12 October 2018

Ms Sarah Court
Australian Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

Email: ACCC-CDR@accc.gov.au

Dear Ms Court

Consumer Data Right Rules Framework

AFMA welcomes the opportunity to provide comments in response to ACCC's *Consumer Data Right Rules Framework* consultation (the Consultation). 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, and that will be directly affected by the Open Banking changes. We also note the potential for parts of the rule making framework proposed to be rolled out to other areas of the economy over time and the subsequent need to ensure the model adopted by the ACCC is optimised.

We have previously provided a submission to Treasury on the Exposure Draft consultation and intend to provide a submission to their *Provisions for Further Consultation* paper that is out for comment.

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. 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 conclusions about the appropriate framework and will confine our comments to refinements around the proposed approach.

In order for the scheme to be successful it is critical that the scheme design is strong and secure so that consumers can have confidence that it will not compromise their information with the risks that entails. There are inherent increases in risk that accompany the distribution of data to more entities, particularly those outside the highly secure ADI environments.

AFMA maintains concerns that the Government's accelerated timetable for release which involves building the standards, rules, and legislative framework all in parallel, while requiring banks to build

systems to comply with these as yet to be finalised framework, standards and rules, and for the Government to build an online secure and reliable directory service by mid-2019 is far from optimal and will increase the risk of insufficiently considered design elements and increased technical risk.

AFMA has also identified some potential market integrity and prudential concerns arising from the sensitive banking data that might be subject to mining.

We welcome the deferral of consideration of the interaction with the scheme with the AML and CTF regimes and raise points in relation to the appropriate integration for a future date.

We outline further concerns in relation to the framework in the paper below and would be pleased to offer further information, clarification or assistance if required.

Yours sincerely

Damian Jeffree

Contents

1. Legislative Framework

While we understand that the Consumer Data Right necessarily needs a significant degree of flexibility given its proposed application to potentially disparate parts of the economy AFMA supports finding an appropriate balance between the legislative, regulatory, and rules layers.

The legislative framework is currently quite limited in the structures that it puts around the rule-making powers. We also understand that while regulations that could provide additional structure for the rule making power and are contemplated in the legislation there are currently no plans to introduce regulations.

AFMA supports getting the balance right between the legislative, regulatory and rules layers. While maximum flexibility in the rule making power may appear attractive as convenient, the scheme legitimacy and success depends on consistent and predictable rule making within a known legislative and regulatory framework. Excessive flexibility increases uncertainty and thereby decreases confidence in parties that are subject to rule changes and this can lead to increased costs.

As such we suggest that ACCC work with Treasury to ensure that the legislation and regulations create a firmer foundation with more structure and limits to the rule making powers than is currently the put forward in Treasury's latest draft.

2. Policy process

While the implementation phase of the scheme is proceeding to a compressed and non-optimal timetable that is likely to increase risks, the policy work behind the Open Banking regime had a more appropriate and structured process. This commenced with the 2014 *Financial System Inquiry*, included the 2015 *Competition Policy Review*, the 2016 *House of Representatives Standing Committee on Economics' Review of the Four Major Banks*, the Productivity Commission's *Data Report* of 2017 and finally and most significantly the *Review into Open Banking: giving customers choice, convenience and confidence* (the Open Banking Review) of 2017.

AFMA made a submission in response to the Open Banking Review noting the risks associated with the proposed timing and scope, the inclusion of wholesale customers, non-market-based price setting arrangements, the need for primacy in relation to security concerns, the potential for the private sector to set standards (as is typical practice in a wide range of areas), and the risks of a 'write' phase amongst other matters. In the event, the Government accepted the report in its totality with only some phasing changes coming out of the consultation.

Notwithstanding ACCC's indication that it intends to treat the Open Banking Review as "a reference point"[1] we are now concerned that the positions of the Open Banking Report do need to be maintained unless there is industry consensus for change.

[1] ACCC, Consumer Rights Rules Framework, p. 8.

