17 September 2018

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Mr McAuliffe

Treasury Laws Amendment (Consumer Data Right) Bill 2018

I write in relation to Treasury's consultation on the Exposure Draft of *Treasury Laws Amendment (Consumer Data Right) Bill 2018, A Bill for an Act to amend the laws relating to competition, fair trading, consumer protection and privacy, and for related purposes* (the Draft Bill).

AFMA represents the collective interests over 120 firms in the wholesale markets including 22 Authorised Deposit-taking Institutions (ADIs) that are not branches of foreign banks that will be directly affected by the Open Banking changes.

Open Banking and the Consumer Data Right more generally propose profound changes to the banking and economic environment, the scale and reach of which should not be underestimated. We encourage the Government not to rush consideration of these changes and risk unintended consequences. The resources of government and the affected industries are limited and haste risks counter-productive outcomes. Given the types of risks associated with banking as well as business and consumer data we believe the investment of extra time now is the best option and could help minimize the risk of serious problems arising later.

Proper consideration of the proposals requires a whole-of-government approach including with APRA, Home Affairs, ASIC, RBA and AUSTRAC combined with deep engagement with industry over an extended period and will require a consideration of prudential matters, financial system stability matters, privacy, market integrity, compatibility with money laundering and counter terrorism programs, and the potential micro- and macro-economic impact. While good progress has been made at this time we are of the view the proposal may benefit from more consideration by the full range of stakeholders to be best placed to progress to implementation.

As stated in our previous submission, 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 to give customers more control over their information.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

To do this requires coordination between firms of the way data is transferred, secured by encryption, managed and kept confidential. This will need to include detailed Application Programming Interface (API) standards, security protocols, and internet-based identity verification services.

While AFMA would prefer a market-based and industry-led solution to deliver these outcomes, as we believe this would offer greater flexibility and lower cost, we accept the Government's decision to proceed with the approach outlined in the Draft Bill of creating a complex regulatory infrastructure. As such, we will confine our comments to refinements around the proposed approach.

We welcome the support that has been signalled by Government for our suggestion to consider moving some of the functions that will be assumed by the government back to the private sector after an initial period in the government sector. Particularly those functions which are new to the government sector but for which the private sector has extensive experience, such as in standards development for secure inter-business financial data communication.

Framework concerns

While we understand that the framework legislation is, as the Explanatory Memorandum notes, just that, a framework, nevertheless, we are concerned at the limited amount of guiding structure that is present in the proposed legislation. More should be done to define the scheme within the legislation. In this regard the proposed extent of the delegation of powers to the regulator contemplated under the scheme has raised some significant concerns.

We also note more generally the difficulties in responding to the Draft Bill when so much of the substantive law has been left to the regulations, rules, and standards. While there is always the possibility that a concern might be intended to be dealt with these lower order instruments there does need to be more structure in the legislative layer to ensure the scheme follows its intended course.

Sectoral scope

The expansion of government regulation into business data comes at a time when many businesses, are understanding themselves as ultimately data businesses. Whether the sector is telecommunications, finance, internet search or media the ultimate product is either data itself or is closely related to data. Even industries that would not appear connected to data often now gain their competitive advantage through their use of data, in theory this could include industries as diverse as mining or farming.

The potential reach of the scheme is therefore economy-wide and this is reflected in the lack of limitation as to which sectors can be targeted by the scheme for designation. From this it flows that the economic effects of the scheme could be significant. If this is not the Government's intention that firms in all sectors of the economy should be at risk of inclusion the scheme then it may be appropriate to legislate limits to the sectors or types of sectors that can be included in the scheme. This might for example limit the scheme to firms with the scale to make the required investments.

The limited experience so far with data right schemes both here and overseas has demonstrated that providing the types of connections demanded by these schemes are more complex and expensive for businesses than might have been assumed. For small ADIs or those with limited retail exposure the costs are high relative to the size of their businesses and the benefits to consumers modest at best, which suggests a potentially economically inefficient outcome. For small businesses in other sectors of the economy the relative costs could be higher still, the benefits to consumers diminutive, and the inefficiency from an economic perspective thus greater.

As with the banking sector the designation of any sector within the scheme is a large, complex and costly challenge that requires the commitment of substantial resources for no gain to participating businesses. AFMA is of the view that, given its implications for affected businesses and the potentially political sensitive nature of these decisions, designation of a sector after impartially balancing these costs and benefits should be solely a matter for the Parliament and the Minister and not delegated in practice the regulator.

