Australian Banking Association

09 May 2019

Mr Bruce Cooper
General Manager
Consumer Data Right Branch
Australian Competition and Consumer Commission

By email: ACCC-CDR@accc.gov.au

Dear Mr Cooper

Competition and Consumer (Consumer Data) Rules 2019 – Exposure Draft

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on the exposure draft *Competition and Consumer (Consumer Data) Rules 2019* (**draft Rules**).

With the active participation of its members, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and community, and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA and its members have appreciated the consultative approach the ACCC has taken in developing the rules. The draft Rules are a critical component of the CDR, given its central role in establishing the framework for the transfer of banking data, and from our perspective provides a good foundation for the implementation of open banking. However, there are a number of areas that have not been addressed in the draft Rules or which require further guidance.

With the simultaneous drafting of the legislation, rules and data standards, it has been a challenge to ensure that there is perfect alignment between these various parts. Our submission identifies areas where there are gaps or misalignment between the legislation[1], draft Rules and proposed data standards. Ensuring that the law, rules and standards are consistent and provide sufficient regulatory certainty should be the key priority before the commencement of open banking.

The ABA understands that guidance material will be developed to supplement the rules in providing clarity to participants on how the ACCC intends to enforce the regime. Many of the issues raised in our submission could be addressed by way of guidance and we look forward to engaging with the ACCC on this further work, as well as key issues not yet resolved in the draft Rules including rules around civil penalties attached to the application of the CDR in the banking sector.

1. Key issues

1.1 Policy certainty in the rules

It is important that key parameters of the regime are defined clearly in the legislation and rules. This includes significant policy decisions around the scope of the regime, such as definitions of 'customer data', 'account data', 'transaction data' and 'product specific data'.

[1] Treasury Laws Amendment (Consumer Data Right) Bill 2019, as introduced into Parliament on 13 February 2019 and lapsed on 11 April 2019.

The ABA strongly recommends that the 'catch all' provisions within the draft Rules associated with these definitions are removed. For example, the customer data definition (Schedule 2 clause 1.3 item 1 of the table) includes:

> *(c) any information that:*
>
> *(i) the person provided at the time of acquiring a particular*
>
> *product; and*
>
> *(ii) relates to their eligibility to acquire that product;*

and also:

> *(e) any other information that is specified in the data standards as being customer data in relation to a person.*

These catch all provisions are problematic in that they could expand the scope of the regime well beyond the policy intent without as rigorous a process for scrutiny as would be the case for amendments to the Rules. While Data61 does provide an online and open process for feedback to the ongoing development of technical standards, we note that this is a technical forum and we do not consider it appropriate as a decision-maker on key questions of scope. We consider that the legislation and rules should determine, without ambiguity, the scope of customer, transaction and product data that is captured by the regime. Any expansion of the scope of the regime should be done through amendment to the rules following appropriate public consultation.

Additionally, ongoing governance of the CDR needs to operate at the appropriate level in order to ensure that ongoing policy maintenance is undertaken at the appropriate level. To this end, the ABA makes the following recommendations:

- The ACCC should be required to formally review key decisions made by the Data Standards Body to ensure they are compliant with the Rules. Where the standards are inconsistent, the ACCC should direct the Data Standards Chair to consult on updated standards.
- The ACCC should remove or amend Rules which are found to be inconsistent with the operation of the Consumer Data Right Bill.
- The Rules should include a minimum period for consultation on the data standards of at least 28 days. This is consistent with the minimum consultation period for the Rules as mandated in the Bill, except where the Chair makes urgent standards in accordance with rule 8.9(1).
- Given the dynamic nature of the Data Standards, the Rules should mandate that at least two representatives, including one initial Data Holder from each designated sector maintain a position on the Data Standards Advisory Committee to ensure all stakeholders are involved in the development of standards for the CDR regime.

1.2 Joint accounts

We welcome the clarification in the draft Rules that joint accounts relate to two individual account holders who are acting in their own capacity and not on behalf of another person. This reduces some of the complexity in implementing a technical solution for such accounts. However, the consent requirements for joint accounts as currently drafted increases the technical complexities for banks.

