Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

23 March 2018

The Treasury
Langton Crescent
Parkes ACT 2600

By email: data@treasury.gov.au

RE: Open Banking Report – Final

This submission from the Australian Privacy Foundation (The "APF") responds to the Open Banking Report (the "Report").

General comments

The APF contends that the current legislation in place is not sufficient to protect the privacy of individuals using open banking. The current privacy laws in Australia are weak compared to the European Union and UK privacy laws (for example, General Data Protection Regulation). The protections in place in the event of a data breach are also inadequate. Worse, the access to justice available for individuals affected by a privacy breach are inadequate. In this context, there is concern that individuals may be harmed when using open banking.

Open Banking will apply widely. It will apply to a wide range of organisations with varying commitments to the privacy of their customers. The risks of data leakage and breaches increase with access to data. Individuals in Australia have very weak control over their own personal information. Sharing personal information with one organisation often means an agreement to share with other organisations. The bundled consents signed by many individuals are on a "take it or leave it" basis. Consent has to be meaningful. It currently is illusory.

Data breaches are a common occurrence in Australia and internationally. APRA has recently introduced a new prudential standard on data security.[1] With data breaches it is not a matter of "if" but "when". The Privacy Act has recently been amended to require the notification of data breaches. That is a step forward but it does not provide reasonable access to justice in the event of a serious data breach. It does not provide a clear compensation and fine framework to incentivise business to avoid data breaches.

In our view, there is no doubt that the risk of a data breach will increase with open banking. Individuals accessing open banking should be made aware of those risks. There are no plans to

[1] See http://www.apra.gov.au/MediaReleases/Pages/18_10.aspx

provide any education on this point. The recommendations do not ensure that individuals are adequately protected. The recommendations should not proceed without these issues being addressed.

We have also had the opportunity to review the submission from Financial Rights Legal Centre and Consumer Action Law Centre. APF supports the recommendations in that submission.

The Consumer Data Right – Fact Sheet

The Fact Sheet has clearly not been consumer tested as it is difficult to read and understand. If a fact sheet is to be developed it needs to be revised significantly.

It does not cover:

- The risks involved with open banking (including the spread of personal information, data breaches, no right to delete and limited ability to control consent)
- Enforcement in the event of a dispute and how to seek compensation
- Details about EDR and how the process will work
- Details of what a high level of security actually means

Fintech

Fintech is being given certain regulatory exemptions to test products by ASIC.[2] It is essential that any fintech with exemptions from ASIC should not be accredited to use open banking. People need to be sure that they are dealing with organisations that are complying with all relevant regulations. This principle should apply to any organisation with any exemptions that may weaken consumer protections.

Specific comments on the recommendations

Recommendation 2.2 – the regulator model

The APF does support the ACCC as the lead regulator because it is an adequately funded and active regulator. The OAIC (in contrast) is an inadequately funded and inactive regulator. As the OAIC remains responsible for privacy (a key part of open banking) it is essential that the OAIC is adequately funded with a commissioner appointed with a real commitment to regulatory enforcement in privacy to build trust.

Recommendation 2.4, 2.5 and 2.6 – Rules written by the ACCC, the Standards and a Data Standards Body

Supported subject to properly funded consumer and privacy advocates to be involved in the development of those Rules and Standards. Industry or Government should fund a participant in the standards working group and a joint consumer/privacy submission. If consumer and privacy advocates are not involved in this process then it will lack credibility as it will not have a consumer focus.

Recommendation 2.7 - accreditation

Supported.

[2] See http://asic.gov.au/for-business/your-business/innovation-hub/regulatory-sandbox/

Recommendation 2.8 – the accreditation criteria

Accreditation should be a barrier to entry. The concern about costs should not be used as a way to undermine the effectiveness of accreditation. Individuals need to be able to trust accreditation as a standard and it should be a high standard.

There needs to be a clear process to remove accreditation in the event of a data breach(es) and complaints.

