Australian Banking Association

Consumer Data Right Rules Framework

ABA Response to ACCC Position Paper

12 October 2018

Pip Freebairn, Policy Director

Barry Thomas, Open Banking Standards Director

Australian Banking Association Inc. ARBN 117 262 978
Incorporated in New South Wales. Liability of members is limited.

Australian Banking Association

Executive Summary

The ABA welcomes the opportunity to comment on the Australian Competition and Consumer Commission's position paper ("**the framework**") outlining the proposed Rules framework for the Consumer Data Right for banking.

ABA members believe that the CDR is a transformative reform and are committed to its success. The CDR has the potential to fuel innovation across the economy and benefit customers through an expanded choice of products and services. ABA members are focused on working with Government, regulators and stakeholders to ensure that the CDR is a world-leading data sharing regime. Maintaining customers' trust and confidence in the regime is key to ensuring the full benefits of data sharing are realised.

The banking industry is now implementing open banking, with major banks required to share data from July 2019. The ABA and our members are working with the four agencies — the Australian Treasury, the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and Data61 — to design an appropriate system of economy-wide legislation, together with industry-based data sharing Rules and technical standards.

The Rules proposed by the ACCC in the paper cover the banking industry and will be the Rules in place for the first tranche of data sharing beginning July 2019. We welcome the pragmatic approach taken by the ACCC to make "Rules on the matters that are essential for the commencement of Open Banking on 1 July 2019."

ABA members support most of the Rules outlined in the paper. This submission focuses on proposed Rules that ABA members believe pose technical complexities or policy issues that require further consideration.

Australian Banking Association

Table of Contents

Australian Banking Association

1. Overview

The ABA welcomes the opportunity to comment on the Australian Competition and Consumer Commission's position paper ("**the framework**") outlining the proposed Rules framework for the Consumer Data Right for banking.

The ABA notes our previous participation in the Productivity Commission's *Data Availability and Use* report (**PC Report**) and Treasury's 2018 *Review into Open Banking* report (**the Farrell Report**). We are also engaged with Treasury's current consultation on the second exposure draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018.

We thank the ACCC for holding stakeholder roundtables to discuss the framework. Looking ahead, the ABA would welcome an ongoing dialogue with the ACCC, industry and stakeholders as the Rules are finalised.

This paper steps through the ABA members' recommendations and areas where members seek clarification on the ACCC's proposed framework. ABA members are keenly focused on delivering customers a safe and secure data sharing framework from July 2019. We look forward to working with the ACCC on future versions of the Rules.

Finally, where headings are numbered in this document, the numbering corresponds with that used in the ACCC paper.

Australian Banking Association

2. Sharing data with third party recipients

Summary of proposed Rules

The ACCC proposes to make Rules to the effect that:

- an accredited data recipient may only collect and use a consumer's data where it has obtained their consent, and only in accordance with that consent.
- a data holder must share a consumer's data with an accredited data recipient where the consumer directs and authorises the data holder to do so.
- data sharing must only occur where the consumer has given relevant informed consent to the accredited data recipient and authorisation to the data holder.
- authorisation and authentication processes will meet certain requirements.
- data sharing must occur via an API. The API will be implemented in accordance with the standards developed by the Data Standards Body, and data sharing must occur in accordance with those standards.

The ACCC proposes that in the first version of the Rules, data sharing will not be subject to fees.

ABA Response

ABA members note that final requirements on the authorisation and authentication requirements are needed as a matter of urgency to inform the technical standards work led by Data61.

ABA members note there may be some circumstances where fees should be charged beyond derived data, and that these circumstances should be covered in the first set of Rules. Specifically, ABA members believe that data holders should be able to charge accredited data recipients ("**ADRs**") for frequent calls on data. We believe a maximum number of times ADR call data should be limited to four times a day for free. Beyond that, data holders should be able to charge ADRs a fee to recoup costs associated with holding and maintaining data.

Australian Banking Association

3. CDR consumer – who may take advantage of the CDR?

Summary of proposed Rules

The ACCC proposes that the first version of the Rules will enable a consumer to direct a bank to share their data only if they are currently a customer of that bank.

The ACCC proposes that the first version of the Rules extend the CDR to consumers who have access to and use online banking, but not to offline consumers.