In order for joint account data to be shared, the draft Rules require all joint account holders to authorise such sharing by using a joint account management service prior to sharing. If the parties have not used the joint account management prior to sharing, the data holder is required to refuse any requests in relation to joint accounts. In addition, the draft Rules contain new requirements that allow either party to amend their consent to share data as well as to revoke data sharing for some accounts but not others. This is unlike the UK model under which data sharing consent can expire or be fully revoked but not amended.

As the consent management and security standards are yet to be finalised, and the approach to joint accounts introduces additional requirements, it is not currently possible to implement a solution for joint accounts.

As implementation of the CDR for accounts with a single (individual) account holder is simpler than for joint accounts, we recommend that the first phase of open banking should commence with individual single accounts and that joint accounts should be phased in at a later stage. This would allow banks to fully focus on delivering open banking for the vast majority of their online customers.

1.3 Derived data

The ABA has consistently argued that derived data should be outside of the scope of the regime. We acknowledge and welcome the clarification provided in the legislation and draft designation instrument[2] that data holders will only be obliged to share data specified in the designation instrument (and not derived data). We also welcome the ACCC's clarification that this does not include materially enhanced data[3].

The ABA understands that Treasury intends to amend the designation instrument to clarify what is meant by "materially enhanced" data. Before this amendment occurs, there is a significant gap in the legislation, rules and designation instrument with no clear guidance on which data sets are in or out of scope.

As the data standards are continuing to evolve, and in some instances include what could be considered to be materially enhanced data, it is a matter of urgency that clarity is provided on the definition of materially enhanced data.

1.4 Privacy protections

As noted in earlier ABA submissions, there is considerable complexity with managing the treatment of CDR data as it moves through the system. This is in part due to banks needing to comply with both the Privacy Safeguards and the Australian Privacy Principles (APPs) depending on the stage at which a customer interacts with the CDR system.

Under the legislation, data recipients are generally subject to the Privacy Safeguards, while data holders are subject to certain Privacy Safeguards with the APPs remaining the primary privacy regime for those entities. However, the Explanatory Memorandum suggests that the ACCC would write consumer data rules for "receiving data holders" which would provide that certain received CDR data could revert to being treated under the APPs and not the Privacy Safeguards. This would occur if the CDR data that is received is '…of a class that the accredited data recipient would generate or collect in the ordinary course of its business outside of the CDR; and the accredited data recipient would use the information for the same purpose as their ordinary business'. Thus, if a bank received bank data, and it used that data for banking purposes, then it could handle the data under the APPs and not the Privacy Safeguards. The draft Rules do not address this transition from the Privacy Safeguards to APPs, and we request this be clarified in the next version of the rules. We also consider the concept of "receiving data holder" should be drafted so that it commences from the point at which an individual makes an application to the receiving institution, and not the point at which they become a customer.

Clarity on which set of privacy protections apply is critical, as depending on the particular use case and whether the CDR consumer is an existing bank customer, determining which regime applies could be a complex task. We demonstrate this by way of an example where CDR data becomes co-mingled with other internal and external sources of information.

[2] Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018, exposure draft published for consultation on 23 September 2018.
[3] ACCC (12 September 2018), *Rules Framework*, p.18.

Example – credit application

Fiona is an existing customer of Bank 1 and Bank 2. It is normal for customers to do their banking with more than one bank so this would be a common scenario.

Fiona has a transaction account with Bank 1 into which her salary is paid and which she also uses for some expenses. Fiona also has a credit card with Bank 2.

Fiona exercises her right under the CDR to transfer her transaction data from Bank 1 to Bank 2 as part of an application for a personal loan with Bank 2.

Bank 2 is required by responsible lending laws to make a decision about whether to approve the loan application based on information about Fiona's financial situation, which would normally include income and expense information (in this case from both banks) and a credit report from a credit reporting body. The responsible lending laws also require Bank 2 to provide the customer with a written copy of the final responsible lending assessment for credit if requested by the customer after the loan contract is entered into.

