23 March 2018

Mr Daniel McAuliffe
Open Banking Review
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Dear Mr McAuliffe

Review into Open Banking in Australia – Final Report

AFMA welcomes the opportunity to comment on the Review into Open Banking in Australia's Final Report (the Final Report).

The Government's Open Banking project is the first stage the establishment of the Consumer Data Right and as a result the approach and structures it creates will have wide-reaching effects on many sectors of the economy for a long time to come.

The proposals address a clearly undesirable present state of affairs where consumers are using less than optimal mechanisms to transfer their data to third parties. AFMA supports the introduction of Open Banking as part of the Consumer Data Right as a way to ensure that the information customers already share with their bank can be safely shared with others they trust, and give customers more control over their information.

A number of AFMA members will be directly affected by the proposals as they stand. We also note the potential for the model proposed to be rolled out to other business areas over time and the subsequent need to ensure the model adopted by the Government is optimised.

AFMA recognises that the proposal put forward in the Final Report has high aims in the rapid deployment of new technology that will be rigorously enforced, but this must also be balanced against the Government's desired outcomes in terms of security, quality, cost, and support for innovation. This submissions sets out our views about how these aims can be achieved.

The Open Banking model as proposed will introduce risks that need to be carefully managed in the prudential framework of the financial system. These risks will increase if it proceeds in a second round to write access arrangements as per the EU direction. It is imperative that these risks are managed from a prudential regulatory perspective by a regulator that has a full understanding of the financial system as a whole and of the risks that can be introduced to the system by access regimes. System security and stability must be of the utmost priority and must not be compromised.

AFMA does have specific concerns with regard to the speed and breadth of the proposed roll-out and cautions against the proposed timetable and initial scope particularly in view of the security risks involved. We strongly recommend the 12 month implementation proposal be reconsidered, and a new timeline adopted that is based on a more limited scope and with appropriate regard for matters related to security.

We note that the UK Open Data regime on which the local framework is based has had low uptake by consumers and low availability on launch. It may be prudent to adopt a more incremental approach in Australia to maximise the chances of a successful outcome. AFMA also recommends that the UK standard not be used as a starting point for any Australian standard given its overly prescriptive nature.

AFMA also recommends that consideration be given, perhaps after an initial period, to moving to a standard industry creation and maintenance process more aligned with the international and domestic norms that have served industry and the community well in delivering a wide range of financial, IT and other standards over a long period.

If you have any queries in relation to this submission, please contact Damian Jeffree at djeffree@afma.com.au.

Yours sincerely

Tracey Lyons
Head of Policy

AFMA Submission

Open Banking in Australia
Final Report

March 2018

Contents

General Framework Response 5
Recommendations Responses 9

General Framework Response

AFMA supports the introduction of Open Banking as part of the Consumer Data Right as a way to ensure that the information customers already share with their bank can be safely shared with others they trust, and give customers more control over their information.

The proposals in the Open Banking Final Report address a clearly undesirable present state of affairs where consumers are using less than optimal mechanisms to transfer their data to third parties. "Screen scraping" in particular is an unsecure and brittle architecture that entails high risks for consumers.

There is general agreement in industry that this state of affairs should not continue indefinitely, for reasons of security and customer satisfaction. At the same time, connections to financial firms that allow access to sensitive data risk harm to consumers and the institutions if they are done incorrectly.

Widespread adoption of the technology, particularly by larger technology players, could result in significant amounts of sensitive financial data moving from the highly secure and tightly regulated onshore financial firms to offshore technology companies that may not share the same high security approach and regulatory framework of this jurisdiction. This risks increasing the chance of data leakage and malfeasance.

If the model is then later expanded, following the European regulatory-mandated lead, to incorporate so-called "write access" to online banking, this could risk exposing consumers and businesses to substantial risk of fraudulent activity with full access to instantly transfer money away. We support any such proposal being subject to a separate review and robust examination and note that this should be considered as a prudential matter.

On the basis of the risks involved it is imperative for these reforms not to be rushed. Against this backdrop the Government is looking at an accelerated timetable for roll-out over the next year, for many products in the banking stack and for all clients from individual consumers to large institutions. AFMA strongly recommends reconsideration of the proposed accelerated approach in order to mitigate the risks of adverse outcomes.

Standards generally take much longer than the suggested timetable to establish, particularly when they are as granular as has been proposed. Standards are almost always voluntarily adopted by industry, although there are precedents for incorporating references to standards in legislation and regulation, particularly on a principles basis. It is highly unusual to mandate a standard before or at the same time that it is being developed.

