Australian Banking Association

Response to the Farrell Report into Open Banking

Submission to Australian Treasury

Pip Freebairn

Policy Director

23 March 2018

Australian Banking Association Inc.
ARBN 117 262 978

(Incorporated in New South Wales)
Liability of members is limited.

Australian Banking Association

Table of Contents

Australian Banking Association

1. Summary

Australia's banks are committed to the success of open data which, if delivered properly, can empower customers to use their data from across the economy to make the best choices for their circumstances and preferences.

The ABA commends the Farrell Report for its thorough and thoughtful examination of open banking and open data more broadly. The ABA believes Mr Farrell's report correctly focused on the needs and wants of customers when weighing stakeholders' needs.

ABA members support the majority of the recommendations in the Farrell Report. Our response is intended to provide Treasury with ABA members' views on the best path forward to ensure open data can be successfully implemented and so customers can benefit as quickly as possible within an environment of strong consumer safeguards. We have not cited those recommendations that ABA members broadly support.

2. Implementation timeframes

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.

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.

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.

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.

ABA response

ABA members do not believe that a 12 month implementation period from the Government's announcement of an open data regime is feasible. This would not provide sufficient time for standards and rules design, and the subsequent technology build that requires the standards and rules before it can begin.

Major banks are committed to implementing open data 12 months after the establishment of the standards and rules, and smaller banks a minimum of 12 months behind that.[1]

ABA notes that consumer safeguards through appropriately designed security and data standards will first need to be designed and in place, as well as economy-wide data sharing rules to address, among other things, protections on customer privacy and liability. ABA members are committed to assisting the

[1] This would equate to total timeframe of 18 months from the legislation of the Consumer Data Right for the largest banks and at least 30 months for smaller ADIs if the rules are standards are set within the six-month timeframe outlined by Scott Farrell in his report. The 12-month implementation period would begin when the rules and standards are set.

Government to devise the rules and standards within the six-month period outlined by Farrell although we note this is an ambitious timeline given the UK experience.

Challenges are likely to be faced by the banking industry as the first industry to fall into the open data framework. This includes the appointed regulator devising the economy-wide open data "rules" or guiding principles in parallel to the Data Standards Board developing the standards to apply to banking. These challenges are not insurmountable but require strong collaboration between the regulator and the Data Standards Board, together with strong participation from stakeholders. With this in mind, the ABA has proposed a path forward on standards setting which appears in the Appendix.

ABA members note that the United Kingdom experience highlights that significant time was spent establishing the product data taxonomy. Consequently, we propose a phased product launch on the data to be shared in Section 3. ABA members believe this is achievable and will focus on delivering the greatest benefit to the largest number of customers as quickly as possible, before subsequent phases are launched leveraging the lessons of the first phase.

Finally, smaller ADIs support the one-year extension in roll out of open data and note that this extension should be applied across all phases. Reforms like open data come at a high fixed cost for smaller and regional banks which, like all ADIs, are faced with a substantial government reform program. The ABA also notes that all ADIs should be able to benefit from lessons learnt through the phases and that the system should retain sufficiently flexibility to be modified to ensure its success.

3. Appropriate funding model

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."

ABA response

ABA members strongly endorse this view. We also note that the industry already directly funds elements of the work of the ACCC through levies applied for APRA and should not be required to pay any further.

Australian Banking Association

4. Product scope

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.

Table 3.1: Farrell Report's proposed list of banking products

Deposit Products	Lending Products
• Savings accounts • Call accounts • Term deposits • Current accounts • Cheque accounts • Debit card accounts • Transactions accounts • Personal basis accounts • GST and tax accounts • Cash management accounts • Farm management accounts • Pensioner deeming accounts • Mortgage offset accounts • Trust accounts • Retirement savings accounts • Foreign currency accounts	• Mortgages • Business finance • Personal loans • Lines of credit (personal) • Lines of credit (business) • Overdrafts (personal) • Overdrafts (business) • Consumer leases • Credit and charge accounts (personal) • Credit and charge accounts (business) • Asset finance (and leases)

Source: *Review of Open Banking – Final Report*, Treasury

ABA response

Australian customers would benefit from a phased approach to ensure that the greatest number of customers can benefit from open banking as soon as possible.

Industry and regulators will need to devise product data taxonomy before data sharing can take place. This involves setting industry-wide standards that standardise the data fields themselves, wording/language, and data quality.