In this scenario, Bank 2 has existing data about the customer which is regulated by the APPs. However, the data transmitted under the CDR framework from Bank 1 to Bank 2 is regulated by the Privacy Safeguards. In order to ensure that it complies with both the APPs and the Privacy Safeguards, best practice would require Bank 2 to separate the CDR data from non-CDR data as it moves through the system.

However, once the CDR and non-CDR data reach Bank 2's credit decision engine it becomes impossible to separate them as they are necessarily co-mingled with all the relevant information required to be considered to make a decision on the loan application. We also consider it would be extremely challenging (if not impossible) to separate the data in such a scenario at the application stage because banks have a single application form (or screen) and it will contain both CDR and non-CDR data.

Based on our understanding of the Explanatory Memorandum, in this scenario, the CDR consumer is not yet a customer of Bank 2 for this product and so the Privacy Safeguards apply as do the APPs for those parts of the data that are already held by Bank 2.

In addition, it is unclear under which regime data provided and already held should be captured (for example customer information such as name and contact details).

If Fiona is unsuccessful in her application for a personal loan with Bank 2, under section 56EO(2) of the draft Bill, Bank 2 must destroy the redundant data or ensure it is de-identified unless the bank is required by law to retain it. Given for example, the co-mingling in the above scenario, it would be extremely challenging (if not impossible) to separate the data in order to treat the data which is covered by the Privacy Safeguards differently to the data that is covered by the APPs.

Fiona could also revoke consent during the credit decision process. In this case, we would face the same issue in trying to separate data to treat it differently under different regimes.

Similar complexities arise with other types of use cases.

1.5 Outsourced service providers

Under Part 7 of the draft Rules, an Accredited Data Recipient's (ADR) CDR policy must include a list of outsourced service providers (whether based in Australia or based overseas) and for each provider state the nature of the services it provides and the CDR data or classes of CDR data that may be disclosed to it. In addition, it must also in some circumstances include a list of countries which the service providers are based.

We understand the desire for transparency around the movement of CDR data but query the utility and practicality of maintaining an updated list of all outsourced service providers. Particularly where the publication of such information reveals commercially sensitive information regarding suppliers.

A requirement to list all outsourced service providers (either in dynamic form or through updating lists) would be a practically complicated and time-consuming exercise without any clear consumer benefit. In practice such an obligation would be very difficult for a large organisation to comply with.

In addition to the practical difficulties of managing and updating lists of outsourced providers, there may be security issues associated with publicly identifying suppliers and setting out the type of data they hold.

Finally, there is an open question as to whether data which is passively stored or passes through a system which is provided by a third party constitutes "use or disclosure" by the ADR. The ABA welcomes clarification on this point.

At present, banks are required to comply with a range of obligations related to their outsourcing arrangements including APRA's Prudential Standard CPS 231 on outsourcing. Under CPS 231, banks have a detailed framework for managing outsourcing arrangements, including controls around securing data, monitoring processes and notification. Banks must also ensure they have documented legally binding agreements in place with outsourced service providers.

The ABA submits that existing obligations on banks provide appropriate assurances to consumers that their data is being handled securely without requiring ADRs to list service providers as contemplated in the draft Rules. This objective could be achieved by relying on APP 8 and Privacy Safeguard 8 which require disclosers to ensure that any recipient is appropriately required to protect that CDR data (e.g. by being subject to an equivalent enforceable binding law or scheme or by taking reasonable steps to ensure the recipient will not breach the requirements such as by contractually obliging that recipient to comply with appropriate requirements).

1.6 Reciprocity

Reciprocity is a fundamental principle in the CDR regime and one that the ABA has advocated for since the Farrell Review and re-advocated for in the Rules Framework. The ABA reiterates its comments in the submission to the ACCC's consultation on the Rules Framework:

> "The ABA believes reciprocity is a key condition for the CDR to function as intended to benefit customers. The ABA believes Rules should cover full reciprocity from July 2019. Once an accredited person joins the CDR, either at the mandated point or voluntarily, they should also be required, if directed by their customer, to share in-scope data to other accredited CDR participants."

We also note the Farrell Report Recommendation 3.9 was "reciprocal obligations in Open Banking 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."

