10 May 2019

Mr Bruce Cooper
General Manager
Consumer Data Right Branch
Australian Competition & Consumer Commission
23 Marcus Clarke Street
CANBERRA ACT 2601

Email: ACCC-CDR@accc.gov.au

Dear Mr Cooper

Consumer Data Right Draft Rules Consultation

The Customer Owned Banking Association (COBA) appreciates the opportunity to comment on the ACCC's Draft Consumer Data Right Rules (Draft Rules).

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $118 billion in assets, 10 per cent of the household deposits market and 4 million customers. Customer owned banking institutions account for around three quarters of the total number of Authorised Deposit-taking Institutions (ADIs) operating in Australia that will be mandated to participate in Open Banking as data holders.

COBA is a significant stakeholder in Open Banking. We are pleased that the ACCC is consulting on the Draft Rules, given the complex nature of the reform and the critical need for the final CDR rules to be appropriately designed to support industry solutions for Open Banking to help drive innovation and competition in Australia's banking sector.

COBA continues to strongly support Open Banking as it presents an excellent opportunity for our sector to further enhance how we deliver value to our customers. ADIs with excellent customer service and highly competitive pricing, like customer owned banking institutions, stand to gain from Open Banking, as do the customers themselves.

However, COBA notes that the enabling legislation, the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (the Bill), remains before the House of Representatives. The ongoing absence of a legal framework has created a high level of uncertainty for industry.

Further fuelling the level of uncertainty, diverse stakeholder positions were put to the recent Senate Inquiry into the Bill conducted by the Senate Economics Legislation Committee. COBA and other key stakeholders like the ACCC made a submission and/or appeared as witnesses at public hearings of the Inquiry.

COBA appreciated the views expressed by the ACCC at the public hearing in Melbourne, particularly its view that the CDR will be "facilitating and enhancing the capacity of others to compete" and that the

ACCC's experience has been that "some smaller, niche and maverick-type players in any market, including the financial market, are the ones that can sometimes provide the biggest competitive spur"[1].

With that being said, we note from the Report[2] of the Senate Inquiry the concerns raised by some stakeholders with the Bill, including from some Senate Committee members, and calls by some of those stakeholders for material changes to be made to the Bill, particularly in relation to privacy protections.

As the ACCC is aware, COBA's view is that the Bill is framework legislation that would enable the CDR to be applied to a range of different industry sectors, and that any identified gaps in the privacy protections in the Bill, for example, should be addressed by the ACCC and/or Data61, the Data Standards Body for the CDR regime. In this respect, COBA's submission to the Senate Inquiry and public testimony in Sydney strongly supported the passage of the Bill through Parliament.

To the extent that further changes are made to the Bill before it becomes law, our view is that this may have a material flow-on effect to the Draft Rules which would likely trigger the need for the ACCC to consult on a revised version of the Draft Rules. Our view is that the stakeholder concerns canvassed in the Report of the Senate Inquiry appear to suggest that further amendments to the Bill are likely.

COBA recognises the intent of the Draft Rules and notes that the ACCC's positions set out in the draft appear broadly consistent with the ACCC's corrected version of the CDR Rules Outline, which was released by the ACCC on 25 January this year.

However, COBA is concerned with the approach taken to drafting and is also concerned with a number of specific aspects of the Draft CDR Rules, particularly Schedule 1—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients. The following sections outline our concerns.

Drafting approach and impact on implementation

COBA is concerned that the Draft Rules lack a sufficient level of detail to facilitate industry implementation. The Draft Rules appear to be more similar, in both language and structure, to a legislative bill rather than rules that determine how the provisions of the Bill would be implemented.