ABA members do not believe that this is feasible for all products in Table 3.1 within one year. Instead we propose:

- product reference data and transaction data for those products listed under Deposits in Table 3.1 are rolled out in the first 12-month implementation phase for large banks after the standards and rules are set, and no earlier than 24 months for smaller banks;
- other products are rolled out in subsequent stages with timelines set based on the experience of the first wave, beginning with credit cards.

The ABA notes the importance of credit cards to consumers and therefore the importance of including these products as an immediate next step following deposit and transaction account product data sets. Credit card data fields should be those transaction data that are currently disclosed, and for product reference data should be those data required to be disclosed by the *National Consumer Credit Protection Act 2009*.

This roadmap for implementation is reflective of the volumes of products held by Australians as detailed below. Products in the first phase also have the fewest number of data fields to be standardised.

The ABA/Roy Morgan Customer Behaviour Survey shows that 18 million or 96 per cent of people stated that they had a transaction account.[2]

RBA payments data[3] shows that these products have the greatest number of customers:

- At the beginning of 2018 there were 46.8 million debit card accounts, almost two for every person in Australia. Over the past year 2.1 million more accounts were added.
- The number of credit card accounts was 16.7 million at the end of 2017. The number of accounts has grown by 1 million over the past three years.
- Other lending products have fewer customers. For example, APRA data shows that there are 5.7 million mortgages on the books of banks (both owner occupier and investor).[4]

The ABA also recommends that deployment commence with single account-holders, giving industry time to solve for joint accounts and accounts held by business with complex structures. Industry can work with Government on a parallel roadmap to approach this challenge.

5. Customer scope

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.

ABA response

The ABA recognises the value and benefits of data to personal and SME customers. However, large business loans are highly specialised and should not form part of open banking, especially as demand for this data being shared via an open banking platform has not been established. Large business customers have well-established relationships with their banks that can enable them to request data in the way that is most suitable for them.

The ABA recognises the difficulty cited in the Farrell report that "it might be harder to exclude large businesses than include them" given the difficulty finding an appropriate definition of small business.

Ideally, the Consumer Data Right legislation would contain a small business definition that applies across the economy to the open data framework consistently, and small business in is not defined sector by sector. The Australian Banking Association's recently revised *Banking Code of Practice* contains a definition of the small business that could form the basis for an open data framework definition. The Code has been consulted on extensively.

[2] ABA/Roy Morgan Customer Behaviour Survey
[3] RBA payments data https://www.rba.gov.au/payments-and-infrastructure/resources/statistics/payments-data.html
[4] APRA data http://www.apra.gov.au/adi/Publications/Documents/QPEX_December_2017.pdf

What is a "small business"?

A business is a "small business" if at the time it obtains the banking service all of the following apply to it:

a) it had an annual turnover of less than $10 million in the previous financial year; and

b) it has fewer than 100 full-time equivalent employees; and

c) it has less than $3 million total debt to all credit providers — including:

i. any undrawn amounts under existing loans;

ii. any loan being applied for; and the debt of all its related entities that are businesses.

6. Recognising the economic value of data

Recommendation 3.11 – no charge for customer data transfers

Transfers of customer-provided and transaction data should be provided free of charge.

ABA response

Open data should be directed primarily towards helping consumers make better decisions and in the banking context, enabling them to manage their finances more effectively.

ABA members believe that the open data economy should recognise the economic value of data.

The ABA supports transaction data being transferred for free when the transferee is limited to using that data for the direct use case. For example, if a customer consents for their transaction data to be transferred to a third party for the direct use case of comparing a new loan product and limits the transferee's right to use that data for that purpose only, then no charge should be levied on either the third party or the customer.

Furthermore, for data that is transferred for free, the ABA considers that to avoid unnecessary burden on industry there should be clear service levels on how that data is made available. Compelling data holders to make data available without charge and on demand will create substantial cost when most use cases do not require that level of availability. The ABA agrees with the Farrell Report that there should be expectations set on the number of times data can be 'called'.

In the cases where customers provide consent for unrestricted use cases, the transferee is likely to be able to gain value for that data beyond the use that directly benefits the customer. For example, the transferee may be able to derive significant value through segmentation and aggregation insights, which it can then recoup through selling those insights. This is beyond the objective of open data and the ABA believes that further consideration should be given for an economic model in the case of data transfer for unrestricted use cases.

Australian Banking Association

7. Digital Identity

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.

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.

ABA response

Establishing a system of trusted digital identity is not only vital to innovations like open banking, but to strengthen and improve Know Your Customer (KYC) reforms and to prevent online payment fraud. Each of these objectives is complex and requires careful consideration.

