Australian Finance Industry Association Limited
ABN 13 000 493 907
L11 130 Pitt Street Sydney NSW 2000
02 9231 5877 www.afia.asn.au

The Treasury
Langton Crescent
PARKES ACT 2600

23 March 2018

By email: data@treasury.gov.au

Dear Sir/Madam

Open Banking in Australia – Final Report

The Australian Finance Industry Association (AFIA) welcomes the opportunity to comment on the *Review into Open Banking in Australia – Final Report* (the Report).

AFIA is uniquely placed to advocate for the finance sector given our broad and diverse membership of over 100 financiers operating in the consumer and commercial markets through the range of distribution channels including digital access.

AFIA supports new technologies such as open banking because of the potential benefits for the customer. We note open banking aims to increase competition in banking and lead to new services being developed for customers. The Report recommends that open banking will be available for all bank customers whether consumer, small business or commercial. We also note that the Government is committed to rolling out a consumer data right that will eventually give all customers a right to direct their data to be shared with others they trust.

To assist the Government frame its response to the Report, AFIA makes comments in the following areas:

1. The Data Standards Body
2. Sharing of identity verification assessments
3. Types of data to be shared under open banking
4. The proposed reciprocal obligations.
5. Implementation timelines
6. Existing mechanisms for data sharing and consent models.
7. Liability mechanism
8. Accreditation
9. Renaming the Consumer Data Right as the Customer Data right to reflect that all types of entities will be able to access and share data about themselves under open banking.

We also raise issues for clarification, so that standards, rules and operationally crucial system builds can be developed efficiently and with confidence.

Data Standards Body

The Report recommends the establishment of a Data Standards Body to determine the necessary technical standards (including the transfer, data and security standards) for open banking. The Report recommends that this body should be made up of potential accredited-parties, customer representatives and data transfer experts.

AFIA agrees that the proposed Data Standards Body should include a broad representation of industry participants as wide and diverse representation will ensure the development of appropriate standards for open banking to work effectively and efficiently. This should include data-holders and potential data-recipients and accredited entities across financial services, as well as data servicing providers on whom many financial businesses rely to provide technological support.

AFIA recommends:

1. The proposed Data Standards Body includes broad and industry wide representation from data-holders, potential data-recipients and accredited-entities, as well as data-servicing providers on whom many financial businesses rely to provide technological support. AFIA would welcome the opportunity to participate.

Sharing of identity verification assessments
AFIA seeks further clarity on recommendation 3.4 (identity verification assessments).

In principle, we support ways for entities to meet their AML obligations efficiently. However, further work is needed before this recommendation could be considered. This should include determining the liability framework between entities for relying on a shared identity assessment and amending the AML/CTF laws to cater for an ability for one entity to compliantly rely on another entity's assessments. Without these two issues being resolved, it is likely sharing identification outcomes would result in a potentially unacceptable level of risk for both data-holders and data-recipients.

Further, industry and Government are undertaking work to establish a digital identity system, which may remove the need to share identity verification data in an Open Banking system.

Some Members also raised concerns regarding paragraph 3.12 (transfers of identity verification assessment outcomes) given that they incur significant costs in undertaking identity verification. They disagree with the Report's assumption that the cost of the activity is marginal (virtually zero) and that a verifying entity should be able to recover costs whether or not the risk to them increases as other parties rely on it. By being required to share outcomes, our members note that there will be an uneven playing field between entities that undertake identify verification and others that rely on that assessment and do not independently undertake their own.

Further, clarity is sought over who needs to store the original identify verification data when it is relied upon by another party. Potentially, an entity that undertook the original assessment will need to store these records indefinitely, causing challenges. Currently entities must hold verification records for seven years following the end of the relationship. However, if another entity relies on this verification, would this seven year period restart for the entity that undertook the original verification from the date that the other entity relied on the assessment?

AFIA recommends:

2. The Report should take into account the work already being undertaken by industry and the government regarding digital identity.
3. Further work should be undertaken regarding the allocation of costs and liability for identity verifications in open banking, including who will be required to store verification data that is being relied upon by a third party and for how long?

Types of data to be shared under open banking
The Report recommends that customer-provided data, transaction data, and identity verification assessments should be shared at the direction of a customer. Value-added customer data (or transformed/derived data) and aggregated data are outside the scope of open banking.

Often there is some overlap in these types of data or data could fall into multiple categories. As a result, policy development and implementation would benefit industry if clarity is provided on:

- At what point does transaction data becomes transformed data (e.g. if a data holder combines transaction data with another data set to provide additional information about an account for a customer).
- Whether the definition of transaction data extends beyond the products listed in Table 3.1 of the Report. For instance, will merchant acquiring accounts (that are neither deposit or lending products) be subject to open banking? Or be defined as equivalent data? In our view, the scope of transaction products subject to open data should be clearly defined.
- What data fields will make up transaction data? Some Members have the view that this should be defined and so that any enhancements to this data should not be subject to data sharing (but the underlying transaction data would still be shared). One Member has suggested transaction data could be defined as:
    - account number, account name
    - statement number and time period of statement
    - transaction type (ie is it credit/debit)
    - amount of the transaction
    - date of the transaction
    - status (i.e. did the transaction go through or not)
    - fees/charges

  - name of the product under which the transaction is made.
- Who is entitled to request data to be shared in relation to corporate credit cards issued to individual employees as an individual employee is issued with a credit card (that is in their name) but the credit account is held by a business entity?
- Some members recommend that certain types of sensitive information, including data that is commercial-in-confidence, proprietary, sensitive or legally privileged should also be excluded from the Open Banking regime (in addition to the exclusions already listed in the Report) as it would not be appropriate include these types of data in the scope of Open Banking.