To accelerate matters, the Government is proposing not to use the regular international approach for standard setting adopted by leading typically non-profit bodies.

The 'standard' approach to the construction and maintenance of standards through industry bodies and voluntary uptake has a long and successful record of achievement across a wide range of fields.

Notable organisations include:

- the International Standards Organisation and Standards Australia – responsible for thousands of standards across many fields including financial data interchange standards;
- the World Wide Web Consortium and Internet Engineering Taskforce – responsible for the standards that have underpinned the world wide web since inception and the internet since the early 1990s;
- the mutually owned New Payments Platform Australia which developed and recently launched the NPP that is now delivering instant low cost payments;
- the international standard setter for interbank standards, the banking cooperative SWIFT; and
- the Institute of Electrical and Electronics Engineers (IEEE) which develops many computing and electrical/electronic standards.

AFMA suggests, noting the Government's desire for an accelerated outcome, that the standards associated with the Consumer Data Right be moved to a similar model, perhaps after an initial period of Government control.

Instead of the standard approach outlined above, the proposal is to set up a Committee by Government statute with a selection of industry appointees, consumer advocates, all financial regulators as observers and overseen by the ACCC. The regulator is new to standards creation and management and to financial data standards in particular.

In addition to overseeing the development and setting of the standards the ACCC will be tasked with enforcement of the standards.

It may be useful to consider whether some of the costs associated the creation of a new and costly regulatory scheme to enforce a particular inter-business standard can be avoided. This has been achieved in major jurisdictions already. APIs are already developed and available for some institutions and in progress for others, and the industry is committed to improving connectivity through market mechanisms that are likely to be more flexible, lower cost, and ultimately better performing than a government overseen and enforced standards process.

If there is a legislated principles-based requirement to provide customers with their data in a reasonable format, then breaches of this requirement could be addressed by the courts. We would suggest that for financial institutions there would likely be a high level of compliance with principles-based legislation approach and prosecutions may be highly unlikely.

Business to business interconnection is usually done on a voluntary basis, standards are developed on a co-operative basis and without Government management, and market forces determine which standards will be adopted, promoted and abandoned. Market-based approaches to designing and implementing detailed business practices and processes have long been shown to have inherent efficiency and flexibility advantages over more centralised practices. Lower costs to the taxpayer are also a feature of industry-based solutions. It may be the case that creating and maintaining an expensive new regulatory function as is proposed is not necessary in the longer run and we note in this regard while the report notes several jurisdictions looking to potentially follow the UK lead, the US has indicated no intentions of doing so and will rely on market mechanisms.

While industry experts will help in the statutory committee, ultimately the ACCC and the responsible Minister will be responsible under the proposed design for ensuring the standard finds the right balance between security and privacy, innovation, speed to market, the level of granularity and detail, and the level of difficulty of implementation and cost.

This is a difficult balance for industry to get right in the usual industry-led voluntary processes. Examples of some of the challenges are listed below:

- Different security approaches can be used which will have different costs and benefits, including ease of customer use, implementation cost and complexity, vulnerability to hacking, flexibility to deal with different security levels for different interactions etc. With the mandating of a security standard there are risks that firms will be forced to take on security risks that they are not comfortable with, yet will be still be liable for failures of the required standards.
- There are many elements of standard design that will affect the ability of firms to innovate if the standards are mandated. Standards can vary greatly in their level of extensibility and this can restrict innovation. SWIFT has been a highly successful standards-setter over many years, including ISO 15022 and ISO 7775 which relate to interbank message types. ISO 15022 was developed in part because the overly prescriptive nature of ISO 7775 made innovation difficult as it contained too high a level of detail (being the message standards themselves) rather than principles to which compliant messages should conform. Standards can aid or retard innovation depending on quite technical details. Standards can be designed to be more innovation ready – for example the XML standard which is self-describing and can be used to define data types in a wide range of fields. HTML by contrast is more limited and designed only for screen display of typically web content. Yet XML itself is only a partial implementation ie. a simplification, to ease implementation costs of an earlier and more sophisticated but now little used mark-up language SGML. This demonstrates how getting the balance right is critical for a standard to be successful.
- The Government and ACCC would need to determine a release and update schedule for the standard and these would need to change over time as the standard matures or adapts. This decision would affect multiple firms with differing levels of implementation resourcing and priorities. Detailed infrequent releases would cause large system changes that would need to be coordinated across the industry. Smaller more frequent releases would also need to be coordinated but would mean constant resourcing load on participants.
- A standard will have to be set to a certain level of detail – the current proposal extends to the data field level which is a very high level of detail. Exact definitions of each field will need to be agreed by multiple parties and systems changed at participant firms to ensure they produce data in conformance with the exact definition agreed. The advantages of this approach are the need to build to a singular data schema. The disadvantages are that it would stifle innovation and restrict the offerings firms could make within the standard. A higher level standard with less prescriptive criteria would be more flexible but would mean there may be a range of API builds that are required by firms wishing to connect to multiple institutions. This approach however would be more flexible and supportive of innovation.
- There are also a myriad of design choices that will have to be made for example in relation to connectivity protocols. While the process in standards creation globally works on the basis of what parties are willing to do, the “oversight” of the regulator may interact with these choices