The framework proposes at 56AE (3) that the Commission may publically recommend in writing to the Minister that a sector be designated. While it is of course entirely appropriate for the Minister to seek the advice of the Commission on the suitability for a sector to be designated this should be done only at the Minister's request and the advice for the Minister's consideration only. The Minister is well placed to balance the costs to business and potential benefits to consumers. Allowing the consumer commission to make public recommendations to the Minister will place considerable political pressure on the Minister to accede to the advice of the commission. As such we would recommend 56AE (3) should be removed from the Draft Bill.

A concern specific to Open Banking, and of significance to AFMA members, is the certainty of the exclusion of non-foreign bank branches from the scheme. While this category of ADIs was specifically excluded in the Open Banking Review paper given that they are "not authorised to take initial retail deposits of less than $250,000 and are concentrated on wholesale banking operations, extending the obligations to branches of foreign banks would not be consistent with the objective of providing opportunities to the general public."[1] There is no legislated exclusion in the Draft Bill. We would seek to have this exclusion firmed through the legislative process and not be left to a potential future overturning recommendation by the regulator.

Definition of consumer

The Draft Bill currently excludes the Competition and Consumer Act 2010's definition of 'consumer' at 4B(1) from affecting the definition of CDR consumer at 56AF(5). The effect of this is to include wholesale business including multinationals and large corporates into the scope of the scheme as 'consumers'. This is a substantial reshaping of the Competition and Consumer Act in relation to the regulator's interaction with business.

The Competition and Consumer Act is generally designed to level the playing field between 'consumers' defined as purchasers of products and services of modest value for non-commercial use

[1] Open Banking customers choice convenience confidence, p. 43.

and the businesses that supply those services, a definition consistent with the dictionary definition of "A person who purchases goods and services for personal use"[2]. The reasoning from the power imbalance that supports a desire to 'protect' consumers does not apply to large businesses as consumers. While an extension to small businesses, appropriately defined, might be sensible, the inclusion of all persons and all firms including multinationals undertaking any interaction wholesale or commercial in the concept of 'consumer' effectively renders the concept meaningless in the context of the affected part of the Act.

The application of a framework designed to protect individuals against large businesses to instead 'protect' potentially large businesses against each other could also lead to unintended consequences. The interactions of wholesale clients are not extensions of the interactions with retail clients and some wholesale clients are larger than the businesses that serve them.

Further, given the complexity of business relationships with wholesale clients there are a wide range of services that are often bespoke to their category of needs. These offerings will not be enhanced by additional services that have as their target retail consumers, and it is likely to be inefficient economically to require them to be offered.

Non-consumer data

The scheme extends beyond consumer data capturing "disclosure, use, accuracy, storage, security or deletion of CDR data for which there are no CDR consumers". There is no requirement in the Draft Bill for a connection of the data with any consumer and "CDR data" is defined as any information designated by the Minister. The effect is that any data held by a business in a designated sector could in theory be caught by the regime. This is potentially a substantial change from the object of including non-consumer data in the Open Banking Review that was limited to products and already publicly available.

The Open Banking Review held that, what it called 'product data', should be made publicly available under Open Banking where banks "are under an existing obligations to publicly disclose information on their products and services"[3]. That is, Open Banking was not designed to make more data public, just to make the data that was already required to be public more readily accessible. The change that would accompany the Draft Bill of potentially bringing any business data within scope should be refined down to the scope outlined in the Open Banking Review.

This is particularly appropriate as non-consumer data cannot be justified by an appeal to a connection with a consumer. The extension to any business data and not merely business data associated with consumers that is already public extends the scope of the scheme potentially beyond the bounds of the justifications for the scheme.

The legislation should limit the information that is required to be brought into the scheme to that which is already required to be made public by other regulatory requirements.

[2] https://en.oxforddictionaries.com/definition/consumer
[3] Recommendation 3.6.

Introducing new non-consumer data disclosure requirements

Further, if it is the intention of the Government to require more non-consumer data to be revealed, then for the same reason, a legal 'rights' framework may not be the appropriate place to situate this requirement. For there is no reason for a consumer, however defined, to have a right of claim against data from a business where that data has, by definition, nothing to do with them. Noting this is less the case where the customer has or wishes to apply for a particular product that the firm seeks to offer them.

