with clarity regarding data assets that can continue to be shared under market-driven arrangements.

Recommendation 4 – Focus on consumer protection. Additional measures should be considered to protect vulnerable customer segments. This includes ensuring that there is verified, informed consent from all affected customers before their data is

shared, and also ensuring that there is a robust mechanism for capturing consent in the context of joint accounts and complex business structures.

Recommendation 5 – Robust, evolving accreditation standards. The accreditation framework should set appropriate standards for all Open Banking participants, and should not erode existing levels of data security and integrity. Those standards should reflect global best practice at the outset, and continue to evolve so that level of assurance is maintained.

Recommendation 6 – Reciprocity should benefit consumers. The Commonwealth Bank agrees with the Farrell Report that for a sustainable and competitive banking environment the principle of reciprocity should underpin Open Banking, meaning that all participants should be prepared to share equivalent data sets with each other. Importantly, the Commonwealth Bank believes that equivalent data sets should not mean data sets that are identical or close to identical, but rather customer data sets that relate to the core business for the non-bank participant.

This submission focusses specifically on each of these recommendations. The Commonwealth Bank is of the view that each of the above recommendations are necessary to ensure a sustainable Open Banking framework that can effect positive change for Australian consumers.

Recommendation 1 Phased Implementation

The Farrell Report appears to contemplate a very broad range of in-scope data sets. In particular, 27 banking products are proposed to be covered by Open Banking (see Recommendation 3.2 and Table 3.1 of the Farrell Report). The report proposes that for each product, all customer types holding that product should have a Consumer Data Right (CDR) for their data pertaining to that product.

Open Banking will result in substantial flows of data which, if uncontrolled, will expose consumers to security and privacy risk. The proposed breadth of the product list across all customer types needs to be phased to address this risk as well as practical implementation challenges for the sector.

The Commonwealth Bank suggests firstly that the product list be reviewed and those products no longer being generally offered by the market should be removed (for instance, pensioner deeming accounts).

For the remaining products, the Commonwealth Bank recommends a phased approach for applying Open Banking obligations sequenced by product types as well as customer segment.

Initial Phase – Establish Standards Infrastructure

Immediate ‘foundational’ work should commence to establish the Data Standards Body and setting appropriate Technical Standards. In the Commonwealth Bank’s view, infrastructure design and Standards-setting needs to be completed to enable a strong foundation for the reforms, before data on any product sets are available to access and share within the Open Banking system.

First Phase – Transaction Accounts

Within 12 months of Standards being finalised, deployment should commence with personal and small business transaction banking products, held by single account holders.¹ This initial product set will enable broad early reach for Open Banking. Over 96% of adult Australians hold a transaction account and so inclusion of this data set will enable immediate broad reach for Open Banking. Looking at the customers of the Commonwealth Bank, over 80% of transaction accounts are single account-holder. Product Reference Data for personal and small business transaction accounts should be available on the same timeframe.²

Within a further 6 months of sharing of the above data sets being enabled, implementation can then focus on joint account holders and small business entities with complex structures (e.g. multiple director corporations, partnerships and trusts) for products within First Phase. The internal operational infrastructure required to enable data sharing for these customer segments is substantial and complicated, compared to the data sets in the First Phase.³ It is critical that these capabilities are well designed to ensure consumers have the requisite level of control over their data.

Second Phase – Credit Card Products

Within a further 6 months of the First Phase completing, personal and small business credit card products for single as well as multi-party accounts can be safely brought in-scope. As at the end of 2017, there were 16.7 million credit card accounts held in Australia. Accordingly, combined with transaction accounts, this product set will deliver Open Banking to the majority of Australian banking customers. Product Reference Data for personal and small business credit card products would also be made available during this phase.

¹ The definition of “small business” from the Code of Banking Practice should be applied as it is well-accepted by industry, namely businesses which (i) have an annual turnover less than \$10m, (ii) have fewer than 100 full-time employees and (iii) has less than \$3m in total debt.