There appears in certain areas, notably reciprocity, to be movement away from the recommendations and the principles that informed them. This should only occur with the support of the industry.

3. Cost benefit considerations

While it is appropriate for the ACCC to consider the draft legislations list at 56AD(1) of what it should have regard to when making rules we note that we have suggested in our submission to Treasury that as currently drafted the list may not achieve an appropriate balance between costs and benefits.

Currently the list is detailed on the potential benefits (1)(a)(i) to (1)(a)(v) but only one cost (1)(b). 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. In addition the economic costs of removing niche business models should be considered for the potential wider economic effects.

There needs to be a balanced approach to considering the rule making power and this requires a proper consideration of not just the effect on consumers, but the effect on businesses as well that will bear the costs of the rules, this is the underlying intention of the drafting.

4. General Obligations

As raised in our submission to Treasury we are concerned that the consent-based framework may not address all the relevant issues associated with data mining adequately, particularly in relation to highly sensitive bank transaction data.

Notably in relation to the financial markets we find there are potentially substantial risks associated with statistically significant data samples. In brief, these may provide what might be considered 'inside information' being information that is not generally available that is relevant to the securities of retail facing businesses and other companies that provide consumer services.

In relation to prudential concerns we note that it would be relatively straightforward to construct a 'bank risk' product from a statistically significant sample of transaction accounts associated with a particular bank, drawing from information around late loan repayments and withdrawal activity. In addition to potentially being inside information in times of economic stress, such a product could potentially contribute to systemic instability.

In relation to the risks identified in relation to prudential and systemic matters, we support ACCC and Treasury working with the relevant regulators to ensure these risks are addressed.

We also note our concerns around data leaving the system. Once out of the system the types of risks noted above persist but beyond the system's control. Similarly the control over data that has left the jurisdiction is also substantially reduced if not removed.

The current approach of informed consent and an extraterritorial claim of application appear insufficient to address the risks posed for improper use. This is discussed further later in this submission.

5. Fees

Government fixing of prices in relation to fees introduces market distortions, and as these costs must be recovered elsewhere can risk increasing prices in other areas of the affected firms business. Such an approach does not allow the forces of competition to work as they should in a market economy. AFMA views market competition as the best mechanism for finding the appropriate level for prices within a market economy.

AFMA would support the ACCC adopting a position of supporting competition as the appropriate mechanism by which fees should be determined by firms participating in the scheme rather than the prices being determined by the Government.

Contrary to the claims in the Review the implementation costs will be substantial for all ADIs involved and particularly, in relative terms, for the smaller ADIs. The arguments presented in the review against allowing market pricing are not substantial and in some cases, notably that it could be a cost saving, are speculative at best. The experience of banks so far is that this is a significant and expensive undertaking.

The UK Open Banking regime targeted nine banks, whereas the Australian scheme proposes to capture around 100 ADIs. This larger scope likely increases the costs for the economy and for the included businesses as a group. It is appropriate that if the Government is to mandate involvement in the scheme then it should not mandate that these costs not be recoverable through data fees.

6. CDR Consumer

AFMA opposes the expansion of the definition of consumer for the purposes of the scheme to include entities beyond consumers, with the exception of small businesses, appropriately defined.

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.

It is not at all clear why a large multinational interacting with a much smaller Australian bank needs protection under Australian consumer legislation.

We encourage the ACCC to refine the scope of consumer to allow it to focus its efforts on ensuring consumers in the sense under the Competition and Consumer Act (perhaps expanded to include small business suitably defined) are catered to by Open Banking, and to leave the interactions between large companies to those companies to manage.

7. ADIs

The *compulsory* inclusion of approximately 100 ADIs in the Open Banking program, in contrast to the UK scheme's 9 large banks, will substantially increase risks and costs associated with the scheme and in ways that are potentially economically inefficient.

Notwithstanding this, a number of smaller firms are actively interested in being in the first round in 2019 (or as rescheduled) along with the major banks presumably in order to gain competitive advantage.