given the ultimate responsibility of the Government for the standards under the proposed design.

- The Government will also have to balance speed to market. Speed should not be prioritised over the need to ensure that security concerns are comprehensively addressed. Speed to market will also affect the maturity of the released product. Faster time to market is likely to result in a less mature product, requiring sooner and more frequent updates and changes.
- Finally, cost will have to be balanced by the standard. There are costs for all participants in standards creation processes and users of standards. Some standards can be more difficult and costly to implement but might provide more features, easier evolution, higher security and greater flexibility. Where to land on the many detailed and structural standard questions is as always difficult to get right and will need updating over time.

The proposed compulsory nature of the standard means that the Government will be required to determine the appropriate level of each of these matters and then the regulator would presumably prosecute firms who fail to conform to the release schedule. Industry normally makes arrangements to coordinate rollouts of new technology but it is not yet clear how this might work in the proposed framework.

As noted in the Final Report, the regulator will need extensive powers under the model proposed to review internal processes and schedules to determine if firms are making reasonable efforts to meet Government deadlines.

Recommendations Responses

The Final Report makes the following recommendations:

> **Recommendation 1.1 – allowing for competing approaches**
> Open Banking should not be mandated as the only way that banking data may be shared. Allowing competing approaches will provide an important test of the design quality of Open Banking and the Consumer Data Right.

AFMA fully supports this recommendation. While the general approach of the Final Report is regulator-centric this is an important concession to the standard way that businesses approach standards. Competing approaches, and competition in general, should be allowed to emerge, and recommendation 1.1 appears to support this outcome.

Following from this, if in the future Open Banking becomes redundant, as standards often do, then it should be retired, including its regulatory structures.

The regulatory program should not extend to cover international standards. If the Open Banking standard does become redundant then its costs should go too. The purpose of the regulator in the Report is to make available a particular standard designed and approved by Government processes, not to enforce standards that are outside those processes.

> **Recommendation 2.1 – a layered regulatory approach**
> Open Banking should be implemented primarily through amendments to the *Competition and Consumer Act 2010* that set out the overarching objectives of the Consumer Data Right. The amendments should enable the designation of a sector by Ministerial direction and create the power to set out regulations and operational Rules for sectors. This structure will embed a customer and competition focus in Open Banking, while allowing the Consumer Data Right to be scalable across sectors.

Originally the Consumer Data Right was about individual consumers and small businesses, however, over time this has been expanded to include medium business and now is proposed to include all businesses regardless of size. “Consumers” refers to individual people (OED “A person who purchases goods and services for personal use”). Medium and large firms at a minimum are not consistent with this definition, and as such the Consumer Data Right is no longer as proposed solely about consumers but is a general right at law if it is extended to these classes of persons.

Even where we consider the case of the individual consumer, while the data and right to download is theirs, the practical matters for enforcement may not involve consumers directly. They will be between the businesses supplying the data and the businesses receiving the data. That is, they will be business to business matters that will need to be resolved.

Care needs to be taken that framing these issues within an individual consumer framework does not lead to undesirable outcomes. Data connection protocol issues between a large financial firm and large technology firms are best understood as commercial matters to be resolved through normal commercial mechanisms, even where there is a required standard. Where smaller firms are involved

as data receivers a case might be made for a mediated arrangement, but this still is unlikely to involve the type of arrangements set up for consumers.

In relation to competition, while firms could at least in theory resist providing the protocols for anti-competitive reasons, this is a theoretical concern at present. Firms are far more likely to face competing priorities for resources internally than a fear of competition when considering how to facilitate Open Banking.

In any case, similar issues are present and already dealt with by sector regulators in the financial sector. Access on fair terms to a range of systems and facilities – for example payments, financial market exchanges, clearing & settlement - are already facilitated.