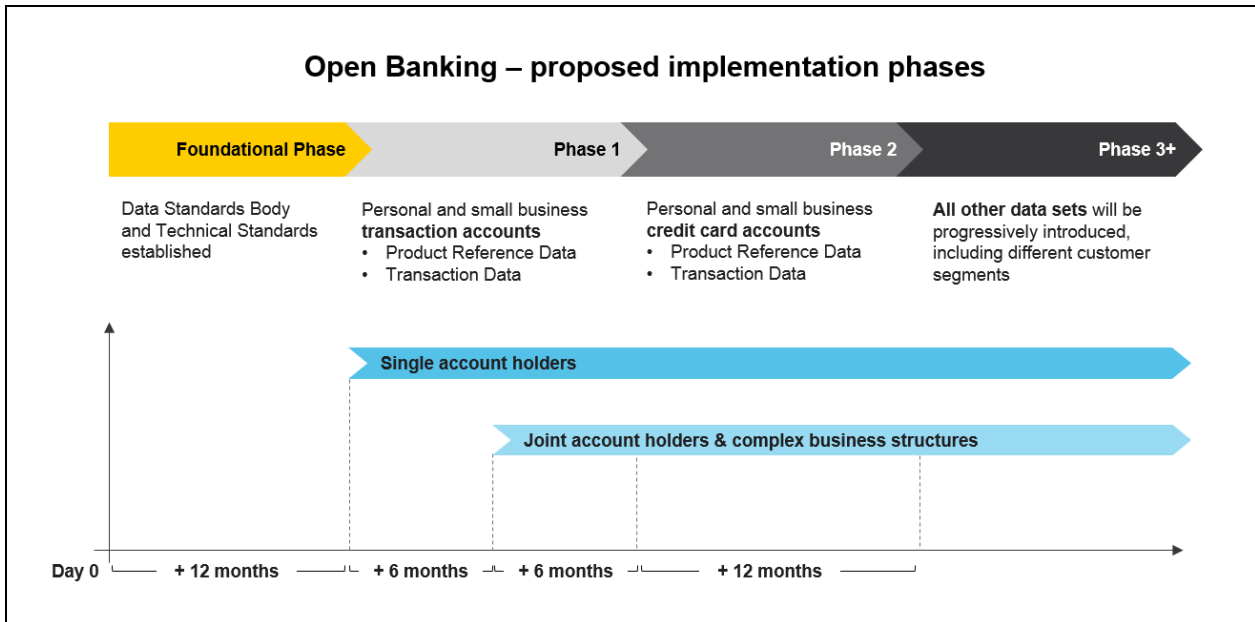
² Product reference information would typically comprise published product terms and conditions, product features, published rates and charges, and could also include service information such as ATM and branch information. This list is consistent with the UK’s approach to reference data.

³ The Commonwealth Bank has been in communications with administrators such as the Digital Transformation Agency and has confirmed that our view of the complexities associated with ‘entitlements’ and ‘authorities’ are shared across sectors.

Third Phase – Remaining Account Types

The Transaction Data and Product Reference Data for any remaining product sets outlined in the Farrell Report would be progressively delivered as a final phase of Open Banking. Deployment should occur as Standards are progressively agreed for a product set.

The Farrell Report proposes a liability regime that places accountability on data-holders for the quality of data that is shared under Open Banking, as well as the security of the data transfer mechanism. The implementation roadmap outlined above will allow data holders to ensure they are able to assess the suitability of this level of accountability.



**Recommendation 2
 Secure Authentication Models**

The Commonwealth Bank is of the firm view that consumers must not be encouraged to share data in a way that puts their finances or identity at risk. This happens if consumers disclose their log-in, security credentials and passwords to parties other than their bank. The most effective way of addressing this risk is through a strong authentication model applied to Open Banking; the Data Standards Body should allow industry to develop appropriate mechanisms within a certain framework.

The Commonwealth Bank strongly supports adoption of the “OAuth 2.0” protocol, as referenced by the Farrell Report, as a recognised technology standard, which allows for variety within its implementation whilst still observing a high level of security. The Commonwealth Bank is cognisant of the lessons from the UK industry who started a similar process with “OAuth

2.0” as a recognised baseline but also incorporated additional security protections throughout the standards design process.