The ACCC seeks stakeholder views on what would be a reasonable timeframe for extending the CDR to former customers and offline consumers.

ABA Response

3.1. Former customers

The ABA supports ACCC's decision not to include former customers in the first set of Rules of data sharing. As the ACCC recognises, technical and compliance issues around authentication exist which would make this infeasible to deliver in Stage 1.

The ABA also supports limits on how long a former customer can access data under the CDR.

Record keeping obligations require banks to keep former customers' details for seven years. This data is held in systems that are not always easily accessible digitally, especially since former customer do not have access to online banking channels. The ABA recommends that the CDR apply only to data that is currently accessible and publicly available in digital form.

The use cases for former customers to access data for seven years are limited. Product comparison and personal financial management transaction history use cases will all be serviced adequately through a shorter history. This point also holds for existing customers, who will be able to access 2.5 years of data at the start of open banking at January 2017. Given both limited use cases and the technical complexities of building and maintaining a CDR data store, ABA members believe that there should be limits on the length of CDR historical information.

3.2. Offline customers

ABA members support not including offline customers.

The ABA's 2017 Consumer Banking Survey found that 80.9 per cent of customers access their accounts using internet banking.[1] This proportion is likely to be higher when the use of mobile apps is also considered.

ABA members believe that offline customers are likely to be better served through other initiatives that are more appropriate to their circumstances.

[1] The ABA commissioned Roy Morgan to undertake a survey of 4000 Australians in November 2017. The questions covered issues on financial products and services provided by banks and other financial institutions.

Australian Banking Association

4. Data holder – who is obliged to share data?

Summary of proposed Rules

The ACCC proposes to make Rules to give effect to the phased implementation of Open Banking as outlined by the government.

The 'four major banks' will be within scope of the Rules for the initial phase. The ACCC proposes to exempt the related brands of these banks from the first version of the Rules.

Other ADIs, with the exception of foreign bank branches, will be brought within scope 12 months later, including related brands of the four major banks.

The ACCC proposes to make a rule to acknowledge that exemptions for certain entities from some or all obligations may be granted in certain cases, should the need arise.

ABA Response

ABA members support the phased implementation outlined in the Rules, including the phased product introduction and the one-year extension for non-major ADIs. The phasing recognises the technical and compliance builds required to implement a safe and secure CDR regime.

We believe, as was intended by Farrell, that any ADI wishing to enter the CDR earlier than their mandated date should be required to share data as a data holder if they wish to receive data. We also believe that entities from non-designated sectors should be required to share equivalent data if they enter the CDR.

We also that many banks (especially non-major banks) have outsourced some of their product holdings to other financial institutions, or what is known as white-labelling. Further discussion and clarification on how data is exposed in these circumstances is required.

Australian Banking Association

5. Datasets – what data is within scope?

Summary of proposed Rules

The ACCC proposes to make Rules to specify minimum inclusions for 'customer data'. In relation to customer data, the ACCC also proposes:

- to make a rule to the effect that the obligation to share customer data will only apply to this information where it is kept in a digital form.
- to make a rule to the effect that product data which relates to an account that a customer holds is within scope.
- to not include identity verification assessments within the scope of customer data in the first version of the Rules.
- to not include data relating to authorisations to share data given under the CDR within the scope of customer data in the first version of the Rules.

The ACCC proposes to make Rules to specify minimum inclusions for 'transaction data'.

The ACCC welcomes submissions from stakeholders on what transaction metadata could be within scope; what benefits to consumers it could deliver; and what risks would arise.

The ACCC proposes to make Rules to specify minimum inclusions for 'product data'.

The ACCC proposes to make Rules to the effect that data holders will be obliged to make 'generic' product data publicly available (see section 11 below).

The ACCC proposes to make Rules which specify that the standards will include further detail with respect to the relevant datasets, including specific fields and formats and a detailed product data taxonomy. The ACCC proposes to make a rule to the effect that data should be shared in the format as determined by the standards.

ABA Response

5.1. Draft legislation and designation instrument

The ABA supports changes in the CDR exposure draft that would limit the ACCC's rule making power on designating datasets. ABA members support that the power to designate data rests with the Minister and that the Minister must consider any likely effect on intellectual property from the data included in the designation instrument.