Introducing additional data *disclosure* as opposed to *publication format* requirements would be better done through the normal legislative processes around each industry. This process would ensure that appropriate consideration and balance is given to the rights of business to keep their data private. Giving discretion over which business data should be required to be public to a consumer regulator may risk favouring outcomes which place more weight on the benefits to consumers than the costs to businesses.

Risks of requiring non-consumer business data to be made available in a particular format

Even where businesses are required to make certain data publically available already there are still risks of negative economic impacts by requiring the data be made available in a particular format.

The example provided in Open Banking paper was of retail product information. A firm might invest significant resources to determine at what price it can offer its goods and services. Currently, consistent with the principles of a market-based economy, the firm has a wide discretion about how and when it presents this information to potential consumers, this allows them to target different consumer segments.

It may be a significant disadvantage for firms that wish to target particular market segments to be required to make their pricing public in a standardised way that might not present their product with its particular features in the best or even an accurate light. One could imagine economic incentives to build products to look good on the pricing comparator scheme but with a lack of features or flexibility.

There could also be disincentives created to innovate if new features would not show up on the existing models for the comparison of pricing and features, and firms facing a long and uncertain path to get the model changed.

Further, there are issues of intellectual property to consider in relation to data that is not connected to consumers, as requiring its public disclosure may well decrease its value. For example, a firm that believes market conditions warrant a lower price offering may wish to maximise the value of this pricing by beginning with a targeted and quiet marketing campaign that does not initially alert its competitors to the opportunity to lower prices that it has identified.

By requiring this firm to disclose the intellectual property contained in its price to the public it may also alert its competitors and thereby reduce the value of the business opportunity that the

intellectual property contained. This also potentially creates further disincentives to create the intellectual property and advantage to consumers in the first place.

Wholesale non-consumer data

We also note there is no restriction in the Draft Bill of the non-consumer data being mandated to be released to be confined to data related to retail offers. Thus wholesale offers are at risk of being included in the data that must be made available depending on the rules that are adopted by the regulator.

Wholesale information may be entirely unsuitable to be made available publicly in this manner and to require firms to do so may risk putting Australian firms at a competitive disadvantage. If the Government does proceed with this measure we would request that the scope be explicitly limited to retail offers.

Derived data

The Draft Bill at 56AF(2) seeks to ensure that data gained via the scheme cannot be readily taken out of the scheme through the mixing with other data or derivation. While this is an understandable intention, the inclusion of derived data within the scheme leads to unintended consequences and an operationally unworkable scheme.

After transformation by businesses derived data may not be consumer data. For example, collecting insights from consumer spending may allow a business to create a marketing plan for its next product that is more likely to be effective with its intended audience. It would not be aligned with the original nominal intent of the scheme (to make consumer data accessible to consumers) to require this marketing plan to be available publicly under the scheme just because it relied on scheme data.

The scheme also requires 'special' treatment of data gained from the scheme so that the requirements of the rules can be met in relation to that data. In practice this will require careful separate management of the data gained from the scheme with particular operational rules for the physical and virtual servers that manage the data, and related compliance systems to ensure they are backed up, and secured in accordance with the rules. This separate treatment of scheme data adds expense and operational risk and in many cases may not be possible.

One effect of including derived data in the scheme means that if data gained from the scheme is mixed with other business data to create derived data then that other business data will be affected through including or being influenced by data from the scheme. The treatment of that data will then need to comply with the various rules both present and future of the scheme. From a system point of view this may not be possible. The back-up and data security features of a core banking system may not be compatible with the rules that the regulator creates for data management. For example, the backup schedule for a mission critical system may mean that it is not practical to delete data from the system and all its backups once the data has entered the system, and may run contrary to other data retention requirements.

As such, and contrary to the intentions of the scheme, firms may be incentivised to ensure they do *not* make business use of the data gained from the scheme in relation to their existing systems. As once the data is affected by use of the CDR data, firms may face significant costs to make those systems compatible with the rules and potential future rules of the scheme or they may not be able to comply with the scheme in relation to the affected data.

Risks to be managed with scheme data and derived data

We understand the Government has concerns, which the regulations seek to address, that entities may establish themselves with the purpose of gathering the consumer data of large numbers of consumers and acting as a 'funnel' to minimally transform this data (if derived data was not included) and then on-sell it to firms outside of the scheme and potentially outside of the jurisdiction.