AFMA supports the option for any firm to become involved early. However, there are many smaller ADIs that, given their business models and the net costs and benefits to consumers, would prefer for the scheme to be optional. Customers desiring these services would of course be free to switch to providers that provide them.

For consumers, while requiring small providers to provide Open Banking would ensure it was available from their current bank, this bank would have to fund this at the cost of other consumer services and returns to owners, which in the case of customer-owned banking again could negatively impact the consumer.

AFMA holds the scheme should be voluntary for all banks, but early inclusion in the scheme should be open to all ADIs.

8. Phased Implementation

Given the tight timing for the first release of the rules, standards, legislation, and software we again support a delay of the scheme start dates by 12 months. Such a delay would reduce the risk of trade-offs being made to meet the deadline for release and help ensure the security and integrity of those operating in the scheme.

The UK progressed their scheme on a compressed timetable to an unsuccessful launch which damaged the reputation and momentum of the scheme. It is in the interests of the scheme both in the short and long run not to rush the implementation either of the regulatory framework or the software implementation.

9. Data Sets

AFMA welcomes the additional certainty that will come with Treasury's proposals to limit rules relating to consumer CDR data to information in the designation instrument in 56BC, and for non-consumer data the limitation to product information as specified in 56BD.

This will ensure greater clarity of purpose in relation to the regime which was previously lower in predictability.

In relation to the proposal to make 'generic' data available this should only be required where there is already a requirement for the data to be public, consistent with the Open Banking Review and the discussion at page 11 in the Consultation Paper. Further ACCC should ensure that there is a way in the schema of providing information for products that are not amenable to the existing data taxonomy – to ensure that a lack of a specialised data taxonomy for a new type of product does not prevent businesses from releasing those products.

On a broader point we note again that the framing of access to product information in terms of a 'consumer right' is inappropriate and a more appropriate framework should be constructed. This is because this information is intellectual property that by definition does not relate to a consumer and has been created by the firm involved at their expense. It is not appropriate to create a right of consumers to access firm intellectual property to which they have no connection. Notwithstanding that where the consumer is a user of the particular product then it is appropriate for these terms and conditions to be available to them.

10. Derived Data

AFMA supports the restriction put forward in the amended proposals currently under consultation by Treasury that "rules can now only require data holders to allow customers access to derived data that relates to a customer where the derived data is specifically included in a designation instrument" and that "Rules can now only require data holders to provide access to data that does not relate to a customer where that data is about the product".

AFMA has raised concerns with the broad scope for the inclusion of derived data in the draft legislation with Treasury, noting the above limitations now proposed. We support ACCC's general approach of clearly listing the derived data that is to be within scope.

As we have raised with Treasury there is substantial potential for the inclusion of derived data to create an unworkable system for firms that receive Open Banking data. Existing systems may not be capable of ensuring that the rules set for data from scheme can be complied with. This could encourage firms not to use Open Banking data to avoid the risk that it influences other bank data for example the data held in a core banking system and then requires that data to also comply with the Open Banking rule requirements.

11. Anti-money laundering

AFMA welcomes the postponement of AML/CTF considerations to later phases of Open Banking given the appropriate framework has not been created.

We expect that consumers may wish to use Open Banking data to assist banks with AML risk assessments. This might be likely to bring the outcomes of these assessments potentially into the scope of derived data. While this would also be intellectual property and so would need to be considered by the Minister under Treasury's amended proposals there is no guarantee this would be sufficient to keep it excluded. Noting the updated Treasury proposals that would require such information to be listed in the designation instrument we outline some initial thoughts on why AML and CTF assessment results should not be included in the scheme.

AFMA would not support the sharing and the reliance of risk assessments results relating to customers by reporting entities as part of Open Banking. These risk assessment results reflect the risk appetite and risk tolerance unique to an individual institution and thus are not common nor consistent across the industry.

