KING&WOOD MALLESONS

Level 61
Governor Phillip Tower
1 Farrer Place
Sydney NSW 2000
Australia

T +61 2 9296 2000
F +61 2 9296 3999

www.kwm.com

22 September 2017

To Open Banking Review Secretariat
The Treasury
Langton Crescent
PARKES ACT 2600

By email: OBR@treasury.gov.au

Dear Open Banking Review Secretariat

Review into Open Banking in Australia

We refer to the call for public submissions from the Treasury in relation to the Issues Paper on the introduction of an open banking regime in Australia.

We welcome the opportunity to make this submission on this important development in financial law, which will set an important precedent for future Open Data developments in Australia.

Overview

The Productivity Commission Inquiry Report into Data Availability and Use (**Data Report**) recommended the introduction of a new right for consumers that would allow them to 'trade and use' their data (**Comprehensive Right**).[1] This report has led to the release of the Issues Paper under which consumers could request financial institutions to provide or share their data (**Open Banking**).

While Open Banking is the first consultation in respect of a specific industry that has resulted from the Data Report, it is our expectation that the Data Report's principles and recommendations should be of general application and apply more generally across the economy in a consistent manner.

If our expectation is correct, then it seems fundamental to us that the principles and regulatory framework that are developed for Open Banking must be capable of being applied across all sectors of the economy (with common principles but also with the flexibility in the regulatory design for the principles to be adapted to a specific sector), as and when the Government so decides, and not be specific to the financial services industry. Furthermore, if the Open Data regime is applied more broadly across the economy, it may be advisable at a later stage to introduce a requirement for data recipients to submit to the regime to ensure that competition is supported and parties are not gaining the benefits of receiving data without also being willing to share their own data.

---

1 Productivity Commission, *Productivity Commission Inquiry Report into Data Availability and Use* (2017) 15 (Data Report).

KING&WOOD MALLESONS

Our submission on Open Banking is divided into seven key propositions. They are set out below. The roadmap and timetable for the implementation of Open Banking will not be addressed in this submission, since they fall outside the legal framework and design issues upon which we are best placed to comment.

Proposition 1: Categories of consumer data drive the regulatory framework

Open Banking requires a clear definition of the different types of consumer data to which the regime will apply to achieve the appropriate balance between the interests and concerns of all relevant parties. A key consideration in establishing the definition will be the varying privacy, security, liability and risk concerns associated with different types of data, which in turn will determine the regulatory and legal framework for Open Banking.

In our view, the Government should consider establishing a number of specific categories of consumer data and consider introducing these categories in separate phases, having regard to the specific privacy and risk concerns and the tailored regulatory regimes required as a consequence. The consumer data available under each of the categories below should be limited to only that data already held electronically.

The first category could be "general data". It could consist of the basic transactional data on a consumer's account held by an institution – such as details of accounts held by a consumer with that institution, and details of the changes in the balances of those accounts over time. The consumer could have the right to direct its general data to be provided to it, or a third party at its direction, as a "one-off" transfer or on a continual, regular basis. The distinguishing feature of general data should be that it is created as a direct consequence of a transaction by the consumer with the institution so that it is, in effect, a record of the consumer's actual activity.

The second category of data could be "product data", which could be information on the types of accounts, financial products and other services provided by a financial institution to consumers in general, and which would be useful to consumers to receive in a standard form so as to easily compare the terms and costs of similar accounts, products and services offered by competing financial institutions.

The third category could be "identity data", which is highly sensitive, as it carries a significant risk of identity theft or fraud if not sufficiently protected. In terms of Open Banking, this could be data that is generally collected and held by a financial institution in connection with its "know your customer" procedures. Due to its higher risk profile, identity data should have greater security and privacy protections that perhaps a central data custodian or another regulated entity could provide.

The fourth category of data could be "imputed data", as referred to in the Data Report.[2] This includes data that an institution has developed itself from general data, identity data or data otherwise obtained from some other source independently of the consumer, and which is the result of the application of some type of process, analysis or interpretation by that institution. In our opinion, imputed data should not fall within the scope of consumer data which is subject to the Comprehensive Right, as it constitutes the expert analysis of an institution.

---

[2] Data Report, 207.

The totality of our submission, and our suggestions for the initial regulatory, risk and liability framework for Open Banking, is based on the proposition that "general data" and "product data" are initially the subject of Open Banking. The application of Open Banking to "identity data" will, in our opinion, require a thorough weighing of the balance between consumer convenience and concerns associated with the recycling of this information. Since the extension of Open Banking to "identity data" would require a stricter regime for security, privacy and liability, and possibly the development of a framework and infrastructure for the storage and access to that data, we suggest that it should be considered only for a later phase of the Open Banking or Open Data regime.

