



22 September 2017

Open Banking Review Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600
via email: OBR@treasury.gov.au

Dear Sir / Madam,

Review into Open Banking in Australia

Cuscal appreciates the opportunity to respond to Treasury's Issues Paper "*Review into Open Banking in Australia*".

Cuscal is an end-to-end payments provider that services more than 100 established and challenger brand clients with access to Australia's financial system and payments landscape, including the majority of the mutual banking sector. We are an ADI, a holder of an Australian Financial Services Licence and an Australian Credit Licence. We are presently rated A+ by Standard & Poor's.

Our services include payments processing, card scheme sponsorship, card issuing, card production services, merchant acquiring, ATM fleet management and digital and mobile banking platforms. We act as settlement agent for many of our clients through our ESA account with the RBA. We process approximately 12% of the electronic retail payments market.

We are at the forefront of payments innovation and investing heavily in technology development. For example, we are a founding shareholder and primary participant in the National Payments Platform and an industry leader in the implementation of digital wallets including Apple Pay and Android Pay, having enabled nearly 40 of our clients with this technology.

Cuscal also works closely with small and large Fintech companies seeking access to the Australian payments ecosystem and has enabled the connectivity of companies such as Square and Adyen. These companies are perfect examples of innovators in the merchant acquiring space that provide better customer outcomes through smart products and business models.

Cuscal is experienced in developing API's for our clients and is compliant with the Payment Card Industry's Data Security Standards (PCI-DSS). The secure handling and transmission of customer financial transactional data is core to our business and Open Banking is of high importance to Cuscal, our customers and the Fintech partners who we support.

Cuscal supports an industry environment which encourages sound competition and innovation, but which does not place unreasonable cost burdens on the industry. In this context, we have provided comments below based on the key issues Treasury has outlined for examination in the review.

What data sets should be shared and between whom?

The introduction of Open Banking should serve both the public benefit of increased competition as well as the private benefit of enabling access and control over an individual's banking data (alternatively labelled as "the Comprehensive Right" by the Productivity Commission). In serving those two outcomes, we believe that the data sets should be wide enough to include the type of data typically collected by a retail bank.

To this end, Cuscal strongly supports the two following recommendations of the 2016 Report of the Review into the 4 Major Banks ("The Coleman Report"):

- 5.22 *Generally the greater volume of data shared, the greater the potential benefits. However, for technical, legal, cost and regulatory reasons it is not appropriate to make all data sets accessible.*
- 5.23 *The committee believes that there is a strong case for increasing access to, what the banks themselves regard as, customers' data.¹⁶ This includes, for example, a customer's transaction history, account balances, credit card usage, and mortgage repayments.*

The banking data sets subject to Open Banking should include any data that is typically accessible by the customer through their internet or mobile channels. This would include:

"Retail Banking" product data:

- Transactional account data;
- Saving / Deposit Account data or statement data;
- Mortgage Statement data;
- Credit card transactions and statement data;
- Personal loan statement data;
- Current interest rate and fee information related to all of the above account types;
- Scheduled payments;
- Payee lists.

"Wealth" product data, including data related to:

- Insurance products held with the financial institution;
- Superannuation products held with the financial institution.

The inclusion of "wealth" products would provide the benefit of allowing the customer to see a more complete picture of their financial position. This would be of significant benefit in allowing the customer to make use of third party services that could provide general or personal advice based on a full view of the customer's circumstances. It is well reported that the large majority of Australians do not actively seek financial advice, due primarily to the cost involved. The access to cost effective financial advice is particularly relevant to the growing number of Australian's with self-managed superannuation.

Several Australian Fintech companies have already established workable business models based on the provision of automated ("Robo") wealth advice, although there is still significant effort required by a customer to take advantage of those services. Applying open data to all the above data sets would allow a third party to easily aggregate a customer's complete financial situation and provide more accurate advice with less effort required by the consumer.