For example, the following sections of the Draft Rules adopt high-level language, such as "reasonable" and "timely" (as emphasised in bold below), which would be open to interpretation and create implementation uncertainty for industry:

a. 1.12 Consumer data request service (4)(a): "allow a request to be made in a manner that is **no less timely**, efficient and convenient than the online services that are ordinarily used by customers of the data holder to deal with the data holder;"

b. 1.8 Meaning of CDR contract (3)(c): "the consumer will have the option to terminate the CDR contract within a **reasonable period**, that is specified in the contract, after the withdrawals."

c. 3.5 Refusal to disclose in response to consumer data request (1): "A data holder that has received a valid consumer data request made under this Part may refuse to disclose CDR data in response to the request if it has **reasonable grounds** to believe that the disclosure would:"

d. 5.15 Revocation of accreditation—process (1)(b): "give the accredited person a **reasonable opportunity** to be heard in relation to the proposed revocation."

e. 5.17 General process for suspension of accreditation or extension of suspension (2)(b): "give the accredited person a **reasonable opportunity** to be heard in relation to the proposed suspension or extension."

f. 5.18 Process for urgent suspensions or extensions (3)(b): "give the accredited person a **reasonable opportunity** to be heard in relation to whether the suspension should be removed."

g. 5.9 Conditions on accreditation (2)(b): "give the accreditation applicant or accredited person, as appropriate, a **reasonable opportunity** to be heard in relation to the proposal."

[1] ACCC witness appearance at the Public Hearing on 5 March 2019 in Melbourne.

[2] Senate Economics Legislation Committee Report: Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Provisions].

h. 1.7 Step 5—Manage and report security incidents (1): "An accredited data recipient must have procedures and practices in place to detect, record, and respond to information security incidents in a **timely manner**."

    i. COBA notes that the term "timely" is used a number of times in Schedule 1 covering information security requirements for CDR data held by accredited data recipients. The broader issue of information security requirements is covered in detail further below.

As the ACCC would appreciate, the absence of a sufficiently detailed CDR Rules framework means that implementation of Open Banking becomes an even more challenging process. Detailed CDR Rules are not only important from an entity-level implementation perspective, but also from a whole-of-sector consistency perspective; the latter of which may benefit the ACCC and OAIC's future audit activities.

A clear CDR Rules framework is required to assist in directing resources and mitigate against the risk of inadvertently proceeding down a misinterpreted/incorrect path, which could be costly to unwind. As smaller ADIs, our members' resources for Open Banking implementation are more limited, compared to the larger banks for example, and therefore need to be more carefully managed.

While the customer owned banking sector has set aside a significant amount of resources and time towards implementation with positive progress being made already, it would be important for the ACCC's final CDR Rules to help build on this progress by providing a sufficient level of detail. Otherwise, there would be a material risk that implementation does not align with the ACCC's intent.

Security of CDR data held by accredited data recipients

As COBA also emphasised in its submission[3] to the ACCC on the CDR Rules Framework, a strong information security framework is a necessity of Open Banking, as this will help assure the level of consumer trust that is crucial to its success and the success of the CDR regime more broadly.

We recognise that the expected growth of third parties in the provision of financial services, through Open Banking, may see an increase in financial crime (such as online fraud) if the information security framework applying to accredited data recipients was poorly designed.

COBA recognises that information security is central to the CDR accreditation process and that the quality of an accredited data recipient's information security framework will have a significant influence on its ability to receive accreditation from the ACCC. In this respect, we appreciate how the ACCC has recognised the importance of this matter by separately setting out the requirements at Schedule 1.

As the ACCC knows, APRA released in November last year the final version of the new cross-industry prudential standard for the management of information security risks.

APRA's new Prudential Standard CPS 234 Information Security (CPS 234) sets out minimum requirements for the management of information security and will be complemented by a revised prudential practice guide CPG 234 Information Security (CPG 234) to support implementation. CPS 234 commences 1 July 2019 and applies to all APRA-regulated entities including, for example, ADIs.

COBA's view is that the requirements in Schedule 1 appear to be based on APRA's CPS 234 and Draft CPG 234 (the latter of which APRA is publicly consulting on). To provide some examples, set out below are some of the proposals in Schedule 1 on information security capability, governance and policy and controls assessment, compared against similar requirements in APRA's CPS 234.

a. Information security capability

    i. *Schedule 1*: Under 1.2 Interpretation

    "information security capability, of an accredited data recipient:

    (a) means the accredited data recipient's ability to manage the security of its CDR data environment in practice through the implementation and operation of processes and controls; and

[3] COBA's submission to the ACCC of 12 October 2018, refers (page 9).