While it appears to be the Government's intention that the Consumer Data Right will reside in the *Competition and Consumer Act*, it may also be appropriate to consider whether it should form part of a coherent whole with the protocols and rules in a separate "Data Act".

> **Recommendation 2.2 – the regulator model**
> Open Banking should be supported by a multiple regulator model, led by the ACCC, which should be primarily responsible for competition and consumer issues and standards-setting. The OAIC should remain primarily responsible for privacy protection. ASIC, APRA, the RBA, and other sector-focussed regulators as applicable, should be consulted where necessary.

A non-prudential regulator may not necessarily be a natural home for a data regulator, given that the primary role concerns defining and maintaining data protocols and business-to-business communication both of which generally lie outside the scope of competition matters.

Further, and of critical importance in the financial sector, there are judgements that need to be made about the amount of risk that should be allowed to be introduced into the financial system by the Open Banking regime.

Open Banking will address some risks already in the system associated with screen scraping but it will also introduce some risks and if it moves to a read/write model these risks could become substantial, particularly as we move to an environment where payments can increasingly be made almost instantaneously.

A series of unauthorised transfers out of a bank via Open Banking protocols or a significant data leak at a data company with many clients with accounts in the banking system could readily have prudential implications.

In such a circumstance, judgements will need to be made about how much weight to place on the prudential concerns. For this reason we support the multiple regulator model where the RBA and APRA have a key role in the consideration of any prudential matters.

APRA and the RBA would ensure that system stability has primacy. While the innovation provided by fintech applications is an important development that should be supported by Government and industry, the scale and consequences of system stability must remain a primary focus.

As noted, while the consumer is central to the data right and the policy, the disputes and balances that will have to be reached are between businesses. The sector regulators are better placed to understand the interactions between the businesses in the wider context of sector developments and the priorities that should be made.

Recommendation 2.3 – the banking Consumer Data Right
Banking should be designated as a sector to which the Consumer Data Right applies.

AFMA supports the extension of a Consumer Data Right to the ADI sector as a way to improve services and security for consumers.

Our comments relate only to the mechanisms and regulatory frameworks through which these outcomes are achieved.

Recommendation 2.4 – Rules written by the ACCC
The ACCC, in consultation with the OAIC, and other relevant regulators, should be responsible for determining Rules for Open Banking and the Consumer Data Right. The Rules should be written with regard to consistency between sectors.

Following on from the above comments, Rules should be principles-based and incorporate primary regard for the stability of the financial system.

Recommendation 2.5 – the Standards
The Standards should include transfer, data, and security standards. Allowing supplemental, non-binding, standards to develop (provided they do not interfere with interoperability) will encourage competitive standards-setting and innovation.

Industry expects to have a key role in helping to develop the standards for transfer, data and security.

Given their success in delivering world leading payments infrastructure this year, and all financial business to business standards over many years, market forces can be reasonably be expected to create standards through such processes as banks compete to be compatible with popular software through open APIs and other technical solutions. Evidence of this can be seen in the existing APIs already available from some banks. These products have emerged out of the existing regulatory system and neither the industry nor APRA have concerns that they pose undue risks.

Recommendation 2.6 – a Data Standards Body
A Data Standards Body should be established to work with the Open Banking regulators to develop Standards. This body should incorporate expertise in the standards-setting process and data-sharing, as well as participant and customer experience.

Australia has well established, internationally recognised standards setting bodies, most notably Standards Australia. Standards Australia is currently leading the global work on block chain standards for example, and has previously created many standards that have been subsequently been globally adopted by ISO.

We suggest that Standards Australia is well-placed to lead the work on developing the required standards.

Standards creation does take time, but this is appropriate given their importance. It is perhaps surprising that the Final Report only considers Government bodies such as Data61 as capable to run the Data Standards Body when the great majority of standards are produced by industry bodies such as Standards Australia.

We note with some concern the proposal on page 22 to override the Data Standards Body if standards are not produced quickly enough (presumably as judged by the Government or the regulator), as this approach may have consequences for sound security and other design elements. We anticipate that the Government (or the regulator) would only seek to override the Data Standards body in the most serious circumstances.

> **Recommendation 2.7 – accreditation**
> Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.

We note again the need for prudent management of risks associated with access to the Open Banking system. These risks should be assessed by participants and regulators with a deep understanding of these risks. A non-prudential regulator cannot be expected to have the same deep understanding of the prudential and systemic implications for setting and monitoring accreditation criteria and will likely require the assistance of a prudential regulator.