The ABA notes that Rule 5.2(e) provides a mechanism for inclusion of a limited form of reciprocity at a later date. However, the ABA recommends that the ACCC should make rules requiring the Accreditor to make reasonable enquiries as to the data that a prospective Accredited Data Recipient holds, or will hold under the CDR, for the purposes of determining whether reciprocal obligations apply.

Australian Banking Association

2. Other issues

2.1 Reporting, notification and record keeping

The ABA recommends that timeframes for notifications required under the draft Rules be reconsidered. Our view is that timeframes have been applied inconsistently throughout the rules, with timeframes for some notifications likely difficult to implement in practice and other important events not triggering a timeframe for notification.

For example, under draft Rule 7.7 the timeframe for notification in relation to data quality is 24 hours. This is particularly onerous in the context of the likely volume of individuals involved and number of transactions. We consider these requirements should be aligned with the APPs where possible. Eg the threshold of "as soon as practicable" would appropriately balance protecting consumers with practical considerations.

On the other hand, there is no timeframe specified under draft Rule 5.20 for the Data Recipient Accreditor to notify the Accreditation Registrar of the surrender, suspension and revocation of an ADR's accreditation. We consider that a timeframe for notification is important to ensure that participants are aware in a timely manner when such significant events in relation to accreditation occur.

Regarding notifications provided to consumers, there should be guidance on the form of such notification. We note that not all consumers have access to electronic notifications, and there should be flexibility for participants to determine the most appropriate and accessible method of communication in relation to a particular customer.

Clarification is also required on whether a data holder who is also an ADR can keep records collected in either role together in order to avoid the impractical logistics of having to keep those records separate.

2.2 Data definitions

Schedule 2 provides the definitions of customer data, account data, transaction data and product specific data.

2.2.1 Eligibility to acquire product

The definition of customer data extends to "eligibility to acquire a product"[4]. We would welcome clarification that this does not extend to data relating to credit decisioning as the number and type of documents captured would be too large. As drafted, the definition could potentially include all documents considered for loan approval (e.g. all documents relating to income, assets, expenses, liabilities, business plans etc). We note that paper documents received in connection with a product application are normally scanned and stored digitally so the restriction that only data held in a digital form should be captured as required consumer data has little impact in practice. We consider there should be a narrower definition of "eligibility to acquire [a] product".

2.2.2 Mobile numbers

The ABA's previous submission[5] noted that mobile numbers provided by a customer do not appear on statements or in online banking channels. Consequently, many banks use mobile numbers as a source of authenticating a customer. We seek clarity that the inclusion of a customer's "telephone number"[6] in the definition of customer data does not require the sharing of mobile phone numbers.

2.2.3 Customer account numbers

Account data is defined to include "the account number", which may include account numbers, BSBs and credit card numbers; all of which could be used to identify an account. The ABA had previously

[4] Schedule 2, 1.3, 1(c)(ii)
[5] ABA (12 October 2018), *Consumer Data Right Rules Framework*, submission in response to ACCC position paper.
[6] Schedule 2, 1.3, 1(b)(i)

submitted that consideration should be given to the tokenisation of this type of data, to minimise the potential security risks.

2.2.4 Third party data and privacy

In the ABA's previous submission, we noted that privacy of data related to third parties should be appropriately protected. This includes data in relation to a counter-party to a transaction (captured under the definition of transaction data) and payees under account authorisations (captured under the definition of account data). We consider the counter-party's privacy should be considered when they have not been notified or provided consent to their details being disclosed.

2.2.5 Account authorisations

Under the definition of account data[7], "authorisations" could potentially cover the details of who is authorised to operate an account. We recommend that "details of who is authorised to operate an account" be excluded from the definition.

2.3 Direct debits

Similar to joint account data, the ABA does not believe that data related to direct debits should be in scope for the first phase of open banking.

To set up direct debit arrangements, customers complete a Direct Debit Request (DDR) authority with the business that will be collecting payments from their account. The customer gives deposit account details (BSB and account number) to allow the merchant to debit the customer's account regularly to pay for the services they provide the customer. They do not instruct their bank to put in place this payment. As such, a bank does not have full visibility over what direct debit arrangements a customer has in place and is unable to guarantee an accurate list of direct debit arrangements at any point in time. Banks can only derive direct debit data from transaction history, and this derivation will result in an incomplete result set.

