



23 March 2018

The Treasury  
Langton Crescent  
PARKES ACT 2600

email: [data@treasury.gov.au](mailto:data@treasury.gov.au)

Dear Sir

### **Review into Open Banking in Australia – Final Report**

Thank you for the opportunity to respond to the Final Report into the Review of Open Banking in Australia (released 9 February 2018). Overall, we support the framework proposed in the Final Report. We believe the Review struck a reasonable balance between privacy, security, innovation and competition, for the ultimate benefit of Australian consumers, small and medium businesses and the financial services industry.

Equifax is a global information solutions company. We use data, innovative analytics, technology and industry expertise to transform knowledge into insights that help our customers make informed decisions. Headquartered in Atlanta, Equifax operates in North America, Central and South America, Europe and the Asia Pacific region.

Established as The Credit Reference Association of Australia in 1967, then as Veda and now Equifax, we have strong discipline in data governance across the personal information lifecycle and compliance with privacy principles. We continue to invest in our data and security processes, systems, people and policies.

We are already collaborating with a number of Australian financial institutions to understand and use bank transaction data, extracted from appropriately permissioned accounts, to deliver innovative products and services for consumers. We are also strong contributors to the open banking regulations being implemented in the UK and Europe.

We look forward to working with the Government, Regulators and the industry to ensure robust, flexible Standards and Rules that support the ultimate objective of the proposed reforms; expanding consumers' right to access their data to facilitate choice, efficiency and innovation in an evolving digital landscape.

At this time we highlight four key lessons gained from our experience.

#### 1. Tiered Accreditation

The Report recommends a tiered risk-based accreditation model (Recommendation 2.8). The risks being assessed are 'the harm that may arise if there were to be unauthorised access to the data.'<sup>1</sup> Protecting privacy, and ensuring certainty of recourse for any harm, is a critical aspect of any data sharing regime. As highlighted in the Report, the framework should also reduce unnecessary barriers to entry.

The proposed accreditation model should be flexible enough to allow data users, who do not access, view or store raw consumer data, but who request consumer attributes from a secure and accredited data hub. In this case, the data hub would be subject to the strongest level of regulatory oversight and security protocols. The data user in this example need be subject to lighter licensing requirements.

For example, a particular end application needs to confirm that a consumer is above an age threshold. With explicit, informed consumer consent, the end application could instruct a data hub to access the consumer's data. Rather than disclosing or transferring data (in this example, sensitive personal information about the consumer's date of birth) to the end application, the data hub could authenticate an age attribute (either the consumer is or is not above the requested age threshold).

Older technology is based on data being transferred to the point of analysis (in this example, transferring the consumer's date of birth to the end application to calculate whether the consumer is above the required age threshold). New technology turns this around; analysis moves to the where the data is held (in this example, the data hub or even the original data source).

The less data has to travel results in fewer copies and limited opportunities to intercept data which improves overall security and privacy. We suggest the benefits of an open data regime can be better achieved if the accreditation model, Rules and Standards start from this data and analytics frame.

---

<sup>1</sup> Review into Open Banking – Final Report page 25.

The Report appears to contemplate this approach (Recommendation 5.8 Intermediaries), although that recommendation refers to the data transfer mechanism and not accreditation.

## 2. Data Standards

We support the Report's recommendation to use the UK Open Banking technical specifications as a starting point for the Australian Standards (Recommendation 5.2) and a willingness to keep such standards open and accessible. We recognise the importance of such Standards (Data, Transfer and Security) to the efficient functioning and success of any Open Data regime.

However, open data discussions all too often turn into technical arguments about standards and technology. This is often at the expense of actual end-uses that benefit consumers and instil confidence and a willingness to use the rights engendered by the proposed regime.

The Report appears to acknowledge this tendency by recommending that the ACCC (as proposed regulator) retain standards-making powers should the Data Standards Body be unable to produce Standards within a reasonable time (Recommendation 2.6).

## 3. Payments

One key difference between the UK/European regulations and those proposed for Australia is that the Report contemplates only "read" access to accounts. The UK/European regimes incorporate "read" and "write" access.

The ability to affect a bank account through write access (for example, instructing a bank to make a payment) has had a profound effect on the Standards, Rules, accreditation and workflows implemented in the UK and Europe. The additional oversight and accreditation needed for a read/write regime may not be entirely suitable for a read-only regime and may unnecessarily bog down implementation and innovation. We suggest Regulators keep the distinctions in mind when assessing the applicability of the UK experiences to Australia.

The Report explains why the proposed reforms are limited to read-access (and points to the possible inclusion of write-access post implementation). The Report also calls out the importance of interoperability across industries and jurisdictions. We believe that some of the benefits of a Consumer Data Right may be fully achieved only with read/write access. For these reasons, we suggest that representatives from the payments industry be involved at the outset in developing the Standards and Rules that apply in Australia.



#### 4. Credit Information

After an extensive inquiry by the Australian Law Reform Commission, a draft bill and multiple parliamentary inquiries, the Privacy Act was amended and sets out consumer protections about who can access credit information and how that information can be disclosed and used, how long it can be held and obligations for access, correction and disputes

These regulations appropriately balance a financial institution's need to make informed decisions about potential borrowers and a borrower's right to privacy, access to credit and avoiding discrimination. It is conceivable that credit decisions, based on data derived through an open data regime will not be captured by Part IIIA of the Privacy Act, circumventing these substantive consumer protections. We suggest the relevant Regulators carefully assess these impacts.

We support the Report's recommendations regarding consumer education (Recommendation 6.4). This is proving to be a vital part of UK consumers embracing open banking applications. We suggest that consumer education will ultimately be multi-faceted depending on use-cases and the value for consumers in using their proposed Consumer Data Right. Importantly, this approach keeps consumers and small to medium businesses at the heart of any open data rules, regulations and initiatives.

Regards



Julie McKay  
General Manager  
Strategy

Matthew Strassberg  
General Manager  
External Relations Australia and New Zealand