> **Recommendation 2.8 – the accreditation criteria**
> Accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging parties from participating in Open Banking. Using a tiered risk-based accreditation model and having regard to existing licensing regimes should minimise costs for many participants. Accreditation decisions should be reviewable by the Administrative Appeals Tribunal.

The existing prudential framework is an appropriate model for managing the risks associated with firms that wish to be receivers of Open Banking data.

The Report proposes that the competition regulator should "consider what would be needed to passport accredited entities from other jurisdictions into Australia's Open Banking system"[1]. This is a risk assessment function with implications for systemic prudential risks.

Accordingly, APRA will be well placed to judge prudential and operational risks associated with Open Banking parties.

[1] Report p. 27.

Recommendation 2.9 – responsibility for the address book

The ACCC should have responsibility for ensuring there is a public address book showing who is accredited.

There should be a publicly accessible register of accredited persons.

Recommendation 2.10 – customer complaints and remedies

Open Banking should have internal and external dispute resolution processes to resolve customer complaints. Amendments to the *Competition and Consumer Act 2010* should create powers to address complaints (to the extent these do not already exist) and give customers standing to seek remedy for breaches of their rights. There should be a single consumer data contact point - there should be 'no wrong door' for customers. The OAIC should retain enforcement powers in relation to privacy and could also be given enforcement powers of confidentiality for businesses.

Recommendation 3.1 – customer-provided data

At a customer's direction, data holders should be obliged to share all information that has been provided to them by the customer (or a former customer).

However:

• The obligation should only apply where the data holder keeps that information in a digital form.

• The obligation should not apply to information supporting an identity verification assessment. Data holders should only be obliged to share that information with the customer directly, not a data recipient.

The risks associated with customer-provided data centre around identity theft. To manage these risks and consistent with our response to Recommendation 3.2 below we suggest that this sensitive data could be reserved for later phases of the roll-out.

Recommendation 3.2 – transaction data

At a customer's (or former customer's) direction, data holders should be obliged to share all transaction data in a form that facilitates its transfer and use.

The obligation should apply for the period that data holders are otherwise required to retain records under existing regulations. Table 3.1 describes the list of accounts and other products to which this obligation should apply.

Transaction data is high value data. This data directly exposes business and transactional relationships. While personal data exposes risks of identity theft, transaction data in aggregate can expose confidential relationships and valuable market data, potentially including data suggestive of trends that could be pertinent to financial markets. These risks and their interaction with the markets need to be properly explored. For example, a firm with many data customers in a foreign jurisdiction may look to mine the data for market sensitive information.

The approach recommended by the Final Report equates to what is known in the IT industry as a 'big bang' release in terms of making everything available all-at-once. This type of approach, while appearing desirable from a theoretical consumer perspective, can introduce many more risks than a more incremental approach.

The 'big bang' approach has fallen out of favour in IT development due to these risks and the more favoured approach now for most products is to adopt an incremental approach where a limited first release is used to bed down issues and increase the knowledge base for future increases in scope. This "continuous release" ethos is expressed as Item 1 of the software principles associated with 'agile' software development in the Agile Manifesto: "Our highest priority is to satisfy the customer through early and continuous delivery of valuable software."[2]

Given the types of risks associated with the data involved we believe it is appropriate for the industry to adopt an approach that best manages the software release risks, in this case through an incremental release process.

> **Recommendation 3.3 – value-added customer data**
> Subject to Recommendation 3.4, data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.

AFMA agrees with the assessment of the Final Report that value-added data should not be included in the scope of Open Banking.

> **Recommendation 3.4 – identity verification assessments**
> If directed by the customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome.

We note that a comprehensive review of the AML/CTF legislation currently being led by the Attorney General's Department, with the first phase of legislative reform having passed through Parliament in late 2017. Issues related to Recommendation 3.4 could be considered as part of that ongoing review.

> **Recommendation 3.5 – aggregated data**
> Aggregated data sets should not be included in the scope of Open Banking.

AFMA agrees with Recommendation 3.5

> **Recommendation 3.6 – product data**
> Where banks are under existing obligations to publicly disclose information on their products and services — such as information on their price, fees and other charges — that information should be made publicly available under Open Banking.

AFMA has no comment on this recommendation, other than to note our comments in relation to Recommendation 3.2 that the roll out should be incremental and careful, with a focus on security.

> **Recommendation 3.7 – application to accounts**
> The obligation to share data at a customer's direction should apply for all customers holding a relevant account in Australia.

[2] https://www.agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/

AFMA is of the view that the application of the Consumer Data Right to large businesses is currently unnecessary given the nature of these relationships, the resources and relative sophistication of the parties involved, and the complex nature of the data involved.