Accordingly, the Commonwealth Bank sees merit in what the Farrell Report refers to as the ‘low friction decoupled model’ for consent, due to the higher security this entails. We have seen recommendations for this approach appear within international financial API standards. In particular, the Client Initiated Backchannel Authentication (CIBA) standard coming out of the OAuth Financial API (FAPI) working group which supports a “method of users granting access to their resources whereby the flow is started from a consumption device, but authorized on an authentication device”.⁴ This ‘decoupled’ model fully complies with the desired outcomes of an OAuth 2.0 implementation.

Importantly, the ‘low friction decoupled model’ will promote positive consumer behaviour. Consumers can be provided with a simple and consistent message that they should only use their banking credentials with their bank. This principle dramatically reduces the risk of phishing attacks.

Recommendation 3

Clear scope regarding ‘without charge’ transaction data

The Commonwealth Bank notes the Farrell Report’s recommendations that, as part of a Consumer Data Right, consumers should have fair access to fundamental data sets without charge. The scope of this right should be clearly defined by reference to the data fields contained within the concept of ‘Transaction Data’ and the service levels relating to how that data must then be made available without charge.

The scope of ‘Transaction Data’ should be defined by reference to the common unenhanced data fields that banks use in relation to their products, namely:

- account number, account name
- raw description or transaction type (ie is it credit/debit);
- amount of the transaction;
- date of the transaction;
- fees/charges incurred; and
- name of the product under which the transaction is made

The Open Banking framework should also be structured so that the data sets to be provided and the legal terms on which they are to be provided are very clearly specified to provide certainty to all participants. Further, it should be a key principle that the Transaction Data to be provided at no charge is made available on clear terms that are not unfair to data holders.

⁴ The proposal can be found here:

https://bitbucket.org/openid/fapi/src/a9e55356b5f233af804227d5001d3c32d23d1a91/Financial_API_WD_CIBA.md?at=master&fileviewer=file-view-default

Projections of potential traffic volumes indicate that, if usage is not regulated, the impact on systems may be un-supportable.

The Commonwealth Bank has had the opportunity to consider proposed submissions by the Business Council of Australia (BCA). We note the comments of the BCA regarding the potentially adverse economic impact of a model that removes the ability of a firm to charge for access to a valuable asset. We also note that the Productivity Commission acknowledged the need to navigate the legal principles around acquisition of property needing to be on terms that are not unfair. The Commonwealth Bank sees merit in these points, and recommends that Government work with the BCA and industry more broadly to consider those issues fully.

Finally, the Commonwealth Bank notes the Farrell Report's statements regarding sharing the result of KYC verification. Such reform will require AUSTRAC and the Attorney-General to develop a legislative model to allow a recipient to rely on another's identity verification. In the Commonwealth Bank's view, this is a complex area of legal reform that is highly correlated to digital identity, and should be excluded from the scope of Open Banking.

Recommendation 4

Protecting consumers and vulnerable segments

It is inevitable that the introduction of Open Banking will increase privacy risks, particularly carrying with it a potential to adversely impact vulnerable consumer segments. The current privacy concerns surrounding Facebook's use of customer data highlights the need for increased customer control.⁵ The Commonwealth Bank strongly supports the principle that Open Banking should require informed, explicit customer consent that can be easily revoked if the customer so chooses. The Commonwealth Bank agrees with the Farrell Report that informed consent entails:

- consumers having the ability to choose which accounts to share data from, the length of time for data to be shared and give consent to the data recipient, and the purposes for which the data can be used; and
- consumers being informed when their data is proposed to be shared (ie before sharing occurs and not after), and those consents should be re-established regularly.

Certain account types and customers segments carry increased complexity and also heightened risk. Youth accounts and products associated with customer data pertaining to minors should not be available for data-sharing until the appropriate protections are in place. The Commonwealth Bank has witnessed situations where the health and physical wellbeing of customers has been compromised as a result of their personal details being disclosed. Instances occur of domestic violence and physical violence occasioned as a result of contact

⁵ "Calls for action on Facebook data privacy" Australian Financial Review p4 22 March 2018.

details of joint account holders being shared where the individuals are in an estranged or acrimonious relationship. Accordingly, it is recommended that the data for young and vulnerable customers is only included within Open Banking in Phase 3 of implementation once the right protections have been established.