This is a reasonable concern. Firms in possession of large amounts of consumer data particularly outside of the jurisdiction could well be possession of otherwise confidential information that could be used to their advantage.

These risks also exist for data that has not been transformed but has received consent from the consumer to be moved out of the system, and as the regulator paper notes, potentially overseas.

We understand from the regulator's consultation paper that the Government's intention, while acknowledging the risks of data leaving the system and jurisdiction is to rely on consumer consent to limit risks. AFMA holds that more work in this area should be done to ensure the risks that arise from data leaving the jurisdiction and scheme are appropriately addressed. This is particularly important in the light of public concerns about how their data is being used expressed in high profile US congressional hearings.

For example, a firm could pay a small benefit to a large number of consumers and collect their real-time spending patterns at particular retailers. The information could be consolidated by amount and spending destination and on-sold to investors potentially outside the jurisdiction. This consolidated[4] information may well constitute inside information from a share trading perspective.

Similarly, a firm could collect the banking data of customers in order to identify consumers (if direct marketing consent is given), for rival vendors. For example, a firm could look for users of Bob's Pool Cleaning and transform this data into derived data by consolidating it by the suburb in which they are most located and the average fee paid to Bob's. This summary data could be sold to Alice's Pool Cleaning. The economic impacts of these types of services and products should be fully investigated.

In relation to systemic prudential risks, the aggregation of statistically significant data on the withdrawals and missed payments for loans of a significant number of customers of a particular bank could be readily used to create a bank risk rating or stress product. The existence of such a product could exacerbate prudential risks to individual banks and the wider financial system during a period

[4] Each individual's account data would not be inside information as it would not be statistically significant.

of financial crisis. This information might be of interest to investors, foreign businesses and entities. These types of risks might be matters for the consideration of the prudential regulator, the markets regulator and the central bank and other relevant government agencies.

Open Banking moves data from the highly secure banking environment to non-bank data firm, and as the regulator acknowledges[5] this increases risks associated with data theft. Particularly, when the scheme moves eventually to a 'write' phase as mooted in the Open Banking Report (at which time the data would include the ability to direct payments from customer accounts) this could increase risks around fraudulent transfers and, in theory should these multiply, could result in challenges to systemic confidence. There are related national risks associated with the moving of sensitive data to more and varied entities that would need to be addressed before a 'write' phase could be safely implemented. AFMA supports the RBA's preference that digital identity initiative be integrated with the open banking initiative and suggests the RBA continue to be included in an assessment of the risks that could arise from the 'write' phase. These risks should be thoroughly addressed in the design of the scheme. We note the intention of the regulator not to address risks associated with "particular uses" including transfer of data outside the scheme, transfer of data overseas, on-selling of data, and direct marketing.[6]

Risks associated with data and AML/CTF matters

AFMA is concerned of the risk of the rule-making powers being used to require certain non-consumer data public under the scheme. Concerns have been raised with us that data that is required by the Government on money laundering and other risk assessments by firms of customers in relation to financial crime could be required to be made public under the scheme by the regulator. This could have implications in relation to prudential risks and crime prevention that need to be properly explored. The merits of such a decision properly rest with the whole of government including Home Affairs, AUSTRAC and industry.

Concerns have also been noted in relation to the identification processes and their sufficiency for AML and CTF purposes. Firms have internal programs which require certain standards to be met when identifying customers in association with KYC programs. Open Banking and the CDR scheme more generally should be harmonised with these existing arrangements.

More generally, members are concerned with potential conflicts of the requirements of the scheme in relation to security which may not be compatible with the existing high standards required. AFMA encourages Treasury to engage with AUSTRAC and Home Affairs on the potential of the scheme to introduce additional risks and to ensure compatibility of the scheme with existing requirements and arrangements.

[5] Page 49 Consumer Rules Framework Consultation.
[6] *Ibid.* p. 39.

Undefined rule making scope

AFMA is concerned at the wide scope that the framework gives for the creation of rules and standards. In addition to the concerns we have noted above around the designation of sectors we note concerns that more generally there are ineffective legislative restrictions on the rule making power in the Draft Bill.

Under 56BB the scheme rules can deal with the disclosure, use, accuracy, storage, security, and deletion of any business data, the accreditation of data recipients, reporting and record keeping, and any incidental or related matters.