The ABA supports the ACCC's principle that in-scope data should meet the condition of being "widely available to the general public". Regulators have expressed that in-scope data should include data that can be seen on a customer's online banking channel or on their statement. ABA members have taken this approach when working through the datasets, where that information is available in a digital format.

5.2. Derived data

As the ACCC recognises, the spectrum of derived data ranges from simple transformation like account balances, to sophisticated analysis like credit modelling. The ABA welcomes the ACCC's decision to follow Farrell's recommendation on value-added data. That is, data that is a "material enhancement by the application of insights, analysis or transformation by the data holder" should remain out of scope.

We also welcome the updated clarification provided by Treasury in the second consultation paper on the CDR exposure draft that derived data to be shared under the CDR must be designated by the Minister in the designation instrument. This will allow sufficient consultation on designated datasets.

5.3. Datasets

We have addressed issues of both a policy and technical nature below.

ABA members do not support including metadata across any of the datasets. The PC broadly investigated sharing metadata but this was not explored in the Farrell Report, and there has not be adequate opportunity to explore the implications of including metadata, or the consumer appetite for its inclusion.

5.3.1. Customer data

- **KYC Assessments**

  The ABA welcomes the decision not to include **identification verification assessments** in the first tranche. We will await the implementation of the reforms that arise from the statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) that was tabled in Parliament in April 20160.

- **Mobile numbers**

  ABA members note 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 one source of authenticating a customer. So from a security perspective, we question if it is necessary to include this data in the CDR. Also, given that this data is easy for a customer to provide to any third party, we do not see a case for including this data as in scope.

- **Customer Account numbers**

  This includes account numbers and BSBs, along with credit card numbers. These can be used to identify an account. If these data are included in datasets, consideration should be given to the security aspects of exposing these data including increasing the opportunity for malicious transactions. ABA members consider these data should be tokenised. Tokenisation can be considered masking data, which enables important information to be conveyed without compromising security.

- **Payee lists/direct debit authorisations on the account(s)**

  ABA members note from a technical point of view, payee lists can be included in scope from July 2019. However, from a security and privacy point of view, further thought is required regarding a payees' privacy as their BSB, name and account numbers would be exposed under this list. As all payees' consent is unlikely to be given ahead of July 2019, we believe this data should remain out of scope until these issues are worked through.

- **Direct debits**

  It is technically infeasible that an accurate list of direct debits could be delivered in tranche one given the complexities of the Australian direct debit system as compared to the simpler UK system. Therefore, we do not believe that direct debits should be in scope for July 2019.

  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.

  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.

  For example, any existing direct debit that has been setup but not executed a transaction will not show up in the bank's list of direct debits. Other useful information about a direct debit such as

expiry date and frequency cannot be derived from a transaction that a bank can see through transactions.

We note that many ABA members are building technical solutions to comply with the 2019 Banking Code of Practice amendments to identify direct debits from an account's transaction history. The Banking Code of Practice already caters for the constraints that banks have in producing this data, namely that it is restricted to the previous 13 months, and that the list will include only those direct debits and recurring payments that are known to the bank from the information they receive about the transactions on the account. Therefore complete accuracy can not be guaranteed.

- **Scheduled and future-dated payments**

  Unlike direct debits, banks do have full visibility over payments that a customer has set up through their bank's online banking channel (ie their internet banking or mobile app) to another third party.

  These include:

  - periodic payments scheduled to be paid out of a bank account on a fixed scheduled, or "scheduled payments";
  - future-dated transfers are those payments that are one-off.

  These data are technically possible to deliver by July 2019, although like payee lists, consideration needs to be given to revealing personal information of the recipients given their authorisation to share data has not been sought in this example.

  Scheduled and future-dated payments can also be made by a customer to another one of their own accounts. In this instance, ABA members believe this data should be in scope.

- **Unique identifiers**

  The ABA seeks clarification on the underlying rationale of ACCC's intention to include unique identifiers associated with an account. This term is broad and there are many unique identifiers associated with accounts. In some cases, the unique identifiers are used for internal purposes and given this, would not be standardised across banks or convey useful information beyond that bank. It is also unclear what privacy implications may be associated with these identifiers.