Recommendation 2.11 – remedies

Remedies and access to justice is a key right for individuals. Access to justice for individuals must include:

1) Access to free internal dispute resolution to respond to a dispute
2) Access to a free external dispute resolution scheme (the Australian Financial Complaints Authority)
3) Access to Court or the OAIC if the individual does not accept the outcome of the AFCA decision

There is considerable confusion at the moment how the remedy process would work in open banking. A major concern would be that individuals would be forced to take disputes about open banking to the OAIC as the dispute is privacy related.

The OAIC currently provides a dispute resolution process for privacy disputes. There are a number of serious problems with that process including:

1) The OAIC can discontinue the investigation of the dispute under section 41 of the Privacy Act for a range of reasons. This means that the vast majority of disputes are never decided. There have only been 26 determinations since 2010 and before that there was only 1.

2) There is considerable delay (due to a lack of resources) for the OAIC making any determinations.

3) The OAIC is a regulator and it does not have expertise in dispute resolution (compared to EDR).

4) There is a 12-month time limit to make a complaint to the OAIC compared to a 6-year time limit in EDR. This is a significant difference and considerably reduces access.

Currently, the Financial Ombudsman Service excludes privacy disputes from its terms of reference as follows:

5.1 Exclusions from FOS's jurisdiction

The Service may not consider a Dispute:

a) about whether a Financial Services Provider has met confidentiality or privacy obligations unless the Dispute about confidentiality or privacy:

(i) is part of a broader Dispute between the Financial Services Provider and the Applicant; or

(ii) relates to or arises out of the provision of credit, the collection of a debt, credit reporting and/or the banker-customer relationship;

Based on the above terms of reference it is arguable that open banking disputes would need to be handled by the OAIC and consumers would not have access to EDR. This would be a very poor outcome for consumers who would expect access to EDR only to find that it was not available.

Individuals need to be confident about being able to access EDR when a dispute remains unresolved. This means that accreditation to use open banking must require membership of an EDR scheme and that any legislation makes it clear that individuals have access to EDR in the event of a dispute.

It is essential that the terms of reference of AFCA is clear on this point and can consider privacy disputes with a member of AFCA.

Recommendation 3.1 – customer-provided data

Supported subject to the right of the customer being able to review the information being shared. There may be information that the customer shared with their bank that they do not wish to share.

Recommendation 3.4 – identity verification assessments

No comment.

Recommendation 3.8, 3.10 and 3.12

No comment.

Recommendation 4.2 – modifications to privacy protections

We do not believe the proposed modifications represent sufficient protection to ensure that consent is meaningful. The reference to "express consent" is not sufficiently detailed.

We recommend that the proposed changes include a great deal of prescription on consent including:

- Consultation with the OAIC on best practice consent
- The consent must be on a separate dedicated form or web page
- The disclosure on the consent form is consumer tested to be effective disclosure
- Contains information about risks
- There is an option to limit consent to only one entity
- The consent is time limited and when it expires
- How to withdraw consent
- How to complain including IDR and EDR contact details
- That there is no right to delete the data transferred

Recommendation 4.3 – right to delete

This is an example of inadequate privacy rights in Australia. The fact that there is no right to delete is a reason why people may not want to use open banking.

Recommendation 4.4

See comments above at recommendation 2.11 which also apply to small business.

Recommendation 4.6 – single screen notification

This needs to be tested for effectiveness. It may be necessary to be more prescriptive about format as it is likely it could be designed to be difficult to read.

Recommendation 4.9 – allocation of liability

The suggested framework needs further consultation and detail to be effective. In particular, it is necessary to consult in detail with the regulators and AFCA to ensure that the details are clear to all involved.

Recommendation 5.2, 5.3, 5.4, 5.9 and 5.10

Supported.

Recommendation 6.2 – phased commencement for entities

Not supported. Making the banks obliged to start open banking when they are not ready to do so is a risk for individuals. The data of individuals should not be put at risk to meet arbitrary deadlines.

Recommendation 6.4 – consumer education programme

Supported subject to adequate funding and consultation with consumer and privacy advocates to ensure that risks are explained.

Recommendation 6.6

Supported and essential.

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely

Kat Lane
Vice-Chair
For the Australian Privacy Foundation Board
0447 620 694
Kat.Lane@privacy.org.au