In the relevant sections that follow (56BC, 56BD, 56BF, 56BG, 56BH) which could set some initial bounds on what the rules should be about, these all commence with the wording "Without limiting paragraph 56BB(*x*)". The result is that they have no limiting effect as drafted and only serve to ensure the power is not under-read.

The only limitation on the rule making power is that it cannot apply before 1 July 2019 and that it cannot create retrospective obligations. These are extremely modest limitations for a rule making power delegated to any regulator. The rules, which as we have noted are not limited in the legislation to any particular business data in a designated sector, can be made to require any activity and impose any obligation, right or penalty.

This is a highly unusual delegation of the function of government and it potentially is not in the interests of the regulator to have such untrammelled scope for rule making. Given the significant impact of the rules on the affected businesses including smaller businesses, if it is not the intention of the Government to grant a general rule making power in relation to business data, then a more structured framework for the rules is required which at a minimum specified the purposes for which the regulator may and may not make rules, and what the data is that can be the subject of those rules.

As a starting point the regulations should limit 56BB to the matters noted in 56BC, 56BD, 56BF, 56BG, and 56BH, but without the phrasing "Without limiting paragraph 56BB(x)". These broad powers should then be further refined for each sector within the regulations. More generally it may be appropriate to confirm through advice from the Solicitor General that the scope of delegated administration rule-making power contemplated by the legislation is within powers and appropriate.

Fees

AFMA is concerned about the proposal for the consumer regulator to be setting fees for data this is both in relation to data for which there is a consumer and for which there is no consumer and particularly for derived data.

As per our previous submission in relation to non-derived data regarding Open Banking, the proposed fixing of a price to zero by the government introduces a market distortion and requires affected business to find funds to provide this service from elsewhere in their business.

While noting this concern, our main focus in this submission is in relation to derived data. Derived data may have had substantial effort put into its creation and the bulk of the contained information may well not be sourced from scheme data. As such, it is inappropriate for the government to fix the price (and thereby deny competition) that firms can charge for its provision.

Prices are best set by market forces, and in relation to pricing products and services this should be done by the firms that produce those products and services. By using firms to price products and services market economies use the distributed information that is available to those on the ground. Setting prices by government agencies has a poor history and is likely to lead to significant distortions over time, and across different firms. AFMA strongly supports allowing firms to set prices in relation to the services they provide under the scheme.

Further, if the Government does intend to fix prices in relation to the scheme then the consumer regulator may not be best positioned to balance the desire of consumer for low or no cost pricing and the interests of businesses that are required to provide the service. Consumer regulator's incentives might be towards setting prices lower than businesses would set them themselves as this would benefit consumers at the cost of businesses.

Cost

Treasury has asked for information on the costs of implementation of Open Banking. The systems that need to be developed and integrated for compliance with Open Banking require extensive integration with multiple core banking systems. Development of systems that connect to core banking systems must be done with a high degree of care and can be costly. The distribution of these costs across all non-foreign branch ADIs falls disproportionately on smaller ADIs which will have far higher costs per unit revenue than the larger ADIs.

Penalties

The level of penalties varies greatly in the scheme. A level of proportionality is important in considering the level of appropriate penalties. What is at stake is the conformance of firms to data standards, as noted this is, both domestically and internationally not normally an activity to which regulatory schemes or penalties applies. There is also the potential noted in the Open Banking Regime that the scheme may at some time become redundant.

Yet the proposed penalty regime extends to an uncapped 10% of domestic turnover. For financial firms this would mean fines based on the turnover from non-input taxed activities based on s76(5) of the ACL, which is highly variable and essentially unrelated to the business activity associated with the provision of account information.

Oversize fines do not seem an appropriate level of penalties given the potential offence is in relation to not conforming to a data standard. In contrast, the fines albeit relating to offences by individuals, under the Victorian Criminal Code are capped at $475,710 for matters including rape and manslaughter which are more serious offences.

We also note the recommendation of the Attorney General's Department Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers that "a penalty as a percentage of turnover should generally be avoided because of a lack of connection between an organisation's total turnover and the contravening conduct."

These outsized penalties for larger (based on turnover) firms could also convey a misleading picture to the public of the scale of wrongdoing that is being addressed – a larger firm penalised for more minor misconduct might appear a more important achievement to the casual observer than a smaller firm found guilty of a much more serious offence, which can distort incentives.