(b) includes the accredited data recipient being able to allocate adequate budget and resources, and provide for management oversight."

ii. *CPS 234*: paragraphs 15, 16 and 17

"15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.

17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment."

b. Information security governance/policy framework and review

i. *Schedule 1*: Under 1.3 Step 1—Define and implement security governance in relation to CDR data

"(1) An accredited data recipient of CDR data must establish a formal governance framework (that is, the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security) for managing information security risks relating to CDR data.

(2) The accredited data recipient must clearly document its practices and procedures relating to information security and management of CDR data, including the specific responsibilities of senior management.

(3) The accredited data recipient must have and maintain an information security policy that details:

(a) its information security risk posture (that is, the exposure and potential for harm to the accredited data recipient's information assets, including CDR data that it holds, from security threats); and

(b) how its information security practices and procedures, and its security controls, are designed, implemented and operated to mitigate those risks.

(4) The accredited data recipient must review and update the framework for appropriateness:

(a) in response to material changes to both the extent and nature of threats to its CDR data environment and its operating environment; or

(b) where no such material changes occur—at least annually."

ii. *CPS 234*: paragraphs 18, 19, 26 and 32

"18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.

26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.

32. An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance)."

c. Formal controls assessment program

i. *Schedule 1*: Under 1.6 Step 4—Implement a formal controls assessment program

"(1) An accredited data recipient must review and assess the effectiveness of its information security capability and controls relevant to its CDR data environment by establishing a formal controls testing program. The extent and frequency of this testing should be commensurate with:

(a) the rate at which vulnerabilities and threats change; and

(b) material changes to the boundaries of its CDR data environment; and

(c) the likelihood of failure of controls having regard to the results of previous testing; and

(d) the risks associated with exposure to external environments where the accredited data recipient is or may be unable to enforce its information security policies."

ii. *CPS 234*: paragraph 27

"27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:

(a) the rate at which the vulnerabilities and threats change;

(b) the criticality and sensitivity of the information asset;

(c) the consequences of an information security incident;

(d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and;

(e) the materiality and frequency of change to information assets."

For ADIs seeking accreditation as data recipients, the proposed requirements set out in Schedule 1 and APRA's CPS 234 would unnecessarily operate as dual information security frameworks with comparable requirements targeting similar regulatory outcomes.

ADIs presently hold data within scope of Open Banking and are obligated to manage the associated privacy and information security risks under numerous legislative frameworks, such as the *Privacy Act 1988* and APRA's CPS 220 Risk Management (covering all material risks), for example. APRA's CPS 234 will strengthen those frameworks by introducing a bespoke information security prudential standard.

In this regard, the ACCC's rationale to impose the Schedule 1 requirements on ADIs seeking accreditation as data recipients, and the potential benefits from this proposal, are not clear.

COBA considers that it would be appropriate for the ACCC to permit substituted compliance for ADIs with respect to Schedule 1 by providing that the Schedule 1 requirements do not apply to ADIs seeking accreditation where an ADI is required to comply with APRA's CPS 234.

Furthermore, COBA would like to provide feedback to the ACCC on a number of specific aspects of the information security requirements in Parts 1 and 2 of Schedule 1, particularly the concept of a CDR data environment (Part 1) and some of the ACCC's proposed minimum information security controls (Part 2).

a. Part 1 appears to be based on CPS 234. The ACCC's concept of a CDR data environment appears to be similar to the Payment Card Industry Data Security Standard Cardholder Data Environment. We would appreciate further clarity on the scope of the CDR data environment – for example, is it just the externally exposed API integration layer and related infrastructure?

b. Part 2 appears to be based on APRA's Draft CPG 234.

   i. In relation to the ACCC's proposed audit logging and monitoring controls, we note that the period of retention of records is "6 years beginning on the day the record was created". COBA emphasises that the storage requirements from this proposal would be material and have a significant cost impact. As a comparison, the Payment Card Industry Data Security Standard requirement imposes a retention period of 1 year.