AFIA recommends:

4. further clarification should be provided on what types of data will be subject to Open Banking.

Clarifying the Proposed Reciprocal Obligations

The Report recommends reciprocal obligations for those non-mandated entities that participate in Open Banking. Recommendation 3.9 reads:

> *Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.*

We understand the Report's underlying principle is that "*any non-ADI entity that participates in Open Banking as a recipient of data should also be obliged to provide equivalent data in response to a direction from a customer*".

The Report does not provide details on this obligation and, in particular, what constitutes '*equivalent data*'. For example, we do not think the concept of equivalent data works for a credit provider that wishes to access deposit or transaction account information where they do not offer transaction products (e.g. personal loans, credit cards or home mortgages). This becomes crucial to not only credit decisioning generally, but also in responsible lending compliance and hardship management.

Again, members have identified issues where policy development and implementation would benefit industry if clarity is provided on:

- How will the reciprocal obligations apply to different types of products and customers? Will non-mandated participants be able to apply the obligations flexibly so they can participate in Open Banking for certain types of products or customers?
- Will the reciprocal obligations start from the commencement of Open Banking for mandated ADIs or will there be a transition period for non-mandated entities to provide equivalent data? Some Members suggest that it may be necessary to have a transitional period of 12 months to apply from the first date the non-mandated entity received data under Open Banking.
- Some Members strongly support the reciprocal obligations and that eligible entities need to participate as both data-holders and data-recipients so that mandated entities are not the sole providers of data and voluntary participants merely receivers of data.
- How long will data recipients be required to hold onto data transferred to them and how will this interact with existing record keeping obligations? (e.g. the AML/CTF regime[1] requires records to be held for a period of seven years, with customer-initiated documents required to be held even longer, until 7 years after the customer relationship has concluded). Also, the impact of the Privacy Act requires personal information to held only for so long as it is relevant for the purpose for which it was collected, after which it must be either destroyed or de-identified.

On this last point we recommend that data recipients should not be required to store and share data provided to them under Open Banking. Under the new obligations, data transferred to a participant is required to be stored so a customer may direct the data recipient to share this data in the future. For some Members, such as credit providers, this will impose new costs that they previously were not required where there is no clear benefit for the customer. Certain types of data, like transaction records provided at a point in time, rapidly fall out of date and therefore usefulness and storage is of limited value to both data recipients and customers. Often, the data recipient only collects data for a

[1] See AUSTRAC site

single purpose at a point of time. After this time, the customer would need to go back to their first provider to get the most up to date version of their data.

AFIA recommends:

5. That the reciprocal obligations be clarified by addressing the above concerns. This should include further industry consultation on how the reciprocal obligations will operate. AFIA would welcome the opportunity to participate.

Implementation timelines

We note the competitive benefits of Open Banking for customers but AFIA's ADI Members have raised significant concerns around the proposed implementation periods for mandated participants. They note additional time is required to design and implement the necessary systems as the proposed scope of Open Banking is very broad and includes, current and former customers, retail, small and large business, and numerous products including transaction accounts (both deposit and credit products) with a requirement for customers to access the regime through non-digital means.

We further note many Members are already implementing a number of competing projects (including implementation of comprehensive credit reporting) and implementation of a number of new regulatory obligations and reforms.

Some Members have recommended that a phased implementation approach should be adopted based on the complexity of product types and customer types. To allow a seamless transition which achieves the Government's objectives in a way that balances the resourcing and cost for major bank participants, we recommend implementation of Phase One to occur 12 months after the finalisation of the rules and standards. Another Member suggested that for smaller ADIs an implementation period of two years would be more appropriate. This would not preclude early voluntary participation by entities choosing to do so.

Similar considerations will arise in the future of Open Banking when it extends to financiers who are not ADIs. Many of these financiers have either limited or no capacity in-house IT and IS development, so depend on third-party service providers for support. There is only a limited number of providers available. Consequently, resourcing will be an issue when the Government seeks to extend Open Banking to the non-ADI financiers. It is for these reasons that the Open Banking legislation should allow for implementation flexibility as its impact extends beyond its currently planned scope.

Existing mechanisms for data sharing, and consent models and privacy

We support the Report's approach that the final standards will be determined by the Data Standards Body, which will incorporate industry wide representation (as per Recommendation 1).

We note that there are already a number of tools used by some AFIA members to receive transaction data from a third party with a customer's consent. These tools mostly commonly use a method known as 'screen scraping'. Many credit providers use these tools to obtain transaction data to assess a customer's credit risk and to meet their responsible lending obligations (that includes verifying a customer's income and living expenses).