- **Authorisations**

  We seek clarity on what is meant by the authorisations on the account which is not defined in the Rules framework. If this means those parties who are authorised to operate on the account, such as accountants and other third parties, the ABA believes that details surrounding these third parties may need to be masked for security purposes.

  Additionally, account authority information may be paper based, or may be stored in separate locations and formats for each bank channel that can access the account (online banking, corporate online banking, branch and contact centre). The additional technical complexity of including this information is infeasible to deliver by Stage 1 of the Rules.

5.3.2. Transaction data

- **Opening and closing balance of an account for the period specified**

  Opening and closing balance for period is feasible and will need to include currency.

- **The date on which the transaction was made**

  This is feasible and should be included.

- **The relevant identifier for the counter-party to a transaction**

  Like the payee list, the relevant identifier for the counter-party to a transaction may raise some privacy implications for third party whose data is being shared. This should be considered.

- **The amount debited or credited pursuant to a transaction**

Feasible and should be included.

- **The balance on the account prior to and following a transaction**

  A balance check on each transaction is technically very difficult and would put significant strain on the system through an overload of information. Furthermore, many banks do not perform such calculations before and after each transaction, rather doing so and the beginning and end of statement periods.

- **Any description in relation to the transaction, whether entered by the consumer or the data holder**

  Data that is inputted by customers may reveal personal information and this should be masked.

- **Any identifier or categorisation of the transaction by the data holder (that is, debit, credit, fee, interest, etc)**

  The categorisation requested is an attribute of the transaction that is typically held on file, for example, debit, credit, fee, interest. The ABA agrees it should be included.

  Further categorisation, such as “groceries”, “fuel”, etc is value-added data resulting from work done by banks to analyse and categorise spending and should remain out of scope.

5.3.3. Product data

- **Generic versus individual product data**

  We note, as the ACCC does, that two types of product data exist:

  - Generic or reference data that does not relate to a unique individual; and
  - individual product data which relates to product information for an existing account holder.

  To enable practical comparison of products that are available to a customer against the product(s) currently held by a customer it will be essential that the generic product dataset and the individual product dataset be easily comparable.

  As a consequence, the proposed Rules may require the banks to undertake substantial systems re-development to be able to express both their generic product data and the product data held on individual accounts in ways that are at least mappable to new industry-standard taxonomies (see below). While ABA members are supportive of this important use case the scale of this task should not be underestimated. The proposed Rules relating to product datasets suggest very rich product descriptions that will be challenging to implement by July 1, 2019.

- **Product data taxonomy**

  Looking ahead, ABA members note that in-scope product information will set the parameters of product comparisons and thus in many ways define the scope of competition. The underlying product data taxonomy and schema will need to be flexible, extensible and rapidly evolvable to account for ongoing innovations that can be captured in product reference information.

  ABA members foresee challenges in taxonomy and schema development. The concept of “product type” provides a good practical example as there is no industry-agreed definition of what this term means. The term will need to be formally defined, the term’s range of possible values agreed, and the banks will need to determine how they can map their internal concepts of product type to the industry standard. Similar challenges will exist for many of the terms envisaged by the Rules, requiring extensive efforts to devise practical and workable taxonomy and schema.

  We note that work in the UK to develop a taxonomy took significant time and resources. In the Australian context similar efforts to develop an industry standard taxonomy for mortgages (the LIXI standards) was also a multi-year project.

- **Grandfathered products**

  We note that an individual's account data may encompass data relating to product types no longer offered by the banks. While account-specific product information will necessarily include actual product information regardless of whether the product itself is still available we believe that generic product data should only be required to include products that are currently on offer.

- **Product prices: fees and charges, including interest rates, associated with the product and the circumstances in which they apply**

  We understand the intention of including these data types. From a generic product reference data standpoint, providing customers with standard variable rates is relatively easy. However, for individual's product data, it is technically infeasible to provide customers with a meaningful interest rate at this point.

  ABA members note the difficulty of providing interest rate information on an individual account when that interest rate is part of a bundled interest rate deal, or package deal. It may also not account for an offset account, meaning the price is not entirely transparent.

  From a technical standpoint, providing product bundling and relationship discounts in the short term would be challenging. Without them, the interest rate provided to the customer is confusing and would not represent their effective current deal so a flawed comparison market would result.