   ii. In relation to the proposed password authentication controls, we would appreciate clarity from the ACCC on whether 'service accounts' would be included.

   iii. On the proposed encryption controls, we would appreciate clarification on what is intended to be captured under "CDR data at rest". If "CDR data at rest" also captures core banking systems, for example, this may be extremely difficult (if not impossible) to implement for ADIs with legacy banking systems.

   iv. With respect to the end user devices proposals, our view is that it would be very challenging to harden bring-your-own-device (BYOD) systems, particularly as these are not owned or managed by an accredited data recipient.

   v. On the proposed security patching controls, we note that "extreme risk" vulnerabilities would need to be targeted for patching within 48 hours of identification. Given the time needed for security patch testing, this would be unrealistic, and we would suggest a 2-week timeframe from identification.

   vi. With respect to the proposed controls around securing CDR data in non-production environments, we would appreciate clarity from the ACCC on what is intended with "masking data".

   vii. In relation to the scope of the proposed application whitelisting controls, our view is that BYOD devices should be removed as these are not owned or managed by an accredited data recipient.

On balance, the ongoing uncertainty in the operating environment, coupled with the potential work involved to progress the Draft Rules to a final version, places at serious risk the *revised* rollout schedule for Open Banking that was announced[4] by the Government in late December last year.

Should no further material progress be made this financial year, particularly in relation to the Bill, COBA would strongly encourage the ACCC to examine the impact that this would have on the ability for industry to implement Open Banking by the announced dates in the revised rollout schedule. Our view is that this scenario would justify a second change to the timeframes in the revised rollout schedule.

As the ACCC would be aware, a significant number of COBA members rely heavily on third-party service providers for their core banking system and information technology service requirements. In this respect, it is important that our members are provided 'reform certainty' so that they are able to engage and negotiate confidently with their third-party service providers on implementing Open Banking.

On a related matter, COBA notes from the ACCC's corrected version of its CDR Rules Outline[5] that the "ACCC may grant a data holder a temporary exemption from obligations under the Rules, where the ACCC considers it appropriate to do so".

While it appears that this ACCC exemption power is captured under section 56GD of the Bill, 'Exemptions by the Commission', COBA would appreciate this mechanism being explicitly included in the CDR Rules for Open Banking. We suggest that this is incorporated in the CDR Rules at Schedule 2 – Provisions relevant to the banking sector.

[4] The Commonwealth Treasurer's media release of 21 December 2018, refers.

[5] On 25 January 2019, a corrected version of the CDR Rules Outline was published by the ACCC.

As we emphasised in our submission to the ACCC last year[6], in advocating for this exemption mechanism, some of our members are facing particular challenges with implementing Open Banking by the timeframes and would require more time due to resourcing constraints and to avoid unnecessarily burdensome and redundant costs. We explained to the ACCC in that submission that some of our members are in the process of implementing major changes to their information and data systems (software and infrastructure overhauls to replace outdated systems).

For those members, their circumstances have not changed and implementation by the revised time frames would still require legacy systems to be reconfigured to accommodate Open Banking, while work is performed to determine how Open Banking should be implemented across their new systems.

This means that those ADIs would need to operate two systems simultaneously, before closing their legacy systems down at a later stage than initially planned. In this respect, members' significant expenditure to upgrade legacy systems for Open Banking would then be redundant.

Finally, COBA would also like to reiterate that mutual ADIs do not have the scale of information security resources compared to larger ADIs. Unnecessarily onerous accreditation requirements would inadvertently disadvantage mutual ADIs and further exacerbate the competitive imbalance between mutual ADIs and larger ADIs. As the ACCC would appreciate, this scenario would work against the competition and consumer policy objectives of Open Banking and the CDR reform more broadly.

COBA looks forward to continuing to work with the ACCC to progress the CDR Rules for Open Banking to help facilitate a smooth and efficient transition to the new system. In the interim, if you have any questions or comments in relation to any aspect of our submission, please do not hesitate to contact Tommy Kiang, Senior Policy Manager, on [redacted] or at [redacted].

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer

[6] COBA's submission to the ACCC of 12 October 2018, refers (page 2).