Risk assessments are individual settings that take into consideration a particular reporting entities' customer base, set of designated services provided to their customers and the circumstances in which the services are provided. It is important for entities to assess their own risk and AFMA considers risk assessments as propriety information to the relevant firm. AFMA does not believes that either risk methodology underpinning an assessment nor the results of any assessment should be made public (given the risk they may be able to re-engineered in order to uncover the assessment framework) and therefore be used to evade detection.

Further from the above concerns, if the AML/CTF Framework (that is currently underpinned by a risk-based approach by each reporting entity) was to be adjusted to allow for the sharing of the outcome of each customer's risk assessment and reliance was allowed, it would effectively mean that each data recipient would be accepting the risk assessment of the data provider regardless of their own risk appetite and tolerance. This could lead to situations where open banking participants would either need to agree on a standardised approach or could find themselves in positions where their risk appetite and tolerance did not match the potential new customers that were facilitated through Open Banking. It is not yet clear how the risk-based approach that underpins the AML/CTF Regime could apply in a situation where a standardised approach was agreed and followed, lending itself to a level of prescription.

Alternatively there are other opportunities that Open Banking may bring to AML/CTF. Potentially the sharing of transactional data would allow AUSTRAC access to transaction monitoring across the banking industry and also to other 'regtech' entities. This would allow insight on common industry wide scenarios and may also assist with transparency. There would also be the potential to allow for recipients of transactional data to pre-filter out customers that may pose additional risk based on access to their transactional data. This may even allow (over time) for AUSTRAC to revise its transaction monitoring requirements and may be able to assist involved reporting entities to reduce or redirect part of their cost base.

In in a similar vein, there may be opportunities for new participants to offer value-added services such as customer identification procedures (CIP) as a viable outsourcing partner to industry, by having the ability to access large volumes of customer profiles (at customer's discretion) and being able to cross-reference independent data sources to provide an efficient identification profile that could be relied on. This has the ability (if executed well) to lower the cost base of reporting entities and delivering efficiencies to customers as they elect multiple financial services provider's products.

To enable this type of functionality OAIC & the ACCC may have to consider its stance on sharing of unique identifiers (such as passport, Medicare numbers etc.) as these are often used to verify customer information on independent government databases.

AUSTRAC should consider a customer's consent of sharing information as part of Open Banking and how that may satisfy a reporting entities obligation to collect personal information from the customer when undertaking discrepancy management or a OCCD/KYC Refresh of a customer's profile. There may be benefits to a reporting entity's cost base by allowing the reliance on information shared under open banking to be considered as obtaining personal information from the customer.

12. Reciprocity

Without discussing the merits of the particular definitions proposed by Treasury AFMA welcomes the amended Treasury proposals to highlight the policy principle of reciprocity on which sections of the Bill are based.

We disagree with ACCC's claim at page 21 of the Consultation ("this was not a condition of the data sharing obligation") that the policy position of the Open Banking Review did not formally recommend a requirement for the ACCC to determine 'equivalent' data and that entities participating be required to share this data if requested by the consumer. We read Recommendation 3.9 as clearly requiring the sharing of this data and anticipating the ACCC having determined what this 'equivalent' data should be.

Reciprocity is designed to address the imbalance in indirect advantage that a scheme without this design element would have. Specifically, without a reciprocity arrangement data would (at the customer's request) flow only from Australian ADIs to potentially largely foreign data companies. This indirect effect of the scheme could create a net negative impact for the Australian economy.

Reciprocity is a design element that is intended to go some way to address this imbalance by requiring those beneficiaries to be required to share data in the reverse direction if so requested by the consumer. While the CDR is framed in consumer terms, it will have extensive impacts on the economy and indirect effects and it is important that these are not to the net detriment of Australian businesses.

We do agree that reciprocity does raise complex issues, but it is appropriate that these be addressed as a matter of priority lest the balance in the design of the scheme is upset.