2.4 Meaning of phase 1 and 2 products

We note that under the phase 1 product category[8] there is a "credit and charge card (personal) account". Some banks do not have any products that are described/categorised as a "credit and charge card". The ABA suggests instead that these categories are presented separately.

Under phase 2 products, a "residential mortgage" is listed as a product category. We note this should be described instead as a home loan as the mortgage is the security over which the loan is held. All major banks call these products home loans and investment property loans.

2.5 Required consumer data

Under Schedule 2, Part 2, 2.2(e), required consumer data is defined to capture active accounts, or if not active, accounts that are closed on or after 1 January 2017. Note 3 then states:

> *So long as the CDR consumer has an account that satisfies paragraph (1)(e), they will be able to make or cause to be made a consumer data request that related to any account they have with the data holder, including accounts that do not themselves satisfy that paragraph.*

It is unclear to us whether the effect of Note 3 is to capture accounts closed prior to 1 January 2017, and if so, the extent to which historical accounts will be captured.

The ABA submits that accounts prior to 1 January 2017 should not be included in the regime as historical data may not be available in a digitally accessible format. The ABA welcomes clarification that

[7] Schedule 2, 1.3, 2(d)
[8] Schedule 2, 4.3, 1

the position under the draft Bill and designation instrument is correct i.e. that only transaction data dated 1 January 2017 or later on any type of account is required to be disclosed.

2.6 Historical Data

There is a gap between the Rules and standards in respect to specifying the extent to which historic data should be made available. The Data61 Decision 021 on ***Non-functional requirements*** states that '*requirements around data extent (ie the time periods for which data should be made available) will be specified by the ACCC rules*'. We note that the Rules are silent on this issue. In the absence of such timeframes in the Rules, the implication is that the time extent of data to be shared will be unlimited. For example, if in 2027 a data recipient makes a call on a data holder for transaction data on a customer a data holder would be required to provide 10 years of data.

The ABA recommends that the Rules be amended to include time period which were proposed in a draft version of the Data61 Proposal 21, namely:

- 24 months of transaction data for open accounts should be available
- 12 months of transaction data for closed accounts should be available

2.7 Consumer data request

Under Division 3.2, when a consumer data request is made by a CDR consumer, the data must be disclosed in human readable form and in accordance with the data standards. We note that the data standards only cover data to be disclosed in machine readable form, and request clarification on the effect of this rule.

2.8 Refusal to disclose in response to a consumer data request

Under draft Rule 3.5(1)(a), a data holder may refuse to disclose CDR data in response to the request if it has reasonable grounds to believe that the disclosure would "create a real risk of serious harm or abuse to an individual". We recommend that the ACCC provide some guidance around the type of scenarios it would consider would constitute serious harm or abuse.

In relation to draft Rule 3.5(2) it is unclear whether a failure due to a blocked customer account (for example, due to fraud) would amount to a permitted refusal. In addition, one of our members blocks 1,500 customer accounts per month, it would be a significant burden if there is a requirement for a 24-hour notification for such accounts as is currently required under draft Rule 3.5(2).

2.9 Use and disclosure of data collected pursuant to consumer data requests

Under draft Rule 4.8(1)(b) there is a reference to "providing" data to an outsourced service provider. We note that this is different to the concept of disclosure of data under the APPs which encompasses the transfer of data as well as access, and the APP Guidelines in relation to APP 6 which also identify that in certain cases, a disclosure to an outsourced service provider can be considered a "use" by the data provider in which case liability remains with the data provider rather than the data recipient. We suggest that the rules should be aligned with established concepts in privacy law by replacing the references to "providing" the data with "disclosing".

Under draft Rule 4.8(4) there is an absolute obligation for the ADR to ensure an outsourced service provider takes the steps in Schedule 1. We suggest aligning this requirement with Privacy Safeguard 8 which sets out a reasonable steps qualification for consistency i.e. that the ADR takes reasonable steps to ensure that the recipient will not breach the Schedule 1 standards.