Workshop questions

1. Is the list of factors to be considered when designating a sector and making rules (s56AD(1)) an appropriate list of factors? Should the wording of these factors be aligned to reflect similar considerations in any other Act or part of the *Competition and Consumer Act 2010*?

In addition to our concerns noted above around the process for designation and the proper management of the conflicts associated with that process, AFMA is of the view that the Minister should first be required to consider the likelihood of market forces being able to create similar outcomes for consumers without government intervention. This is a principle of good regulation – determine if there is a market failure and if that market failure can be addressed by market forces before considering regulation. For more on this point see the ICSA Principles for Better Regulation.[7] Only then should the type of considerations contemplated in 56AD(1) be reviewed.

The matters required to be considered are limited to the broad form of a cost benefit list, with five matters ((1)(a)(i) to (v)) considering likely benefits to one (matter 1(b)) considering likely costs. This should be more balanced with more specificity around the likely costs. The term 'likely regulatory impact' should be sharpened to include a consideration of the total costs on businesses that would be required to supply the data, all associated compliance and legal costs as well as the relative cost burden for smaller firms, and the additional costs of administration by the regulator.

Critically, it is not just implementation costs that need to be considered. The introduction of new rules or designation of a sector will risk damaging business models. For example, firms that are targeting particular niches of the market might be encouraged into lowest price competition. These developments should not be assumed to increase overall economic efficiency. Niche markets are often where margins are greater and innovation can be more worthwhile, this effect can be seen in a wide range of industries, from automotive to financial products. Moving to an economy where there are fewer niche players might appear to increase efficiency, but experience has shown that while a focus on a smaller range of goods saves development costs the detrimental impact to innovation can hamper competition and create net inefficiencies for the economy.

[7] https://icsa.global/sites/default/files/PrinciplesBetterRegulation.pdf

Once all the costs have been determined, including these economic effects, an assessment should be made as to whether there is a net public benefit by a party such as an accounting firm (or similar) that is independent of the relevant conflicts, based on the costs to business and the public. This analysis should be made public.

2. As drafted, s56AF(1) creates the potential outer-bound of the scope of the definition of CDR data for three different purposes:
   - The scope of what data the right to access and right to data portability could apply to (for data holders and accredited recipients under reciprocity);
   - The scope of what data the ACCC can make rules about; and
   - The scope of what data is protected by the Privacy Safeguards.

   As drafted, s56AF(1) does not separate these purposes within the definition of CDR data. Should CDR data be defined to include derived data for all the above purposes, for some, or for none?

The scope of the definition of CDR data is perhaps the most critical question, sector designation aside, to get right.

AFMA supports the use of separate definitions to define the scope of data with regards to rights to access; regulator rule making; and the privacy safeguards.

The use of a single definition risks making artificially the same what might be best considered separately for these very different purposes. We would be pleased to work with Treasury to create definitions that achieve the appropriate balance, noting that this is not an easy task.

With regard to the exclusion of derived data, this should definitely be excluded from the scope of data for right of access concerns. This is proprietary data and is not appropriate to be included as a consumer right.

3. As drafted, s56AF(4) could include the data holder or accredited recipient in the definition of CDR consumer. How could we best narrow the definition of CDR consumer so that it does not include the data holder or accredited recipient?

AFMA would support an amended definition that excluded data holders and accredited recipients from the definition of consumer, as part of our general recommendation that the definition of consumer be kept in alignment with the definition in the Competition and Consumer Act.

4. We would like the geographical application of this part (s56AH) to be capable of capturing the range of behaviour in respect of data that is captured by the *Competition and Consumer Act*

2010 in respect of the supply of goods and services, [8] and the *Privacy Act 1988* in respect of personal information.

- Does s56AH currently achieve this outcome?
- Do you think the scope of s56AH will lead to unintended consequences?

The drafting of s56AH is very broad and will likely catch a wide range of activities. Section 56AH(3) in particular creates extraterritorial law for CDR data including in relation to "acts, omissions, matter and things". The Government proposes to regulate certain data globally regardless of jurisdiction.