We understand that ACCC has indicated that it "will always take the consumer perspective"[2], however, as noted we would support ACCC taking a balanced approach to the costs and benefits of the scheme. The costs of the scheme are at this point real and the benefits still only potential. It is appropriate for ACCC to evenly consider the consumer benefits with the costs to business, including the competitive disadvantages created by the scheme and that are sought to be addressed by reciprocity, in a manner that supports competition as the driver of pricing and efficiency in its work on Open Banking and the Consumer Data Right more generally. Not to do so will risk inefficient and unbalanced outcomes.

13. Accreditation

AFMA supports a single robust threshold for participation in Open Banking in the first instance. While we understand there is interest from the fintech community in having lower standards available for certain applications we caution against that at this time, noting that the key to success for the scheme is the successful implementation of a security regime and the associated public trust that will come with this.

For data receiving firms to successfully implement the required security schemes is a significant undertaking and will require significant organisational resources. A compromise of the firm's internal systems, of its third party suppliers, or its complex internet connectivity infrastructure could be sufficient to compromise data security.

For reasonable levels of assurance around the implementation of security data receivers (and data holders) will have to implement a substantial stack of security features and practices. These include:

- API security;
    - The OAUTH 2.0 authorisation framework;
    - JSON security;
    - Credentials management;
    - Keys management;
- Customer authentication standards;
- Customer consent management;
- Customer fraud detection;
- Network security for their network including firewalls;
- Third party application vetting and security;
- Penetration testing;
- Assurance, vetting and tracking of third party suppliers and supply chains;
- Privileged access management – this includes tracking of staff joiners, mover and leavers and security access around this;
- Information security and development requirements being embedded into the development lifecycle;
- Cybersecurity function;
    - Strong Firewall defences
    - Vulnerability and Threat management
    - Antivirus and malware protection

[2] ACCC Workshop Sydney 25 September.

    - Denial of Service (DoS) or Distributed Denial of Service (DDoS) protection
    - Patch management
    - Email filtering
    - Web filtering
    - Administration privileges
    - Access control
    - Intelligence and information sharing
    - ISO27032:2012 accreditation alongside ISO27001:2013;
- Adequate security and application testing including:
    - Integration testing;
    - Conformance testing; and
    - Regression testing.

If a data receiver fails to properly implement any element of the required security infrastructure such as one of those listed above this will increase the vulnerability of its customers to data theft, privacy breaches and fraud. If and when Open Banking proceeds to a 'write' phase as envisaged in the Open Banking Review this would also include the risk of monetary theft due to any of these failures.

It is difficult to assess the level of risk that entails to consumers and the economy if a substantial number of firms of various sizes are required to diligently implement and stay up to date with the latest security developments in the areas listed above. However, we do note that the risks and challenges above suggest support for the case for requiring a robust accreditation standard for data receivers.

14. Consent

We support the proposal to make rules prohibiting the on-selling of data and the use of CDR data for direct marketing. These will likely reduce the risks of misuse of data. It may be beneficial to clarify whether the use of Open Banking data for political purposes would count as direct marketing for the purpose of the rules, as the transaction data may identify or suggest political preferences and political uses are subject to exemptions to the Privacy Act.

As noted in the General Obligations section above, AFMA is concerned about the potential for leakage of data out of the system and for the use of statistically significant data samples in relation to market sensitive information and prudential risk. We do not believe the consent framework is sufficient to address these risks. We support the ACCC working with the relevant regulators and industry to address these issues.

These risks are increased by the proposal to allow data to go to recipients outside of the regime outside of the jurisdiction. We believe the case for allowing data to go to unaccredited parties has yet to be made.

The proposal to allow data to go to parties outside the scheme and jurisdiction seems at odds with the rest of the scheme design. The data that could go to these parties is or is informed by *the exact same data* held and shared by data holders in the scheme. The accreditation requirements for data

receivers and penalties for data holders to allow data to go to a non-accredited firm are there to protect this very same data. We do not understand why data receivers should be able at the customer's request to send the data to any non-participating recipient in any jurisdiction (except for direct marketing or on-selling purposes) when this same data was so protected when it was in the possession of the data holders. This could not be because data holders are less trustworthy than data receivers, as data holders in the Open Banking context are all ADIs.