As we have noted previously this proposed extension takes the Right beyond something associated with consumers, who are, by definition, individual people. The rationale for a general data right at law including large business to large business would be very different to one justified and motivated by concerns for the imbalances in resources and sophistication experienced by individual consumers.

AFMA does not agree with the conclusion that "actually carving a set of customers out of scope could prove to be an additional cost, not a cost-saving". It is our view, based on consistent member input, that this would likely be a significant saving given the additional complexities involved. On this basis we encourage the Government to reconsider this proposed design element as it will introduce significant and ongoing costs for little gain.

> **Recommendation 3.8 – application to ADIs**
> The obligation to share data at a customer's direction should apply to all Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches. The obligation should be phased in, beginning with the largest ADIs.

Customer demand should determine which ADIs participate in Open Banking. There are likely to be inefficiencies for introducing mandates for ADIs for which there is no or limited customer demand.

> **Recommendation 3.9 – reciprocal obligations in Open Banking**
> 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.

> **Recommendation 3.10 – eligibility to receive data**
> Authorised Deposit-taking Institutions (ADIs) should be automatically accredited to receive data under Open Banking. A graduated, risk-based accreditation standard should be used for non-ADIs.

AFMA agrees that ADIs should be automatically accredited given their ADI status.

> **Recommendation 3.11 – no charge for customer data transfers**
> Transfers of customer-provided and transaction data should be provided free of charge.

While it may be appealing for the Government to set prices as "free" in reality there will be costs associated with providing Open Banking. These costs will have to be paid by the business which in turn will use money from other businesses to meet the costs.

It would be helpful if there is greater clarity around what types of data policy makers believe should be provided for free, and the service levels that should attach to that.

Recommendation 3.12 – transfers of identity verification assessment outcomes

Provided that the liability borne by the original verifying entity does not multiply as the outcomes of identity verification assessments are shared through the system, those outcomes should be provided without charge.

We refer to our comments in relation to Recommendation 3.11.

Recommendation 4.1 – application of the Privacy Act

Data recipients under Open Banking must be subject to the Privacy Act.

Recommendation 4.2 – modifications to privacy protections

The privacy protections applicable to Open Banking should be modified as suggested in Table 4.1.

Recommendation 4.3 – right to delete

Given the many complexities involved in legislating for a right to deletion (including the range of legal obligations to retain records) and the fact that individuals currently have no right to instruct deletion of their personal information under the Privacy Act, it is beyond the scope of Open Banking to mandate a special right to deletion of information.

Recommendation 4.4 – dispute resolution for small business

Small business customers should be given access to internal and external dispute resolution services for confidentiality disputes similar to those that exist for individuals under the Privacy Act.

Recommendation 4.5 – customer control

A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions.

Recommendation 4.6 – single screen notification

A data holder should notify the customer that their direction has been received and that the future use of the data by the data recipient will be at the customer's own risk. That notification should be limited to a single screen or page. Data recipients should similarly provide the customer with a single screen or page summarising the possible uses to which their data could be put and allow customers to self-select the uses they agree to.

Recommendation 4.7 – joint accounts

Authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from the joint account. Each joint account holder should be notified of any data transfer arrangements initiated on their accounts and given the ability to readily terminate any data sharing arrangements initiated by any other joint account holders.

AFMA makes no comment on Recommendations 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, or 4.7.

Recommendation 4.8 – security standards

In order to be accredited to participate in Open Banking, all parties must comply with designated security standards set by the Data Standards Body.

Recommendation 4.9 – allocation of liability

A clear and comprehensive framework for the allocation of liability between participants in Open Banking should be implemented. This framework should make it clear that participants in Open Banking are liable for their own conduct, but not the conduct of other participants. To the extent possible, the liability framework should be consistent with existing legal

frameworks to ensure that there is no uncertainty about the rights of customers or liability of data holders.

Broadly in relation to Section 4 and Recommendations 4.8 and 4.9 in particular we note our concern that the Final Report considers that "too great an emphasis on privacy and security could delay or even undermine the effective introduction of Open Banking"[3]. AFMA is of the view that there cannot be too great an emphasis on privacy and security when dealing with financial sector data. It is essential to the success of the Open Banking regime that the security and privacy settings are robust and protect consumers. The stability of, and trust in, the system must be the Government's priority given the stakes involved.

There is currently high public confidence in the safety of the banking system's security systems, which have been entirely developed by the private sector. The Government mandated systems proposed will, as the Final Report suggests, introduce new risks and these risks must be carefully managed.