  Additionally, the mortgage lending rate for an individual will reflect the package and benefits they have, priced for them using contextual information gathered by a bank that is not the scope of data sharing. Therefore, using this individual's interest rate product may be meaningless if it is compared to generic product data that takes no account of an individual's circumstances.

  Interest rates on credit cards also raise several issues around balance transfer rates along with credit card lending rate for an individual.

  In summary, ABA members do not believe that meaningful interest rates on an individual's product reference data can be delivered in Stage 1. We note that the UK narrowed the scope of the individual account product sets in scope given these challenges.

- **Features and benefits**

  These data are not standard across banks so we believe this information should be shared in a free text field from July 2019.

- **Customer eligibility criteria**

  These data are not standard across banks so we believe this information should be shared in a free text field from July 2019.

Managing data requests

Most banks will avoid exposing APIs directly from their core banking technology platforms, as API demand is unpredictable, spiky and will increase exponentially as more accredited parties come on board. Non-major banks, in particular, note that scaling core banking systems to demand will pose challenges. Consequently, it is likely that most CDR participants will expose read-only APIs from a scalable copy of the data outside the core banking platform.

ABA members seek clarification on how timely the datasets need to be as these copies are being designed and implemented.

5.4 Reciprocity

ADIs may join the CDR earlier than their mandated start date of July 2020. We believe any entity should be able to join the CDR ahead of its mandated start date.

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 ADI 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. Given that ADIs will also hold the designated datasets, this is a relatively simple application of reciprocity.

For example, Bank A is a small ADI and is the first non-major bank to join the CDR in July 2019. Bank A becomes accredited to receive data and is able to access data from the four major banks. Bank A receives data when a customer of a major bank directs their bank to share data with Bank A. Importantly, because reciprocity is in place, the customers of Bank A will also be able to share their data held at Bank A and access the benefits. Reciprocity will ensure that Bank A is both a data holder and data recipient at accreditation, and the customers of Bank A will be able to direct their data to any other accredited data recipient. Under this circumstance, the most customers benefit.

The broader principle of reciprocity should also apply to any entity from other industries wishing to access the CDR regime. Entities from other industries may not hold data covered the designation instrument. But they will hold data about their customers that is valuable to their customers. This core customer data should be surveyed as part of the accreditation process.

The ABA believes that the core customer data that should be placed in scope is the data that would benefit customers if customers were able to direct it to a third party. For example, online retail transaction data that could provide third parties with a greater insight around a customer's spending behaviour. This data, combined with banking data, could be used by a fintech to develop a personal financial management tool that would benefit a customer.

The ABA's view on reciprocity follows from the Farrell Report. We believe that reciprocity being in place from July 2019 is key to ensuring that customers benefit from a dynamic and competitive data sharing framework.

Farrell Report Recommendation 3.9 – 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.

Australian Banking Association

6. Accreditation

Summary of proposed Rules

The ACCC proposes to provide for a single general tier of accreditation in the first version of the Rules.

The ACCC also supports the development of lower tiers of accreditation, and welcomes the views of stakeholders about the tiers that it would be practical to implement and the basis for any reduced accreditation requirements.

The ACCC proposes to make Rules that the Data Recipient Accreditor grant accreditation to an applicant if it is satisfied that:

- the applicant is a 'fit and proper' person to receive CDR data
- the applicant has appropriate and proportionate systems, resources and procedures in place
- to comply with the legislation, the Rules and the standards including in relation to information security
- the applicant's internal dispute resolution processes meet the requirements specified in the Rules and the applicant is a member of an external dispute resolution body recognised by the ACCC
- the applicant holds appropriate insurance. The ACCC welcomes views about appropriate insurance cover, current availability and cost.

The ACCC proposes to make Rules that will specify the manner in which accredited data recipients are permitted to describe their accredited status.

The ACCC proposes to make Rules to provide a streamlined accreditation process for ADIs (other than restricted ADIs or providers of purchased payment services).

The ACCC does not propose to provide for recognition of accreditation in other jurisdictions in the first version of the Rules.

The ACCC proposes to make Rules that will require any foreign entity that is granted accreditation to appoint a local agent that will be responsible for any obligations of the foreign entity under the CDR regime.