Several approaches to establishing an Australian digital identity are emerging. The ABA Council recently identified that working with the Australian Payments Council to establish a system of digital identity is a priority for the industry. This work is being done with extensive input from stakeholders including government, digital identity platforms, industry groups and regulators.

Consequently, we request that identity verification assessments and KYC verifications are scoped out of the Open Banking Framework. ABA members provide a good faith assurance that a parallel workstream to address digital identity will lead to better and least-cost outcomes for customers and industry.

8. Consent and authorisation rules

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 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.

ABA response

The ABA strongly endorses the principle that customer control over data should be paramount, and therefore should be expressed clearly in the rules framework for Open Data. We believe all the principles outlined in Recommendation 4.5 should be incorporated into the final consent model.

A recent example that highlights the importance of informed consent involves Facebook users' data being used beyond a survey they had consented to participate in. In an open banking context, without informed consent, customers could fall prone to predatory participants who use customers' data to offer them products or services beyond the scope of why the customer originally consented to sharing data. This is especially problematic for vulnerable customers and products like payday loans.

The ABA seeks clarification how data already held should be addressed after a customer has revoked authorisation. In this case, it is worth considering if the data can still form part of an aggregated data set held by the third party if the customer has withdrawn consent for their data.

9. Standards

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.

Recommendation 5.3 – extensibility

The Data Standards Body should start with the core requirements, but ensure extensibility for future functionality.

ABA response

ABA supports this approach and the principle of extensibility for future functionality. The ABA's preference is to devise standards relating to APIs and consent models that focus on setting a standard base to enable interoperability and efficiency, but is not overly prescriptive so as to stifle innovation. Standards should also be designed in a manner and forum that enables them to evolve easily.

9.1 API Standards

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.

ABA response

The ABA does not support mandating the UK Open Banking technical specification, and in addition the ABA recommends that a number of changes be applied to the UK Open Banking technical specification to improve the standard and make it more appropriate for the Australian market. Furthermore, the opportunity to leverage the experience from the APIs that have already been published by some of the ABA members could help inform the standard in Australia

Importantly, well designed API standards could provide a source of international competitive strength for Australian banks and fintech start-ups and therefore we believe this is the best path forward. Ensuring that the standards are not overly prescriptive and establish a base level required for interoperability is the best way to enable a competitive market to enable further innovations and the best customer outcomes to evolve.

Positive aspects of UK Open Banking technical specification

The ABA members consider that there are several positive aspects of the UK Open Banking technical specification, notably:

- It is based on widely used open technology standards such as JSON;
- Guidance has been taken from the general tech industry rather than just banking;
- Well documented centrally; and
- Standards are principle based first with the technical specification coming afterwards.

Recommended adjustments to the UK Standards

To date, ABA members have identified that Australia's API standards should differ from the UK standards in the following aspects:

- *Lack of extensibility within the APIs*

There is no room for extension of the UK Open Banking APIs to incorporate out of scope data. We recommend taking an approach where a "minimum" standard payload is defined with the option for participants to define and use extensions.

- *Block versioned*

  The use of block versioning rather than end-point versioning will potentially limit the speed of innovation, or addressing issues with the APIs, because the APIs will only evolve at the speed of the whole. The use of end-point versioning for minor versions and applying major versions at the block level for more significant changes should be considered.

- The management of fine grained authorisation through the APIs is not supported by the ABA members. Coarse grained authorisation concepts such as whether the third-party can access the API are appropriate to be managed through the standard and can probably be managed through an OAuth based solution. However, it is recommended that fine grained authorisation concepts such as the complex methods of operation on an account should be managed internally within the Bank's solution as opposed to being externalised through the API layer. Externalising this logic will drive significant complexity and risk into the solution. Furthermore, given that the first phase of Open Banking in Australia is focussed on read only APIs for reference data and transaction information, these simpler use cases should not require the complexity associated with fine grained authorisation concepts and, therefore, the considerations for how to support these concepts should be deferred to when they are needed.
- The authentication standard should only be prescriptive as it pertains to maintaining a standard set of touch points for third parties. Banks should be able to continue to evolve and iterate their security models to match their - and their customers' - risk appetites.
- The UK payloads, as defined to date, are not entirely appropriate for the Australian market, such as the difference between the UK's sort codes versus Australia's use of the Bank State Branch codes (BSB).

9.2 Security Standards

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.