This approach of creating multiple categories of consumer data, according to the associated privacy, security, liability and risk concerns, would have the benefit of being applicable to sectors across the economy, including to data held by government departments. To be clear, our views below relate to the creation of an Open Banking framework for general data and product data only, unless stated otherwise.

A related consideration to the definition of consumer data is how consumer data should be utilised. In this submission we refer to the transfer of data for ease, but note that consideration will have to be given to what "transfer" means: the sharing of a copy of data (not a transfer), making data available for review, or an actual transfer. Different security and risk implications may be posed, depending on whether consumer data were being read only or also stored by a company receiving a data transfer.

Proposition 2: Consumers should be individuals and small and medium-sized enterprises

The Data Report states that the Comprehensive Right should apply to individuals as well as small and medium-sized enterprises (**SME**) in Australia.[3]

Accepting that conclusion raises the question of the definition of SME, which is an important issue as any company wishing to make use of Open Banking would need to prove that it qualified on each occasion that a request for data sharing was made.

The Data Report recommended that the definition of SME should be related to the turnover of the entity.[4] We believe that the differences in the turnover and number of employees among SMEs mean that consideration will need to be given to the various characteristics of SMEs when developing a definition to suit the objectives of Open Banking.

In our opinion, the Government could consider different options of definition of SME. One option could adapt the definition of "small business contract" in the Australian Consumer Law, which sets out requirements for fewer than 20 employees and a transactional limit.[5] While a transactional limit may not be appropriate here, the employment test could provide a useful definition for SMEs. This definition would have the added benefit of being straight-forward for an SME to prove on an ongoing basis. Another option could be the definition of "small business" proposed for the new Code of Banking Practice, which sets out requirements for annual

---

3 Data Report, 198.

4 Ibid.

5 Australian Consumer Law section 23(4).

turnover, fewer than 20 employees (or 100 employees for a manufacturer of goods) and a $3 million total drawn and undrawn debt limit.

Proposition 3: The Open Banking model should be predominantly principles-based

Open Data and Open Banking models are being developed globally. They are relatively new and have yet to be extensively tested. As a result, in our opinion, Open Banking in Australia should not adopt a specific overseas model, but should create a framework that is suitable for Australia's own legislative and domestic regime. Also, Open Banking should be compatible with current and pending legislation, including the proposed Data Sharing and Release Act, and should avoid regulatory duplication and inconsistency. Also, any existing legislation (including the *Privacy Act 1988* (Cth)) may need to be amended so that the policy intentions of Open Banking are met, and any duplication or inconsistency is removed. We further recommend that consideration be given to the impact that Open Banking (and Open Data) will have on other regimes, for example the regulations on the use of credit reporting information and government identifiers. Wherever policy objectives are broadly similar, harmonisation of laws should be the objective where possible to reduce inefficiencies.

In our view, a combination of a principles-based regulatory framework, combined with more prescriptive protocols for the sharing of data, would be one way for the Government to implement Open Banking. Given the speed of change in technology, markets and products, a principles-based approach is preferable to ensure that the Open Banking (and broader Open Data) regime continues to be "fit for purpose" across a range of industries in future years and is "technology neutral" in its application. If the Government believes that prescriptive protocols are required, then our view is that they are best determined and applied by industry in the data-sharing process, and the technology applications under which the data sharing are provided, to ensure that data can be shared and read in a consistent and cost-effective manner for all parties. Naturally, such a list of protocols would need to be capable of being updated in order to be adaptable to new technologies and should not create an impediment to data sharing.

Proposition 4: Liability under Open Banking should travel with the data

The Data Report and the Issues Paper for Open Banking make it clear that the policy is founded on the basis of a consumer-driven right to be provided with its data, and to direct the transfer of that data to another person.

If data is being provided at the request and with the consent of the consumer to another person (**Recipient**), and the financial institution has transferred the data in compliance with all security protocols, then our opinion is that any liability for subsequent use and/or misuse of data should rest with the Recipient and should be a risk borne by the consumer.