This should enable cost effective access to financial advice by many more Australians. In addition, a broad banking data set will encourage third parties to develop comparative services highlighting to customers the availability of a more suitable or cheaper product or service based on their personal financial behavior. This will benefit both individuals and competition generally.

We acknowledge submissions made by various industry representatives in prior industry consultations concerning the distinction between "consumer owned" personal data and "institution owned" personal data. We agree that where a financial institution applies its own intellectual property in the form of an algorithm or model in order to come up with new information derived from customer data, that derived

information should be considered proprietary and excluded from the open data sets. An example of this would be a proprietary credit score. However a reasonably high bar should be set for derived data so that it does not include the type of data to which a customer would have a reasonable expectation of access.

2. Who should contribute data?

Cuscal recognizes the potential cost burden that an Open Banking regime will place on some parts of the industry. The cost will ultimately depend on the access mechanism, but there is likely to be a substantial fixed cost of implementation followed by continuing maintenance and compliance costs. Those costs will be felt most sharply by the smaller financial institutions who are also the least likely to be able to invest in the technology that would enable them to benefit by gaining access to Open Banking.

For that reason, Cuscal does not support the application of an Open Banking regime to all Australian Deposit Taking institutions. We would suggest that excluding ADI's below a certain number of customers (or balance sheet size) would be a sensible outcome which would still provide benefit to the vast majority of Australians and achieve the competition goals of Open Banking.

We also note that outside of deposit data sets, there are a number of industry participants that hold both credit and wealth data and which are not ADI's. To maximize the benefits discussed above, particularly in relation to financial advice, we believe that those entities, above a certain size, should also be required to provide accessible data. We would suggest a size should be set based on the number of customer accounts held and that the cut off size for inclusion should be based on covering 90% to 95% of the total number of relevant consumer accounts within Australia.

Some of these entities may currently be outside the scope of Treasury's review although we suggest that an industry wide implementation of the comprehensive right to data access would need to include them and they would need to subject to consistent standards that applied to the ADI's. Representatives from those non ADI's would therefore need to be stakeholders in the development of standards and governance for Open Banking.

3. Who should be able to access data?

Data access should be provided to all accredited data contributors as well as to accredited third parties. Those 3rd parties may be Fintech's or existing service providers who establish new services based on access to consumer data. There are two vital elements that need to be addressed in the access regime. These are the accreditation criteria of participants and the consent of consumers for these third parties to access their data.

Accreditation and entry into the Open Banking data ecosystem will need to be managed through the creation and application of agreed standards and the creation of a body to review and adjudicate on applications. We discuss this further under the heading "Regulatory and Governance Framework" below.

Access should only be granted to consumer data once consumer consent is provided to both the financial institution holding the customer data and the third party providing the service to the consumer. For reasons of liability and financial crime prevention, we do not think that financial institutions can rely solely on access consent provided to the third party.

We believe that ongoing customer control of data consent needs to be a key principle of the framework, and that this means more than a choice of authorizing access to "all" or "none". The consumer should be able dial up or down the amount of access that they are willing to provide to their data. For example some consumers might be quite happy to share their transactional data, but may not wish to share information about their mortgage or superannuation, while for other customers the inverse may be true.

In order for such choice to be exercised, the banking information will need to be categorized and the customer's financial institution will need to offer the selection to the customer. A simple categorization could be based either on product type (e.g. credit card, loan) or on a functional basis (e.g. transactional data, balance data, loan repayment history).

Further available choices of data use for which consent could be provided to a third party, could include:

- Use of data for personal benefit only;
- Aggregation of data;
- Use of data to help assess customer credit applications.

A third party should only be able to access that part of the information which is required to provide the service. Data should be used within a certain amount of time from the collection time and once used the data should be destroyed by the third party or, to the extent that record keeping regulation requires it to be kept, it should be de-identified and encrypted.