Given the sensitivity of consumer data in the banking system, the Commonwealth Bank supports the Farrell Report's suggestion that customer-provided data and transaction data under Open Banking should be explicitly recognised as personal information under the Privacy Act to ensure maximum privacy protections for consumers. The role of the OAIC should also be elevated to ensure there is appropriate oversight of privacy issues under Open Banking as well as co-ordination with ongoing privacy reforms.

Recommendation 5

Robust evolving accreditation standards

The Commonwealth Bank supports the statements in the Farrell Report that strong accreditation is essential to engendering customer trust in the system, data security and regulatory oversight. The Commonwealth Bank suggests that the accreditation framework reflects the following key principles.

1. Any participant obtaining accreditation must be able to demonstrate the ability to meet cyber security and privacy standards. For Open Banking those cyber security standards should be commensurate with or explicitly be pegged to APRA requirements, as this data is currently (and rightly) held under high security standards to which APRA-regulated data holders are subject.
2. Accreditation standards must be reviewed and re-set periodically to ensure relevance. For instance, emerging standards such as APRA's proposed CPS 234 focussing on cyber security, as well as the new OAuth standards around the safe authentication (see Recommendation 2) should be reflected.
3. Participants should commit to monitoring arrangements and reporting obligations to ensure consumers are protected.
4. Screen-scraping has been referred to by UK Open Banking as "a model that is both brittle and insecure". Accredited participants should commit to using Open Banking to access data securely and abandon insecure practices such as screen-scraping.

As a whole, the Commonwealth Bank is supportive of the Farrell Report's concept of risk-based accreditation. The accreditation framework should be based on a philosophy of setting minimum acceptable standards of participants that wish to be entrusted with consumer data, and not a low compliance alternative for accessing customer financial data.

Recommendation 6

Reciprocity should benefit all consumers

The Commonwealth Bank supports the Farrell Report's recommendation that the Open Banking framework should be underpinned by a principle of reciprocity. The Commonwealth Bank has consistently supported reciprocity on the basis that mutual data-sharing is beneficial for consumers and is vital to enabling a data-driven economy and to maintain the healthy levels of innovation in banking but also other sectors.

The Commonwealth Bank understands reciprocity to mean that any participant in the data sharing system that seeks access to a dataset must be in a position to share an 'equivalent' data set when instructed by consumers. The Commonwealth Bank supports the Farrell Report's view that an equivalent data set does not mean an identical or similar data set (which is implicit in the idea that Open Data will operate across different industries). In other words, if a banking data set is accessed by a non-bank Open Banking participant, that non-bank participant must be willing and able to grant access to non-bank data sets that relate to the core business of that entity.

Furthermore, in order to ensure that consumers receive maximum benefit from mutual cross-industry data sharing, the Commonwealth Bank believes that equivalent data sets should not be merely limited to data relating to the payment of monies. As an example, datasets relating to the consumer's acquisition and use of products and services could be purposed to drive consumer benefit and so should be considered equivalent data sets to Transaction Data under the Open Banking framework.

The Commonwealth Bank recommends that the complex considerations around cross industry data-sharing should be addressed early. In particular, clear guidance is required from regulators regarding the obligations of participants that 'ingest' data from other data holders. There are heightened consumer risks when data moves between participants that are subject to different regulatory regimes. The Commonwealth Bank is ready to work with regulators to start developing a cross industry data-sharing framework which should include clear guidelines around equivalent data fields.

Final Comments – Moving to Implementation

The Commonwealth Bank recognises the thorough consultation that Government has conducted in relation to Open Banking. We believe this indicates a clear recognition by Treasury of the substantial change that Open Banking will bring to the banking sector, and beyond. It is the obligation of Government, aided by industry, to ensure that the changes are positive.

The Commonwealth Bank is committed to enhancing and also protecting the financial wellbeing of the millions of Australians that are our customers. We are also deeply invested in ensuring that Open Banking effects positive change for those individuals and businesses.

The observations and recommendations outlined in this submission are strongly centred around what is best for consumers. The Commonwealth Bank asks that Government consider these suggestions and frame an Open Banking model that truly benefits Australians.

23 March 2018

Commonwealth Bank of Australia