ABA response

Banks have long inserted customer friction into their own authentication processes to ensure customers are not vulnerable to phishing attacks through learning bad behaviours. Banks do not email URLs to customers that redirect to logon to Internet Banking or that ask customers to verify their account details, PIN, passwords or personal information. This has been a consistent message from the banking industry to ensure that customers follow good security practices to ensure that their finances and privacy are protected.

ABA members believe that a decoupled model is the best and most secure approach to data sharing authentication and authorisation, carefully balancing a small element of friction against the customer's security. Open banking must protect customers, and their username and password should only ever be presented together in a bank's own asset and never on a third-party app.

The risk with any model that redirects from a third-party site or app to a page that asks a customer to provide their Internet Banking username and password is that it is very difficult for the Customer to tell the difference between an accredited third-party who is redirecting to a genuine Internet Banking page, versus a phishing attack that is designed to capture Internet Banking usernames and passwords in order to commit fraud. Hence, the ABA members recommend that the Australian Open Banking standard avoid establishing any process that encourages customers to enter their Internet Banking

username and password into any application other than via the Bank's Internet Banking site or mobile app.

One model of how the third-party could interact with the banks is through a variation of the widely used OAuth Authentication standard where the customer enters something into the third-party which identifies themselves, such as their mobile number or their email address which is then used by the third-party to redirect to the bank. But rather than the bank prompting the Customer to enter their login credentials, the bank instead prompts the Customer to open either their mobile banking app or their Internet Banking app in order to authorise the third-party. This approach is consistent with the OAuth standard without suggesting to customers that it is safe to enter their Internet Banking credentials into pages they are redirected to from less trusted sites. If the customer uses a mobile banking app this interaction could be improved through the use of mobile push notifications to prompt the Customer to authorise the third party and, furthermore, it could leverage enhanced security features available on mobile devices such as fingerprint verification to perform the authentication and authorisation steps.

There is currently work underway by the OAuth Financial API (FAPI) working group to define a Client Initiated Backchannel Authentication (CIBA) standard that has the characteristics referred to above.[5] The intent of the Financial API Standard is to provide a profile for OAuth 2.0 suitable for use in financial services.

The exact design of these consent models could be left to competitive forces. But ABA members warn strongly against approaches that would make customers more prone to phishing and other cyber security risks.

Finally, ABA members recommend against the introduction of the read-only credentials referred to in the report. This is largely due to the risk that the introduction of an additional password is likely to cause customer confusion, in particular the challenge of knowing when to use one password versus the other and, therefore, is unlikely to result in reducing the risk of the customer's password being compromised.

10. Reciprocity principle

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.

ABA response

The ABA supports the principle of reciprocity especially as data sharing occurs across industries like technology.

Scoping how reciprocity extends into other industries is likely to take some time. The ABA supports a principles-based approach to defining equivalent data across industries. We would encourage Treasury to recommend that a review process to investigate and define the concept across equivalent industries is established as a matter of priority given the time it is likely to take to consider a system of economy-wide data reciprocity.

[5] The OAuth Financial API working groups' proposal can be found here: https://bitbucket.org/openid/fapi/src/a9e55356b5f233af804227d5001d3c32d23d1a91/Financial_API_WD_CIBA.md

11. Liability

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.

ABA response

The ABA supports this recommendation and endorses the principles that participants are liable for their own conduct and that customers should be no worse off.