Industry is best placed as the Productivity Commission Data Report suggests to develop industry-specific security arrangements. The argument given in the Final Report that "the right balance needs to be struck to ensure that security standards do not act as a barrier to market entry for new start-ups and lead to lower competition" suggests that the Final Report may not have given the appropriate level of priority to security in the financial sector context. Systemic security has large downside risks for the economy and as such it should be given a much higher weighting when compared against the potential competition benefits offered by new start-ups. The balance that should be targeted should be strongly in favour of system stability and security.

As the Final Report notes "In the UK, the Implementation Entity has released technical security standards in the areas of customer authentication, API specification and encryption. The standards are highly detailed and are prescriptive in nature." It should not be assumed that the UK is the appropriate model for adoption locally. Standards are highly detailed and are prescriptive in nature are often inflexible and costly. We again note that higher level principles would allow industry more latitude to innovate and keep costs down.

We note concerns with the proposal that the financial institutions are to be held liable for data interceptions as proposed in the liability framework – for example:

> "A malicious actor manages to intercept the customer's data during the transmission between the bank and an accredited data recipient…The bank should be liable to the customer for the loss suffered by the customer because of its failure to transfer the data at the customer's direction." [4]

This interception may have occurred despite the firm following the Government-mandated security protocols. These protocols might have become vulnerable to attack and conformance to them may have compromised the security of the data. It would be unfair to hold parties liable to events caused by their conformance to law.

[3] Report p. 50.
[4] Report p. 67.

The potential for such cases highlights the risks associated with the Government taking on the role of detailed security standard setter for the private sector.

We respond below to Recommendations 5.1, 5.3, 5.7, 5.8, 5.10 and 5.11 together and then respond to Recommendations 5.2, 5.4, 5.5 and 5.6 separately.

> **Recommendation 5.1 – application programming interfaces**
> Data holders should be required to allow customers to share information with eligible parties via a dedicated application programming interface.
> **Recommendation 5.3 – extensibility**
> The Data Standards Body should start with the core requirements, but ensure extensibility for future functionality.
> **Recommendation 5.7 – access to rich data**
> Customers should be able to authorise access to transaction data in full. Data recipients should not be limited to accessing pre-set functions or sending blocks of their own code to run on the system of the bank or its partner or prevented from caching data. However, participants should be free to offer services that provide more limited data to data recipients who have lower levels of accreditation.
> **Recommendation 5.8 – intermediaries**
> The Standards should allow for delegation of access to intermediaries such as middleware providers.
> **Recommendation 5.10 – access frequency**
> The Data Standards Body should determine how to limit the number of data requests that can be made.
> **Recommendation 5.11 – transparency**
> Customers should be able to access a record of their usage history and data holders should keep records of the performance of their API that can be supplied to the regulator as needed.

Recommendations 5.1, 5.3, 5.7, 5.8, 5.10 and 5.11 demonstrate why the detailed standards of business to business data connectivity could be better determined by industry and flexible private sector processes rather than by Government.

For example in relation to Recommendation 5.1, industry is better placed to determine the merits of particular technologies and to change to the next (as yet) undeveloped technology swiftly as the need arises. Government mandating of particular technical solutions in the business to business space may be at risk of rapidly becoming out of date, and hampering innovation and business efficiency.

WebAPIs have been around since 2000 with widespread adoption only in the last 6 years or so, but they may be unlikely to be around for a long time given typical technology lifecycles.

Even mandating that a particular technology be made available by industry will crimp innovation as once a firm has been forced to spend money on a particular Government required technology they will be much less likely to also develop a new or evolving platform.

The concern to get the balance around extensibility right faces similar hurdles. Extensibility is ideal but there are trade-offs in terms of complexity and overbuilding a solution, that may still become obsolete. Again Governments may not best placed to be determining these matters for business.

Recommendation 5.2 – starting point for the data transfer Standards

The starting point for the Standards for the data transfer mechanism should be the UK Open Banking technical specification. The specification should not be adopted without appropriate consideration, but the onus should be on those who wish to make changes.

AFMA is of the view that the UK standards – those the Report refers to as "highly detailed and…prescriptive in nature" may not be the best starting point for data transfer standards.

Compared to the US approach, and even the EU standards, the UK standards are the least flexible and most likely to result in a decrease in innovation over time, and technology lock-in. Technology lock-in occurs when it becomes hard to move away from redundant technology.

Australia should aim for a flexible principles-based approach using the benefits of customer demand and market forces to determine what outcomes are efficient.