We note that some jurisdictions do not have rule-of-law and have regimes that are potentially hostile to the aims of the scheme.

For the success and security of the scheme this part of the design needs substantial work.

15. Authorisation and authentication process

The proposals in relation to limiting the security and checking that banks can do before providing information to third parties in Open Banking are at odds with the general direction of security policy relating to ADIs in other areas of Government policy. For example the new APRA security standard is about ensuring minimum standards in relation to information security threats.

The proposed rule that would restrict ADIs from having additional requirements in the authorisation process beyond those required by the standard. Standards become out-of-date and require time to bring up to meet new threats.

The inability of ADIs that have become uncomfortable with the adequacy of a standard to add additional verification requirements under the proposed approach could create unfair outcomes in the event that a deficiency in the standard results in an adverse outcome for a consumer. That is, it is not fair for ADIs to be liable if the rules require them to take risks by having a security standard lower than that with which they are comfortable and this approved/required standard is insufficient results in a loss.

AFMA supports Government action to ensure minimum standards of security across the scheme, but these should be minimum standards that firms are free to exceed to ensure they are comfortable with their risk levels and so that consumers are protected.

16. Making generic product data generally available

The Open Banking Review suggested that where firms are under an existing obligation to disclose information on their products or services then this should be made available under an Open Banking protocol.

Firms in a market economy should generally be at liberty to decide in what form they make their intellectual property, including that relating to pricing and features, public. Also the provision of data that does not relate to a particular customer does not fit naturally into a 'consumer data right'

framework. As such it may be appropriate to allow firms the manner in which they make the required disclosures of product data.

17. Use of data

With regard to the proposed requirement on data recipients to transfer data out of the system at the request of consumers, we caution this could potentially facilitate large amounts of sensitive consumer data with statistically significant market and potentially prudentially sensitive information leaving the jurisdiction.

We suggest ACCC reconsiders this proposal particularly in the initial phase of the scheme where all parties are gaining experience in the risks of a data economy. The reactive approach to managing risks in this regard outlined by ACCC at page 28 “additional use restrictions or regulation can be imposed if this becomes necessary” may be ill-advised.

As the ACCC acknowledges the risks of data breaches can increase in line with greater access to data.

The justification that “A balance must be stuck [*sic*] between the protections provided for within the system and its ultimate usefulness” may be premature at this time before the scheme has commenced. An incremental approach where some benefits are realised early on and consideration is given to incremental extension of the scheme would appear to be a better balanced approach to managing these risks.

If data recipients can be directed consumers to send data to non-accredited parties it would seem logical that similar requests could be made of data holders. It is unclear why such requests should not be allowable except that they would make all the protections of the scheme irrelevant. Why should a bank not be able to direct data through the Open Banking scheme to the ATO if so requested by a consumer when a data receiver can?

This *reductio ad absurdum* would suggest that data recipients should not be able to have data directed out of the system.

18. Data Standards Body

We query the proposal to skip the normal consultation processes in relation to changes to standards. This is not compatible with how standards typically work and we would encourage ACCC to consider the more typical practices around standards.

Standards are not usually used to implement rapid changes to required practice. These would typically be done in the field with the flexibility that is normally available to firms operating in a competitive market economy.

The idea that a change to a standard should then result in an immediate effect in firms complying to the standard does not accord with the typical notice periods and transitional arrangements that accompany changes to standards. We suggest ACCC keep changes to standards within the standard

consultation arrangements that accompany standards and ensure the rules have sufficient flexibility to allow firms to update practices as required between changes to the standard.

We also reiterate our suggestion to previous consultations that the Government and ACCC plan and set in motion a plan to return the standards setting function to the private sector. There has been support suggested for this approach by the Government but we do not see any evidence of planning for this eventuality in the current paper.