Members' views on existing data sharing methods and consent models are diverse. During our consultation with Members the following points were raised with us that we submit should be considered by the Government:

- Some Members agree with the Review's recommendation that screen scraping should be retained as a market check and contend that screen scraping utilising third parties that meets the equivalent data security standards of Open Banking should be encouraged to facilitate innovation and competition.
- Some are concerned about the potential consent models that could be adopted under Open Banking and recommend that the embedded model for consent should be adopted where a customer would give their consent to the transfer of data directly from the recipient's website (as outlined by the Berlin Group[2]).
- Some other Members support a decoupled model for consent rather than the proposed redirect model as it is more secure and drives consumer behaviour on password protection.

[2] Section 5.5.4, NextGenPSD2 XS2A Framework, Berlin Group

- Some Members suggest that the status of screen scraping is ambiguous and this should be resolved during this process. They recommend that screen scraping should be subject to the same proposed accreditation that is proposed to apply for Open Banking participants and that the proposed liability rules would apply to screen scraping in the same way it will apply for entities participating in Open Banking. This means that screen-scraping and Open Banking APIs would be treated in the same way.
- Some Members seek clarification regarding the single screen notification:
    - When is notification going to be required? Will this only be required for the first data transfer?
    - The Regulations should define what can be said in this notification and should not be worded in a way that may bias consumers against a data transfer.

Some Members have raised concerns about the modifications to the Australian Privacy Principles (APPs) particularly regarding the Report's view that express consent must be obtained before a data recipient sends a customer's data overseas (proposed modification to APP 8). This is not in line with APP 8. APP 8 requires consent only if the APP entity is not going to ensure the overseas recipient will not breach the APPs. If this were to become legislation it will limit the ability for offshore call centres to view this data unless a separate consent is obtained. The consent should be in line with APP 8 and provide the accredited party with two options as per the current Privacy Act.

AFIA recommends:

6. Different models of consent by industry should be permitted and accommodated as part of the Data Standards Body's work on determining the necessary standards for Open Banking.
7. The proposed modifications to the APP should be in line with APP 8 – that is give the accredited party with two options as per the current Privacy Act when sending a customer's data offshore.

Liability Mechanism

The Report recommends that a liability framework should be implemented. AFIA, in principle, supports that participants should be liable for their own conduct.

A Member has raised a concern regarding example 4 given in Table 4.2 of the Report. The example makes it clear that a data holder (where directed by the customer) is not responsible to a data recipient for the transfer of inaccurate, incomplete or misleading data to the data recipient. This Member suggests that without adequate safeguards in place data holders may not have the incentive to maintain the quality of their data (or potentially, in an extreme scenario, intentionally provide inaccurate, incomplete or misleading data). They recommend that there should be adequate safeguards in place to prevent this (e.g. potentially through the proposed rules).

We also do not fully agree with the allocation of liability in example 5 in Table 4.2 of the Report. This example makes a data-holder responsible for data being sent to a malicious actor during the transmission of the data between the data-holder and recipient. The data-holder should not be held liable where the malicious act arises from deficient security safeguards of the data recipient (e.g. the interception arose during the data transfer due to an act or omission by the data recipient).

AFIA recommends:

8. The liability mechanism and principles be further developed (including taking into account the above scenarios) before being adopted.

Accreditation

Members have raised the following queries regarding the accreditation recommendation (Recommendations 2.7 and 2.8):

- Will accreditation mean accredited parties are meeting necessary legislation requirements? For example, if an accredited party is sharing identification verification data will accreditation ensure compliance with AML/CTF obligations?
- Will there be ongoing review of accreditation and what form would it be in?
- Will accreditation be tied to existing licensing regimes?

Rename the Consumer Data Right as the Customer Data Right

We note that the Government has committed to legislate a Consumer Data Right[3] and that the Government has committed to a staged introduction across the economy starting with the banking sector. The Consumer Data Right as recommended by the Productivity Commission's Review into Data Availability and Use will allow consenting customers to access and share data about themselves with other parties.

The Review's Final Report recommends that, under Open Banking, the obligation to share data at a customer's direction should apply to all customers holding a relevant account in Australia (recommendation 3.7). This means the 'Consumer Data Right' will apply not just to 'consumers' but also small businesses, large businesses and other entities that hold relevant banking accounts in Australia.

To better reflect the Government's intention that consenting entities can use and share their data with others we recommend that the Government rename the 'Consumer Data Right' to the 'Customer Data Right'. We note that the Productivity Commission Inquiry into Data Availability and Use named their data sharing right the 'Comprehensive Data Right'.

AFIA recommends:

9. The Consumer Data Right should be renamed the Customer Data Right to better reflect the Government's policy and broad range of customer classes that it applies to.

If you have any questions regarding this submission please contact Alex Thrift, Economics & Policy Senior Adviser at alex@afia.asn.au or via 02 9231 5877.

Kind regards

Helen Gordon
Chief Executive Officer

[3] Government press release, 26 November 2017.