10 May 2019

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 Exposure Draft

AFMA welcomes the opportunity to provide comments in response to ACCC's *Consumer Data Right Rules Exposure Draft* 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 have previously provided submissions to Treasury on the Legislative Exposure Draft and Provisions for Further Consultation paper and to ACCC on the Rules Framework.

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.

Consistent with our submissions to the policy processes around the Consumer Data Right, 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. However, we accept the Government's conclusions about the appropriate framework and will not repeat our positions in this submission and instead will confine our comments to refinements around the proposed approach with particular regard to the security framework.

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. It is also important that there is consistency in regulatory requirements for system security across the financial sector.

Consistent regulatory frameworks

Regulatory standards can help bring greater consistency to business practices. While Australia's financial firms have developed sophisticated defences against information security risks over many decades, given the benefits of greater consistency for the system as a whole in the context of the increased threat environment of more recent years, there is support for APRA's recent prudential standard on information security CPS 234. This is a well-developed, high-level, principles-based standard complemented by extensive guidance in the currently draft Guidance CPG 234.

Industry has also been supportive of the Australian Cyber Security Centre's various standards, advisories, and maturity models, which, on a voluntary basis, have assisted firms prepare and respond to the increasing challenges in cyber security. ACSC has adopted a productive and helpful partnership approach to addressing information security risks which have very much been appreciated by industry.

Over the past five years in particular ASIC has significantly increased its level of activity in relation to cyber resilience including cyber security. Its initiatives have included Report 429 released in early 2015 Cyber resilience health-check which increased awareness of cyber threats, directed businesses to resources such as NIST, and alerted market participants to their regulatory requirements in relation to cyber security. ASIC work has also established understandings of resilience in market operators, market participants and the top 100 listed entities.

Infrastructure providers also contribute to the information security requirements landscape. Currently ASX is consulting on updates to its Guidance Note 10 on cyber resilience which is relevant to clearing and settlement participants in its various markets. While requiring firms to adhere to a global or national cyber resilience standard ASX proposes to maintain flexibility as to which standard firms choose to align themselves.

The work of these government bodies, regulators and private infrastructure providers has been complementary and has not resulted in excessive overlap in obligations. AFMA is keen for this type of coordinated approach to continue.

Application of Schedule 1 Part 1 to ADIs

In the Consumer Data Right Rules the Commission proposes wording for Schedule 1 Part 1 that while inspired by CPS 234 creates a new, different and for ADIs participating in the scheme as accredited data recipients, parallel regime for accredited data recipients in the CDR. There are some parallels here in the approach the Commission has taken to privacy standards where the Commission has developed its own unique standard that has crossovers with, and extensions beyond, the existing national scheme.

It is important that the Commission's processes produce policies that coherently integrate with the broader government policy landscape.

While the Consumer Data Right will be applied more generally to other sectors in the economy, for Open Banking ADI entities when undertaking CDR data receipt activities will all be subject in parallel to the requirements of CDR. This is an undesirable outcome from a regulatory perspective. The same controls will have to be assessed by ADIs under these two parallel and different regulatory regimes.

AFMA would support coordination of regulatory information security initiatives to avoid this outcome. We suggest the Council of Financial Regulators Cyber Security Working Group be used to build on the leading work undertaken by APRA in CPS 234 and coordinate a single unified information security standard for financial services firms.

It makes little sense either logically or practically to have different cyber security framework standards for a single sector particularly for the same activities. APRA regulated firms should be excluded from the requirements around information security listed in Schedule 1 Part 1 given they are already covered in the APRA regulations. This could be structured as recognition by the Commission of the APRA regulations for the purposes of complying with the CDR scheme.

It would be inappropriate for ACCC not to recognise the security afforded by the APRA CPS 234 standard. If ACCC has identified inadequacies in the standard then these should be raised through the CFR Working Group for amendment.

Application of Schedule 1 Part 1 to non-ADIs

The security of the Open Banking scheme as a whole depends on consistently high standards of security across all participants.

The security of personal and identity information associated with accounts will be limited to the security of data recipients under the scheme. Compromised security of this type of information could be damaging to the scheme. If and when the scheme moves to a 'write phase' as contemplated in the Farrell Report the security of consumers' assets will be limited to the security of the accredited data recipient that the customer has authorised to access and transfer money on their behalf (we discuss later the undesirability of a separate category being introduced for this activity).

It is therefore appropriate to require consistent ADI levels of security from accredited data recipients under the Open Banking part of the Consumer Data Right scheme.

As we have noted in previous submissions while this is a challenging prospect for the firms involved it is in the long term interests of consumers, participating ADIs and the scheme itself.

Schedule 1 Part 2

Schedule 1 Part 2 lists minimum requirements for the security of CDR data held by accredited data recipients.

For ADIs these requirements are relatively brief compared to the comprehensive draft guidance relevant to CPS 234 in CPG 234 that is currently out for consultation. We view the APRA framework

for ADI security as sound and likely to be effective for ADIs participating in the scheme as accredited data recipients (in addition to their responsibilities as data holders).

As with Schedule 1 Part 1 and CPS 234 if ACCC has identified weaknesses in APRA's CPG 234 framework for ADI information security then it is appropriate that these are taken up with APRA directly rather than by creating a duplicate scheme to be applied to the same activities. ADIs subject to APRA's regime should be excluded from these requirements given they are already covered by the APRA regulations.

For non-ADIs participating in the scheme it is appropriate to create a consistent ADI level of security, particularly in the context of a scheme that contemplates moving to a write phase at a later time. In this context *it is not clear that the abbreviated list in Schedule 1 Part 2 will be sufficient to meet this objective*.

It may therefore be appropriate to adopt CPG 234 for all accredited data recipients[1].

A single standard should be required for all participants in the Open Banking part of the scheme for the long term stability and security of the scheme as a whole.

We would recommend against having multiple levels of security for different participants in the scheme as might be contemplated.

Such an approach could lead to confusion amongst consumers and failures at the lower end of security could bring discredit to the broader scheme. For example if 'read-only' data recipient firms were to require a lower level of security to 'write phase' data recipient firms which were lower than ADI data holder's level of security, it is unclear whether a failure in a 'read only' firm's security would be understood by consumers as not having a bearing on 'write phase' or even ADI security. The credibility and trust in the entire scheme (and potentially the broader prudential environment) could be at risk of compromise.

Specific queries

In the event APRA decides to proceed with the proposed arrangements AFMA seeks more information on the formal controls assessment program that would be required to conform to Rule 7.8.

We also ask for clarification in the context of Schedule 1.6.3 of the definition of the term "senior management" in the context of ADIs which are branches and may not have a local board.

We seek clarification that the independence of the testers required in Schedule 1.6.4. is similar to the expectations of APRA in CP 234 around functional independence.

[1] Note that some changes in drafting would be required – for example the standard refers to APRA regulated entities.

In relation to the requirements under 8.11 for the Data Standards Chair and Committee to formulate data standards it may be appropriate to require that consideration is given to using existing industry standards where available and appropriate.

Conclusion

We trust our comments are of assistance in finalising the scheme rules. Should you wish more information please do not hesitate to contact me on [redacted] or [redacted].

Yours sincerely

Damian Jeffree
Director of Policy