The instructions provided to the third party service provider would need to match the consents provided to the financial institution before the data could be accessed. It will be critical for the consent categorisation to be standardized across the industry so that consumers understand what they are consenting to and third parties can develop products appropriately.

Requiring consent to be provided directly to a Financial Institution will create a point of consumer friction as it will require two sets of instructions to be provided before a third party service can be initiated: one instruction to the third party and a separate visit to the customer's Financial Institution's digital channel to log in and provide the necessary consents. Unless this friction is managed well, the take up of third party services will be greatly reduced, for example if customers cannot easily locate a consent link. We therefore recommend that Financial Institutions be required to offer the consent choices in an easily accessible and highly visible format within their digital channels. Processes will also need to be developed to deal with dual consent for joint account holders.

We believe it will benefit consumers for data access to apply to both individuals and small business data. We recognize that there may be additional complications for business data (such as multiple authorized account holders) which may make small business implementation more complex.

4. How should data be shared?

Cuscal believes that principles should be created to cover the mechanisms for sharing data but that the sharing method itself should not be mandated.

While open APIs are generally cited as a preferred method for data sharing there are alternatives that may be cheaper and faster to implement and may provide a useful interim or staged solution.

For example it should be possible to create a framework based on a more secure method of "screen scraping" by overcoming the risk of providing log in details to a third party. In this scenario each financial institution could be required to issue a unique code to a customer, which can then be registered with the third party. Banking systems would need to be modified to allow read only access to customer accounts when the code is used rather than the full log in details. This method of access would enable third parties to offer a wide range of "read only" based services while providing security to consumers and overcoming the key objections that financial institutions currently have to screen scraping services.

If the above approach were applied on an interim basis and without the detail of data category consent that we have discussed earlier, minimum additional data standards should be required to be developed and implemented.

We consider that open APIs would be appropriate for more comprehensive "read and write" services and is likely to be the best current longer term solution, based on the technology which is available today.

Providing "read" access to customer data alone will not, in our view, generate the most beneficial uplift in competition and innovation. We believe those goals will be achieved through "write access" i.e. the ability to authorise 3rd parties to act as an agent of the customer to initiate payments and/or transfer funds. This would be consistent with the European regime which defines a Payment Initiation Service Provider (PISP) under PSD2.

We believe there is a need to set an availability and performance framework to ensure the APIs are implemented to meet the same service standards as the Banks own internet or mobile banking channels.

Whichever mechanism is selected for implementation now or in the future, data standards and security standards will need to be created and maintained.

5. Data Security and Privacy

We agree that the security of data is paramount and all participants will need to operate with at least the levels of security of the existing financial institutions which currently hold customer data.

Security standards and frameworks already exist which have been developed to ensure the maximum security over customer financial data, for example the PCI-DSS standards that apply to scheme credit and debit card-holder data. Given the amount of information and expertise available, we think it will be a large but not an extraordinary task to create appropriate standards for Open Banking. While the bar needs to be set high for Fintechs and other participants, the certification process for PCI-DSS has shown that high security standards are not an insurmountable barrier to entry. We discuss accreditation further below.

6. Regulatory and Governance Framework

We agree that the framework for Open Banking needs to be considered in light of an industry wide data sharing framework but we do not think that the introduction of Open Banking should be delayed to await the creation of that wider framework.

We believe that there are key roles for both government and industry in the creation of the framework, but that key elements cannot be left entirely to industry development, as the participants with the greatest industry influence are also those who are likely to be most reluctant to fully support Open Banking. We have seen how this influence has delayed the implementation of positive credit reporting, postponing the wide consumer and prudential benefits that could be provided through its full adoption.

We therefore believe that a model of partial self-regulation is most appropriate for Open Banking as outlined below.