Enforcement as a practical matter is dependent on actions within Australia or international agreements on enforceability elsewhere. The relative strength of claim of an Australian regulatory system's claims of jurisdiction of certain data held by foreign firms on the basis of its one-time connection with some particular data in Australia is worth considering. Data that might originate in the system could circulate through many parties overseas over a long period of time, its status as covered or not would depend on its provenance and the way it left the system. It may be unlikely for these firms to have considered the possibility the data is covered by Australian regulation due to its contact with the CDR scheme at some time in the distant past. Further, there are many jurisdictions that would be highly unlikely to respect Australian law on data within their borders. Actors in these jurisdictions would effectively be outside the restrictions of the scheme.

A more cautious approach might be to limit the extraterritoriality to the data collected by Australian firms, citizens and permanent residents overseas, except where workable treaties are established that give a reasonable expectation that the scheme regulations will apply in practice.

It is likely that the approach proposed in the Draft Bill will lead to unintended consequences. International data vendors may be unwittingly caught by the scheme.

5. Does s56BC(a)adequately provide rule-making powers in respect of the concept of reciprocity? – where the scope of 'equivalent' as recommended by the Open Banking Review is effectively defined as being a designated data-set that may or may not be held by a designated entity.

Reciprocity was promoted under the Open Banking Review as a key justification for the Open Banking scheme. Without a proper reciprocal requirement the scheme risks promoting and requiring a large transfer of information from locally based firms to mostly foreign data companies without anything of value being provided in return to the Australian economy. This could risk disadvantaging Australian firms and would not be consistent with the aims of the scheme.

The Open Banking Review at Recommendation 3.9 argued:

> "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."

---

[8] **See the decision in *Valve Corporation v Australian Competition and Consumer Commission* [2017] 351 ALR 584**

Equivalent data was to include "any customer provided data". The competition regulator was to determine for participants whose industries are not designated in the CDR scheme which data would be equivalent.

A framework needs to be established in the legislation to promote the expectation and provision of a fair reciprocal arrangement. In the Draft Bill s56BC(a) provides no indication that reciprocity is expected to form part of the scheme and was an essential argument in its justification.

As outlined in Open Banking reciprocity should not wait until a sector is designated under the scheme. Before approving a scheme participant the regulator should be required to specify which is 'equivalent data' for that class of participants. This process requirement of the regulator should be specified under the legislation.

We understand from its consultation paper that the consumer regulator does not see it as appropriate to proceed with reciprocity in the first instance as the scheme's focus is on consumer benefit. However, while consumer benefit rightly remains the key focus of the scheme there is a risk that of not balancing the indirect advantages of the scheme to data recipients the scheme will create. As without reciprocity substantial benefits will be indirectly created for mostly global firms, and only costs for Australian firms caught by the scheme.

6. Which Privacy Safeguards need to apply to Data Holders?

- It is our intent that the Privacy Safeguards only apply to Data Holders in respect of the disclosure of CDR data in response to a CDR access request, and to the necessary steps to prepare CDR data for such a disclosure.
- Other than what is required for the disclosure of the data under the CDR, it is not our intent that the Privacy Safeguards should place additional requirements on Data Holders in respect of their normal data storage practices. This includes in relation to Data Holders storage of data they currently hold that falls within the definition of CDR data.
- Are there any Privacy Safeguards where we could narrow the language to achieve this intent and do you have any suggestions on preferred wording?

AFMA would support limiting the additional requirements created by the Privacy Safeguards to not affect normal data storage practices.

AFMA notes the privacy safeguards of the scheme are complex and particularly confusing when an entity is both the data holder and the data provider.

7. For accredited recipients, in respect of CDR data, should the Privacy Safeguards apply in parallel to the Privacy Act, or should the Privacy Safeguards apply instead of the Privacy Act?

AFMA supports the position that for accredited recipients the Privacy Safeguards should apply instead of the Privacy Act. To have a both apply in parallel would further increase the already high level of complexity in complying with the scheme.

8. Are there any Safeguards that should not apply to business information? If not, why not?

By "business information" we understand non-consumer CDR data.

Non-consumer CDR data does not naturally fit in with a 'consumer rights' framework or a consumer privacy framework. If implemented as the Open Banking Report suggests this is business data that the government has mandated to be made public but that is not connected with consumers.

As this is effectively public information not related to individuals none of the Safeguards are sensibly applicable to non-consumer CDR data.