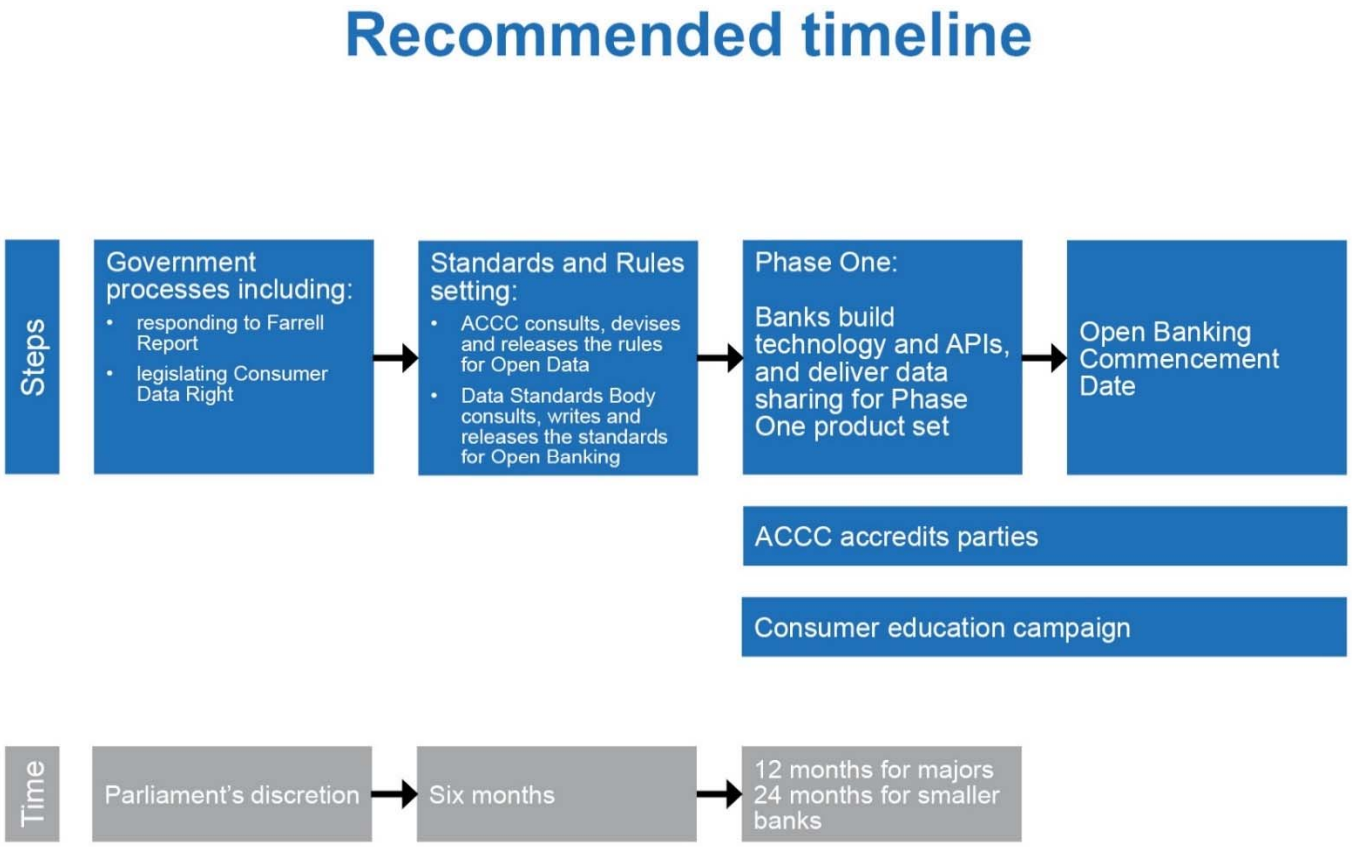
Accreditation criteria will be important determinants in ensuring that liability responsibilities can be adequately met by all participants. For example, ensuring that third parties have adequate insurance and capital, and are mature organisations. Accreditation for data intermediaries such as data exchanges that enable non-accredited third parties to gain data insights will also need to be carefully calibrated.

The review leaves several aspects open around how the liability framework would work including if it is binding and if so, would it be enforceable by a regulator like the ACCC or through the courts.

The ABA also notes that review of ASIC's ePayments Code is more pressing given innovations like open data and the NPP and their implications for liability for unauthorised third-party payments. The ePayments code is administered by ASIC so any open banking rules and standards must seek input from ASIC.

Australian Banking Association

Appendix A – Implementation sequencing and timeframes



Australian Banking Association

Appendix B – Technical Standards Body

The establishment of a Technical Standards body is a key enabler to delivering an API economy based on a safe and consistent exchange of data artefacts. We see the body has primary responsibility for the specificity of the implementation of Open Data across the economy, and would represent specific verticals through specialist presence. As per other international standards development, the remit of the Technical Standards Body should be established by policy without prescription as to the method of execution. A balanced representation of key stakeholders and independent technical experts will then be empowered to debate and innovate.

Currently we are supportive of the recommendation posed in recent Treasury forums with the commencement of the body provisioned by the ACCC with an independent chair, containing key representation across data holders, accredited parties, customer, and technology/industry expertise called the Data Standards Body.