If a Recipient were to use and/or misuse data, or otherwise act in a way that gave rise to a claim against it by the consumer, then there could be circumstances under which a consumer may not have recourse against the Recipient in the case of loss. For example, if the Recipient did not have the resources to meet a claim, if it were to go insolvent, or if a claim against it could not be pursued for jurisdictional or other reasons. For this reason, we believe that a key element of the Open Banking regime will be informed consent on the part of the consumer. We recommend that the consent contain a clear and prominent warning to the consumer advising of the risks involved and the limitations of any recourse available to the consumer. As consent will need to be given in relation to both a single data transfer and the ongoing streaming of data, consideration

should be given to the provision of periodic consumer reminders with the provision for a consumer to terminate the consent. Consideration should also be given to consent requirements where the data relates to more than one consumer, which could apply to joint accounts or accounts with multiple signatories.

Regarding the content of data transfers, we recommend implementing general relief to persons releasing data in good faith in an attempt to comply with the Open Banking regime and the consumer request. This approach would recognise that there may be associated data that the consumer has not sought or that is subject to disclosure that has not been transferred.

Proposition 5: Licensing system is not recommended for general consumer data

A licensing or accreditation system for Recipients could be considered to provide additional consumer protection. This may be deemed necessary in order to ensure that the Recipient is a type of entity against which a consumer is likely to have recourse in the event of a breach of conduct, or to regulate Recipients who obtain shared data and then passing it on to third parties for a commission.

However, a licensing or accreditation system could also add cost and inhibit innovation and increased competition within the sector.

If the Government believes that some form of licensing or accreditation system is required, then one option could be that a Recipient needs to hold some other form of licence or approval – such as an Australian Financial Services Licence or an Australian Credit Licence in the case of Open Banking. However, not all new entrants in the consumer financial system hold such a licence and not all industries will have an appropriate licensing regime. As an alternative to a licensing system, a self-accreditation system or "trusted data handler" mark, which is only available if certain agreed security and other requirements are met, could be developed to indicate a level of reliability to consumers.

Regardless of the approach taken, we recommend requiring Recipients to be corporations based in Australia.

Proposition 6: Make use of existing regulatory expertise

The Data Report refers to the Australian Competition and Consumer Commission (**ACCC**), the Office of the Australian Information Commissioner (**OAIC**) and a prospective National Data Custodian (**NDC**) having roles in the regulation and enforcement of Open Data.[6] However, there is a risk that a range of regulators dealing separately with overlapping regulatory issues may add complexity rather than cohesion to regulation.

If competition is one of the stated aims of Open Banking, it follows from that mandate that the ACCC is an obvious choice as the initial regulator for the regime.

However, again assuming that the Government intends to apply Open Data across multiple sectors of the economy, and not limit it only to Open Banking, we also believe that a combination of pragmatism and coordination will be required in terms of the establishment and coordination of the regulatory framework. There are likely to be industry-specific issues arising in the implementation, oversight and enforcement of

[6] Data Report, 20, 23.

Open Data in different sectors that extend beyond competition, and which need specific industry input and knowledge as part of the implementation and oversight of the regime.

One alternative that could be considered by the Government is to create a "council of data regulators", with representatives from the ACCC and industry-specific regulators, to oversee all issues associated with Open Data. This would have the ability to expand to include regulators for those future industries involved in the Open Data regime, as and when the principles were applied to them by the Government, and would have the flexibility to apply to Open Data economy-wide and the expertise to deal with regulatory issues in relation to Open Data on a consistent basis across sectors. For example, it could be modelled on the Council of Financial Regulators.

Proposition 7: Recoupment of costs

We make no comment on whether costs should apply to Open Banking and who should bear them. The provision of data-sharing services is likely to come at a cost to the parties, and could be incurred in the development of approved platforms for data sharing, through oversight and compliance costs, and in the course of processing each data sharing request.

If the Government decides to allow a financial institution to make a charge for the provision of a consumer's data, then one model to follow may be to ensure that no such costs are excessive, in line with the current position in relation to personal information requests.[7] Such charges would be monitored by the Open Banking regulatory body.

******

We are making these submissions on behalf of our firm, and the views expressed are our own and not those of any of our clients.

We would welcome the opportunity to discuss these submissions with the Treasury, and are very happy to assist should there be any queries arising from this submission. Please contact any of Renae Lattey, Managing Partner, on 03 9643 4065 / renae.lattey@au.kwm.com, Stuart Fuller, Partner, on 02 9296 2155 / stuart.fuller@au.kwm.com or Patrick Gunning, Partner, on 02 9296 2170 / patrick.gunning@au.kwm.com.

Yours faithfully

King & Wood Mallesons

[7] Australian Privacy Principle 12.8.