The ACCC proposes to make Rules specifying the powers and obligations of the Data Recipient Accreditor, including Rules:

- allowing the Data Recipient Accreditor to suspend or revoke an accredited data recipient's accreditation on grounds relating to the criteria for accreditation and to protect the security or integrity of the CDR regime
- providing for the revocation of accreditation where this is requested by an accredited data recipient.

The ACCC proposes to make Rules that will specify what happens in relation to a data recipient's CDR obligations when a decision is made to suspend or revoke its accreditation.

The ACCC proposes to make Rules that will require an accredited data recipient that enters into an outsourcing arrangement involving the disclosure of CDR data to ensure it has appropriate plans and processes in place for managing risk.

The ACCC proposes to make Rules that specify the steps an accredited data recipient must take to protect CDR data from misuse, interference, loss or unauthorised access, modification and disclosure. The ACCC welcomes views from stakeholders about appropriate industry standards that may be recognised under the Rules for compliance with this obligation.

ABA Response

The ABA notes many of the accreditation criteria are focused on the response to a data breach. We believe the Rules should have an equal focus on the ongoing steps that an ADR should be taking after initial accreditation to ensure data breaches do not occur.

We support ongoing monitoring, along with periodic and random audits of ADRs to ensure they can hold customer data safely and securely.

We also note that the data holders should be given the right to withhold any data transfers if they believe that the data will not be securely held. This option has been given to data holders in the Government's Comprehensive Credit Reporting regime.

6.6 Data Recipient Accreditor's powers

The ABA believes that the Data Recipient Accreditor would be best established as a new entity that is given the specific technical and compliance resources to monitor and enforce the accreditation criteria.

6.7 Revocation or suspension of accreditation

6.7.1 Consequences of revocation or suspension of accreditation

In the case where a decision is made to revoke accreditation, the ACCC proposes that the data recipient is to delete or de-identify the data.

ABA members do not believe that deidentification should be an option as it may not be adequately deidentified so as to prevent reidentification. The ABA would suggest changing to deletion only in this context. This step should be thoroughly audited by the Data Recipient Accreditor to ensure that customers' privacy and security are protected.

6.9 Ongoing information security obligations

We note the ACCC's interest in possible information security standards that would demonstrate that an entity has in place adequate policies and systems in relation to risk management and security in relation to management of CDR data.

ABA members support the standards named in the report and note that security arrangements should correspond with the tiers of accreditation that the ACCC is proposing. We believe that further consultation with APRA, ACCC and industry would be helpful to assess which the appropriate standards for each level. APRA have expertise in banking data and systems, and would have important insights from drafting CPS234 Information Security Prudential Standard, expected to commence on 1 July 2019.

We note that the following should also apply to CDR participants:

- A "reasonable steps" provision – data holders can withhold data from accredited third parties if they believe they are not taking reasonable steps under Section 20Q of the Privacy Act to protect customer security. This is akin to the Comprehensive Credit Reporting regime, which enables the regulator to penalise the data holder if the third party is found to have taken reasonable steps.
- Annual attestation would encourage participants to maintain adequate cyber defences. This approach would work with a principles-based approach to regulation, such as that taken in APRA's proposed CPS234 Information Security Prudential standard.
- Threat monitoring – the Australian Cyber Security Centre should have a centralised role sharing threat data, and collecting data on fraud and cyber incidents to enable the development of a data insurance market under the CDR.

7. The Register

Summary of proposed Rules

The ACCC proposes to make Rules relating to the Register, including in relation to the information required to be made publically available online and the powers and obligations of the Accreditation Registrar.

ABA Response

The ABA strongly supports the ACCC's position that the public address book is live, robust and decentralised as well as secure, transparent and include a method of tracing all changes made.

ABA members believe that all CDR recipients must be immediately notified via a dynamic address book when an accreditation has been revoked, suspended or varied. This will enable data holders to take timely steps to protect their customers.

The ABA believes that the CDR directory would be most successful if it was run by an outsourced provider. The effectiveness of the directory is key to the success of open banking and requires a level of technical expertise and agility that would be best met by a stand-alone organisation.

Australian Banking Association

8. Consent

Summary of proposed Rules

The ACCC proposes to make Rules to the effect that where consumers with a joint account hold individual authority to transact on that account they will each be able to give individual consent to share their joint data under the CDR regime. The Rules may require that each joint account holder be notified of any data sharing arrangements and given the ability to terminate them should they wish.