9. The intent of ss56FF, FG, and GB combined is that standards may be either mandatory or voluntary. A standard will be mandatory when adopted by the rules (s56GB) and will therefore have the effect of applying to CDR participants as a multi-lateral contract, as outlined in the Rules. Is this intent clear enough as drafted?

The drafting could be made clearer.

10. Should de-accreditation also be appealable to the Administrative Appeals Tribunal (s56CF)?

Yes.

11. Should a consumer also be able to direct the transfer of data on consents to disclose data to a third party (s56BG(a)). I.e. should data about consents be a designated data set?

Yes, it would appear to make sense for it to be possible for consent data to be directed to be transferred.

12. As drafted s56ER (breach notification) and s56ES (Investigating breaches of privacy safeguards) apply for all CDR consumers data, including the data of large businesses. Should both apply in this way, should one or the other apply in this way, or should neither?

This inconsistency goes back to the broadening of the definition of consumer beyond consumers to include large businesses. We support an appropriate refinement the definition of consumers to address this issue.

13. It is our intent that the individual cause of action provisions (ss82 and 87 of the Competition and Consumer Act) should be class action friendly. Are they?

14. Should the definition of non-economic loss be expanded for the purpose of this section only to include the Privacy Act definition? The Privacy Act definition of non-economic loss or damage includes injury to the person's feelings or humiliation suffered by the person.
    - If so, should this be the case both for the purpose of damages the person can obtain, and for civil penalty provisions (i.e. calculation of penalties up to 3 x loss suffered)?

15. There are currently a range of civil penalty provisions in the Bill. For each civil penalty in the Bill, and for the cap on the civil penalty provisions in the ACCC's rule-making power (s56BJ), are these appropriate levels? Please consider recent changes to penalty provisions in the Australian Consumer Law, and penalty provisions in the GDPR, when providing your answer.

We note our above comments about the penalty regime.

The ACL changes recommended at 3.2.2 in the *ACL Review –Final Report*[9] by Consumer Affairs Australia and New Zealand, formerly the Standing Committee of Officials of Consumer Affairs, sought to increase the maximum financial penalties on the basis that $1.1 million dollar penalties were insufficient for large companies. The arguments given in the final report were limited and appear to be based mainly on the comment by Justice Gordon in *ACCC* v *Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 who said at [105] "The current maximum penalties are arguably inadequate for a corporation the size of Coles".

In the context of the CDR and Open Banking this may not be sufficient reason to create a penalty regime of 10% of non-input taxed turnover per offence for failure to conform to a business-to-business data standard. Appropriate penalty setting takes into account a range of matters beyond the scope of this submission. We note the work done by the Victorian Sentencing Advisory Council in *Maximum Penalties: Principles and Purposes Preliminary Issues Paper*[10].

In relation to the GDPR, Australia is not bound by EU law and the GDPR has received significant criticism for its penalty regime which has often been described as "draconian"[11] for imposing excessive penalties for offences. As such it may not be an appropriate benchmark for consideration by Australian governments.

16. In your opinion, do the provisions dealing with liability (ss56GC, 56EM, and 56EO) reflect liability as outlined in the Open Banking Review?

The provisions appear broadly in line with the liability scheme elements outlined in the Open Banking Review. However, there is a concern that an immaterial breach might remove the protections. We suggest the language include a materiality threshold for the protections to be removed.

[9] https://cdn.tspace.gov.au/uploads/sites/86/2017/04/ACL_Review_Final_Report.pdf
[10] https://www.sentencingcouncil.vic.gov.au/publications/maximum-penalties-principles-and-purposes-preliminary-issues-paper
[11] See for example The National Law Journal - https://www.law.com/nationallawjournal/2018/06/26/the-surprising-news-about-the-gdpr-for-us-law-firms/?slreturn=20180810235058, Forbes https://www.forbes.com/sites/forbestechcouncil/2017/11/13/its-time-to-get-ready-for-strict-new-eu-privacy-regulations/#483fb29456d9 Lawyers Defence Group UK http://www.lawyersdefencegroup.org.uk/gdpr-and-your-firm/

Conclusion

We trust our submission is of assistance and look forward to continuing to engage with Treasury and the regulator in the next stages of the consultation to ensure the best possible outcome for the scheme. Should you require further information on the points raised in this submission please do not hesitate to contact me on (02) 9776 7993 or at djeffree@afma.com.au.

Yours sincerely

Damian Jeffree