Recommendation 5.4 – customer-friendly authentication and authorisation

The redirect-based authorisation and authentication flow detailed in the UK technical specification should be the starting point. Consideration should be given to the merits of a decoupled approach provided it minimises customer friction.

AFMA is of the view that a decoupled approach is more resistant to phishing risk, and given the priority that must be attached to security, a redirect approach should not be mandated by the Government.

If the Government mandates particular approaches that compromise security then liabilities should be realigned. It is not appropriate for liabilities to fall on firms for actions they were required to take by the Government.

Recommendation 5.6 – persistent authorisation

Customers should be able to grant persistent authorisation. They should also be able to limit the authorisation period at their discretion, revoke authorisation through the third-party service or via the data holder and be notified periodically they are still sharing their information. All authorisations should expire after a set period.

The starting point of the Review that "Customer convenience is a key consideration for this Review" means that "a customer should not have to reauthorise an application each time they want to access information" is not a sufficient basis to reach the conclusion that persistent authorisation is an appropriate and secure mode for data connections to ADI systems.

Persistent authorisation increases risks above a transactional approach. The risks to security need to be properly assessed before such a conclusion could be reached. The assessment so far is not sufficiently adequate to give confidence the conclusion is well founded.

Recommendation 5.5 – no additional barriers to authorisation

Data holders may not add authorisation requirements beyond those included in the Standards. Requiring multifactor authentication is a reasonable additional security measure, but it must be consistent with the authentication requirements applied in direct interactions between the data holder and its customers.

Again we note our concerns about restricting the security protections that can be put in place by the industry due to Government rules. Liability cannot fairly flow when financial firms' options are restricted.

A full risk analysis of the risks to the system (which are likely to change over time) should be conducted before a set of security protocols could even considered to be ruled the maximum allowed. The security of the system must remain paramount.

> **Recommendation 6.1 – the Open Banking Commencement Date**
> A period of approximately 12 months between the announcement of a final Government decision on Open Banking and the Commencement Date should be allowed for implementation.

AFMA is firmly of the view that the proposed timing is far too tight to enable a proper standards development process, and to deliver products to the market.

The objectives of this project include speed to market, but also the level of privacy and security, the quality of the standards, policies, rules and regulatory structures, quality of the software implementations at participating ADIs, quality of testing, ease of use and reuse, and extensibility, among other things.

AFMA supports a phased approach. A 12 month timeframe risks compromising the objectives of the process, including security, and should not be attempted.

A more limited delivery of a sub-set of standards might be deliverable within 12 months and this could form a basis for a wider set of standards. Consultation with the industry should be undertaken before the sub-set is determined.

> **Recommendation 6.2 – phased commencement for entities**
> From the Commencement Date, the four major Australian banks should be obliged to comply with a direction to share data under Open Banking. The remaining Authorised Deposit-taking Institutions should be obliged to share data from 12 months after the Commencement Date, unless the ACCC determines that a later date is more appropriate.

While we support a phased approach as per our response to Recommendation 6.1 this should be initially on a sub set of products for the first group. We support allowing customer demand and market forces to determine which ADIs participate.

> **Recommendation 6.3 – commencement date for data**
> From the Commencement Date, Open Banking should apply to transaction data and product data. However, Open Banking should not apply to transaction data relating to transactions before 1 January 2017. Open Banking should apply to customer-provided data and the outcomes of identity verification assessments on a date to be determined by the ACCC.

As noted we support a reduced initial scope perhaps limited to some account types or to product data. We support firms having the option to limit data to recent data.

Recommendation 6.4 – consumer education programme

The ACCC as lead regulator should coordinate the development and implementation of a timely consumer education programme for Open Banking. Participants, industry groups and consumer advocacy groups should lead and participate, as appropriate, in consumer awareness and education activities.

Industry is willing to lead and participate, as appropriate, in consumer awareness and education activities.

Recommendation 6.5 – the appropriate funding model

As banking is the first sector to which a much broader Consumer Data Right will apply, it would be difficult to impose an industry-funded model to cover regulatory costs at the outset. Neither the total costs, nor the number of sectors or participants will be known for some time, so it would be impossible to make an estimate of the average cost until the system is well-established. The funding arrangement could be reconsidered after a period of operation, when there is a more refined cost structure and greater certainty over the number of participants.

We agree with this Recommendation.

Recommendation 6.6 – timely post-implementation assessment

A post-implementation assessment of Open Banking should be conducted by the regulator (or an independent person) approximately 12 months after the Commencement Date and report to the Minister with recommendations.

We support an independent third party assessment of the proposed system including a full cost benefit analysis.

****