The ACCC also wishes to better understand the complexities of the issue of consent in relation to complex accounts and any other relevant scenarios and seeks stakeholder views on this.

The ACCC does not propose to make Rules that would seek to treat minors differently from any other consumer who may take advantage of the CDR.

The ACCC proposes to make Rules to the effect that an accredited data recipient must obtain a consumer's consent to both collecting, and using, specified data for specified purposes and for a specified time.

The ACCC proposes to make Rules requiring consumer consent to be freely and voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn. In particular, the ACCC proposes to make Rules to the effect that:

- accredited data recipients cannot make consent to share data a precondition to obtaining other services not related to, or dependant on, the sharing of CDR data.
- consent must be unbundled with other directions, permissions, consents or agreements, and must not rely on default settings, pre-selected options, inactivity or silence.
- accredited data recipients must provide specified information to consumers as part of the consent process.
- consent be obtained using language and/or visual aids and a process that is concise and easy for consumers to understand, and that, as part of the standards-setting process, the consent process should be tested for consumer comprehension. Accordingly, the ACCC does not propose to make a rule requiring all information to be displayed on a single screen.
- accredited data recipients must disclose, in an unambiguous way at the time of seeking the consumer's consent, the uses to which data will be put. Accredited data recipients may only use data in line with the uses to which the consumer has consented, and should only seek consent to access the minimum data necessary for the uses agreed to.

The ACCC proposes to make a range of Rules which will help provide consumers with a straightforward withdrawal process.

The ACCC welcomes stakeholder views regarding the extent to which a consumer should be able to decide whether their redundant data is de-identified or destroyed.

The ACCC proposes to makes Rules that will require accredited data recipients to have a system in place which allows consumers to manage their consents easily.

In relation to on-selling of data and use of CDR data for direct marketing, the ACCC's current position is that it proposes to make Rules that will prohibit the use of CDR data for these purposes. The ACCC welcomes stakeholder views on this proposal.

Australian Banking Association

ABA Response

8.1. Who can provide consent?

8.1.1. Joint accounts and complex authorisations

The ACCC has adopted the Farrell Report recommendation that uses authorisation to transfer money as the principle to be followed when deciding who should hold authority to initiate data sharing.

The majority of joint accounts have simple authorisations in place, where account holders can individually and independently authorise transactions. In this case, these account holders should be able to initiate data sharing independently. This is technically feasible to deliver. Consequently, ABA members believe joint accounts with simple authorisations should be in scope from July 2019.

More complex arrangements should be out of scope for July 2019 given the technical issues around building consent solutions along with compliance difficulties. ABA members do not believe these issues can be addressed adequately in the short timeframe, and especially given the numbers involved are relatively small.

These scenarios include:

- Joint accounts where two or more account holders are required to authorise money transfers, and therefore would be required to authorise data transfers.
- Accounts were one account holder is able to authorise money transfers but other parties are given electronic access to transact on an account such as accountants in a small business, or employees in a corporate.

8.1.2. Minors and vulnerable customers

We also do not believe minors should be in scope of the CDR as they do not have enough understanding to comprehend what they may be consenting to.

The ABA supports a clear and concise industry consent regime that makes customers aware of what their rights are. The ABA also notes that further consultation is required with consumer groups to ensure that the specific needs of vulnerable customers are considering when designing the consent regime. We also support the ACCC's proposal that consumer comprehension testing of the consent regime take place.

The ABA also calls for Government to lead with industry on a comprehensive customer education around equipping customers with the tools and resources to help them avoid potentially unsafe data sharing activities, such as disclosing their log-ins and password credentials to third parties.

8.3 Consent provided to accredited data recipients

The ABA supports the principles that the ACCC proposes to make Rules to the effect that an accredited data recipient "must obtain a consumer's consent to collecting and making use of specified data, for specified purposes and for a specified time."

Deletion of data

The ABA recognises a customer's right to deletion under the privacy safeguards. As stated above, the ABA believes entities that have had accreditation revoked should be required to delete data given they are unable to safely store the data.