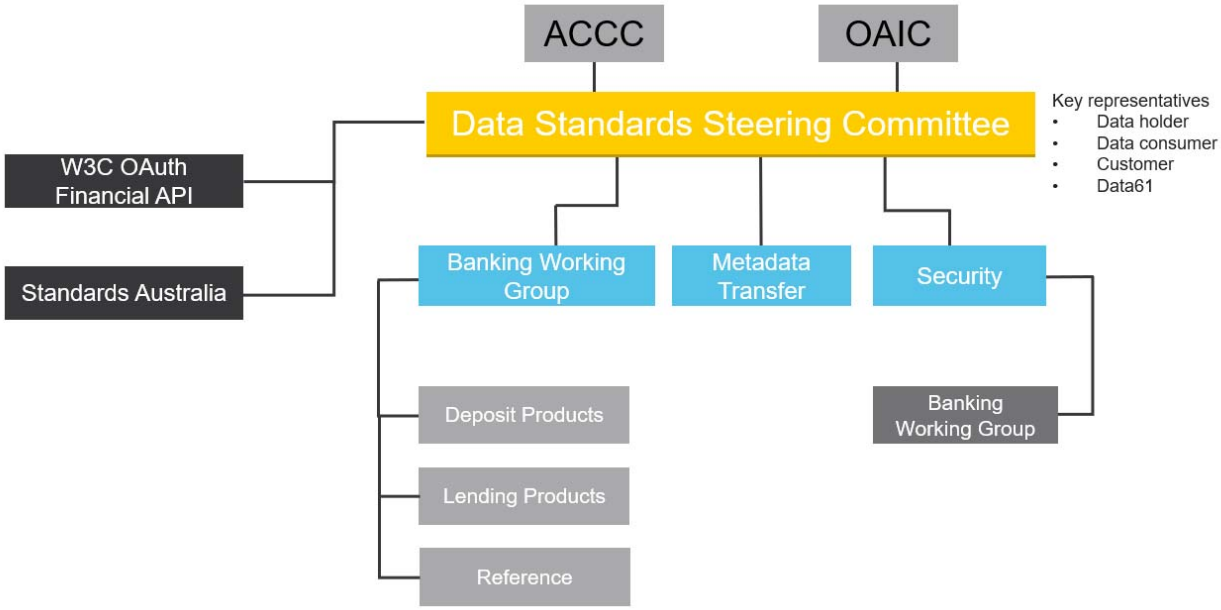
We would hope this formation allows for a centralised governing body looking at the holistic issues surrounding Open Data. Due to the complex nature of the specific topics, we would then ask the centralised committee to form a series of working groups in which specialist skill sets could be involved. To-date the current proposed structure of these groups would be:

- **Security**
    - Reviewing the concerns around customer consent and authorisation, the protection of API endpoints, and the issuing of certificates to verify third party data consumers. Due to specific nuances within the banking domain, we envisage that speciality sub-sections may be required to ensure compliance of these principles to financial regulation concerns.
- **Transfer and Metadata**
    - Coverage includes the handling of data, and its discrete components to be standardised ensuring universal interpretation. This group should also cover schema extensibility, versioning, URI patterns, and other foundation elements.
- **Banking & Financial Service Specific Working Group**
    - Looking at the detailed implementation of the API schematics across the four primary streams as specified within the Farrell report.

Key lessons learned from the established of standards in countries such as the UK, is this process is not effective when managed in a “waterfall” delivery fashion. Each group should essentially run in an agile fashion by maintain a regular working cadence and a visible backlog of work. As a result, we would strongly urge for the correct tooling to be established to support these practices.

We also recognise that the required resourcing and effort required to support the development of standards would vary given the maturity of the standards body. As a best practice, a scaled approach to the formation of the standards body is recommended. It would need to be accepted that greater effort required in the establishment phase, which may see artefacts produced in quick/short intervals for a review. Once mature, we would then recommend scaling back to a maintenance and operational cadence requiring less overall resources delivering amendments and revisions over greater timeframes.

It has been determined that to be truly successful with an establishment of an API standard, it should be derived from a well-founded best practice. To help ensure key learnings, and provide foundational aspects to each of the above practices, that once the Technical Standards body is established it becomes affiliated and established a working cadence with global standards organisations such as the OpenID Foundation (Oauth) and the Open API working group.


ACCC
OAIC
Data Standards Steering Committee
Key representatives
Data holder
Data consumer
Customer
Data61
W3C OAuth Financial API
Standards Australia
Banking Working Group
Metadata Transfer
Security
Deposit Products
Lending Products
Reference
Banking Working Group

Australian Banking Association

About the ABA

With the active participation of 24 member banks in Australia, the Australian Bankers' Association provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.