2.10 Withdrawal of consent to collect CDR data and notification

Under draft Rule 4.11(1) there is a reference to a CDR consumer withdrawing their consent in writing. We query why a withdrawal would need to be in writing when it is not a requirement for the initial

consent. We consider it would lead to a bad customer experience to ask consumers to provide a written withdrawal request.

2.11 Consumer Dashboard requirements

Draft Rule 7.6 states updates which are required to the consumer dashboard. Further clarity is required around the level of detail to be represented on the dashboard. For example, does it need to reflect every API call or can it reflect a summary?

2.12 Correcting CDR data

Draft Rule 7.10 sets out the steps that must be taken when a consumer has requested a correction of data under subsection 56EP(1) or (2) of the legislation. However, further clarity is required around the instances where data would be deemed to be incorrect, and when a written notice is required. Where a record is correct for the purpose for which it was provided but subsequently corrected or updated should not fall under Rule 7.10. An example is, where a customer makes a CDR request to share their address and some months later updates the address with the data holder, a correction should not be required.

2.13 Definition of products branded with the name of the initial data holder

In Schedule 2, paragraph 4.1 refers to products in scope as being those "products that are branded with the name of the data holder" and Rule 4.4 refers to a "product that is branded with the name of the bank". We consider that these provisions could be better expressed.

For some member banks, the registered business names of the parent entity include the brand names under which it operates. To avoid ambiguity, we suggest these provisions specifically list the brand names for each entity.

2.14 Streamlined accreditation

The ACCC had previously[9] outlined a streamlined accreditation process, which doesn't appear to be featured under the draft Rules. We recommend that initial data holders automatically receive accreditation and therefore can immediately participate as ADRs.

2.15 Revocation of Accreditation

The ABA believes that it is critical to the regime that the Rules mandate that the Data Standards develop a dynamic, real-time Certificate Revocation List to ensure data is being shared correctly and safely.

2.16 Information security controls

Part 2 of Schedule 1 sets out minimum information security controls ADRs must meet in order to comply with Privacy Safeguard 12. We note that security controls are often updated to keep pace with new technology and it may be a better option for the draft Rules to refer to accepted international standards on security controls instead of prescribing specific requirements that may become outdated over time. Examples of relevant accepted international standards are NIST Cybersecurity Framework, COBIT 5 and ISO/IEC 27001.

2.17 CDR Contract

As the CDR contract is a new concept the industry will have to consider what constitutes a standard CDR contract and what -flow on effects the CDR contract has. The practical effect of not having a CDR contract in place would be that any requests made under the Rules for CDR data on behalf of a CDR consumer would be invalidated. Therefore, it is important that data recipients have clear guidance as to

[9] ACCC (21 December 2018), *Rules Outline.*

the necessary conditions of a CDR contract. The ABA recommends that the ACCC provide guidance in the Rules on the basic requirements of a CDR contract to ensure that the CDR contract is easy for a consumer to understand.

2.18 Data minimisation principle

The inclusion of the data minimisation principle is a positive step in ensuring that an accredited person does not collect or use more CDR data than is reasonably needed to provide a good or service to a CDR consumer under a CDR contract.

The ABA recommends that the Rules should include a Governance framework, which includes minimum controls and processes for monitoring and the verification of the Data Minimisation Principle.

2.19 Cloud environments

APRA has acknowledged the risks inherent in using cloud environments and provided detailed guidance to APRA-regulated entities. The ABA notes that the draft Rules do not address the need for controls with respect to storage of information in cloud environments, however controls are important in order to mitigate risk. The ABA requests that the Rules include similar controls for the use of cloud environment by CDR participants that are not APRA-regulated entities.

2.20 Other matters where the rules are silent

We have identified the following instances where the rules are silent or do not provide for circumstances:

- Treatment and rules for authorities for authorisations, such as powers of attorney, payroll and multi-party ownership;
- Situations where the imposition of a fee is permissible;
- Customer testing and customer experience references are minimal deferring it to a standard that is acceptable to the Data Standards Chair. As noted in section 1,1 there is a need to ensure that the governance of the CDR aligns decision making to the appropriate forums.

Kind regards

Emma Penzo
Policy Director
[redacted]