7. Role of Government

In the interests of enhancing competition and expediting an Open Banking regime we believe that it is appropriate for Government or Agency regulation of the following elements of the framework:

- The mandating of data sets for inclusion;
- The setting of principles for access including access mechanisms;
- The approval of industry based standards, including accreditation of participants;
- The principles of participation / membership of industry bodies wishing to be part of the framework, including approval of constitutions and terms of reference. (Participation must be inclusive of key stakeholders and balanced to avoid undue influence of any particular category of stakeholder);
- An appeals mechanism for applicants excluded from participation.

We agree that the focus on competition would make the ACCC best placed to regulate and enforce the regime.

8. Role of Industry

We think that industry is best placed to develop the detail of mechanisms and standards that are appropriate for Open Banking, however in this context "industry" is a broad term. The "industry" that Open Banking encompasses includes, banks, mutual ADI's, lenders of various descriptions, payments service providers (including card schemes), as well as data service providers and Fintechs.

There is no one body that encompasses or speaks for all of these participants, rather the industry bodies represent either the nature of their members (such as the ABA, COBA and Fintech Australia, FSC or FINSIA) or a functional segment of banking (such as ARCA for credit and AusPayNet for the payments ecosystem.)

Some of these bodies have existing standard setting or accreditation frameworks that might be extended to cover the operation of Open Banking within their functional area, however the membership and governance of those bodies have not been established with a goal of increasing competition.

For that reason we envisage that a coordinated industry approach to partial self-regulation would require a new body with representation from existing industry bodies balanced with representation from Fintechs and other third party stakeholders and with a new charter, to be approved by the Regulator, with competition and consumer benefit as key principles. This body could then leverage the expertise that exists within the current industry bodies in a more balanced manner. The regulator should also be represented on this body in either an active role or as an observer.

We think that this new body, through appropriate functional sub-committees, should be responsible for the setting of data-sharing standards and an accreditation framework for participants. While we think the minimum data sets for inclusion in Open Banking should be mandated, there will inevitably be grey areas of data which could arguably fall within or outside the definition. We think there is a role for this body in recommending guidelines to the regulator on those grey areas and potentially adjudicating on disputed data.

We suggest there be some reporting mechanism between the body and the regulator to provide oversight of implementation, and the continued performance of Open Banking after implementation.

9. Other Data Sharing Considerations

This submission has focused on "Open Banking" as a customer directed concept as opposed to the broader concept of data sharing. Today, customer related data is already accessed or shared between financial institutions with varying levels of consent and knowledge. Key examples of that sharing are:

- Information contained in credit files held by credit bureaus (which is still predominantly "negative" information);
- Fraud and financial crime information shared through the National Fraud Exchange;
- Sharing of information with government agencies, law enforcement and regulators.

The ability to share that data serves important purposes which are wider than individual customer benefit. As such, the concepts of consumer choice and third party authorization cannot apply in the same way to that data. We therefore recommend that any regulation and communications on the implementation of Open Banking provides consumers with clear expectations as to the data which they may control and that the existing frameworks covering wider data sharing remain separate to the concept of "Open Banking".

10. Timelines and costs

Cuscal would support phased implementation, provided the phasing was designed to speed up the overall delivery of Open Banking, rather than to establish some quick wins at the expense of delaying the services that are most beneficial.

Phasing could be based either on data sets, the inclusion of financial institutions beyond ADI's, personal vs small business data, or based on the technical mechanism for data sharing (such as our suggestion on page 4).

Feasible timing for any implementation, whether staged or not, will depend on a range of items and particularly the mechanism of data access selected. Treasury should be mindful of the ability of Financial Institutions to commence a significant new implementation project of this nature in the short term where

for most institutions budget allocations for the 2018 financial year will have already been made and communicated to stakeholders and shareholders.

We trust this submission has assisted Treasury's considerations. If we can be of further assistance, please contact **Scott Jamieson**, Senior Manager of Compliance on sjamieson@cuscal.com.au or phone (02) 8299 9660.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Kieran McKenna', is written over a light grey rectangular background.

Kieran McKenna.
Chief Risk Officer.