But in the case of CDR participants, the ABA notes there are many complexities involved regulating a right to deletion. These include legal obligations on banks to retain records, the fact that individuals currently have no right to deletion of their personal information under the Privacy Act and the technical difficulties associated with deletion. Rather, APP 4 grants an entity the option to de-identify or destroy

data, which recognises the technical challenges that arise from destroying data. We believe that this option should remain for those entities that remain accredited.

Australian Banking Association

9. Authorisation and authentication process

Summary of proposed Rules

The ACCC proposes to make Rules to the effect that:

- the standards must include standards in relation to authorisation, and that authorisation processes for CDR data must occur in accordance with the standards.
- data holders must clearly communicate to consumers what they are authorising the data holder to do, and provide specified information to consumers as part of the authorisation process.
- authorisation standards must:
    - be subject to consumer testing, consideration by the Data Standards Body's user experience consultative group, and meet certain service level requirements.
    - provide for multi-factor authentication requirements consistent with the requirement for strong customer authentication under PSD2 and the European regulatory technical standard for strong consumer authentication under PSD2 (RTS).
    - provide for the ability for a consumer to grant authorisation for a specific, once-off request, Consumer Data Right Rules Framework 40 or authorisation that persists over time. In terms of persisting authorisations, the ACCC proposes to make a rule that will limit the period of authorisations to 90 days. The ACCC proposes to make a rule that re-authorisation will then be required if the accredited data recipient seeks continuing access to the consumer's data, though this may be via a simplified process.
    - specify permissions for applications to access data. The ACCC does not propose to specify the nature or level of 'granularity' of those permissions in the first version of the Rules. However, the ACCC proposes to make a rule that the Data Standards Body continue to pursue delivery of more finely-grained authorisations.
- data holders should not add requirements to authorisation processes beyond those specified in the standards, or offer additional or alternative services to the consumer or request additional information beyond that described in the standards during and as part of the authorisation process.
- data holders must collect and maintain records and report on API performance, including response times against minimum service level benchmarks set out in the standards.
- data holders must have a system in place which allows consumers to readily manage their authorisations and consumers should be able to withdraw authorisations at any time.

The ACCC is also considering whether the Rules should specify certain service level standards for the authorisation and authentication processes, or whether this is best addressed by the technical standards, and welcomes submissions on this issue.

ABA Response

We note that there are exemptions in place for Strong Customer Authentication (SCA) in PSD2. Clarification would be useful regarding the intended approach to SCA under the Rules.

9.4 Authorisation and authentication model

"This could take the form of a re-direct flow with multi-factor authentication."

ABA members believe that data providers should be allowed to innovate around variants of the redirect or decoupled approaches using newly proposed FAPI / CIBA standards.

9.5 Duration of authentication

We note that it is proposed that reauthorisation may be a simplified version of the process initially undertaken. The concept of a simplified re-authorisation could lead the consumer to "automatically" renew the initial data sharing consent, possibly without having the opportunity to fully review the terms and conditions of the consent and data sharing arrangements. Therefore ABA members believe that once a consent is expired the consumer should be asked to re-start the authorisation process.

9.9 Revocation of authorisation

"Consumers will be able to end a data sharing arrangement through either the data holder or accredited data recipient."

On this topic, we propose that revocation of authorisation is performed on the same channel where authorisation was granted in the first place. That is, on the Data Holders' consumer dashboard. From a security perspective, this provides:

a) a consistent approach to the consumer and assurance that the consent is truly terminated (at the origin where it was originally granted);

b) It eliminates the need for data holders to expose an API with right/delete access for consent revocation, improving the security posture by reducing the landscape for security vulnerabilities.

"If a consumer revokes an authorisation via the data holder, the data holder must notify the accredited data recipient and any intermediary."

The concept of intermediaries, their roles and responsibilities need further definition. Where an intermediary becomes a TPP that is used as a proxy by fourth parties - the proxying of consent revocation from the bank to the intermediary and then to the fourth party (a TPP with lower level data access privilege) introduces technical complexities and potential security issues. To simplify the solution we suggest that Data Holders should always have a one-to-one relationship with a TPP and avoid the complexities of a daisy-chained consent model.

White-labelling

In the case of white-labelling — that is where a bank has outsourced a product such as a credit card — the authentication (credential) may reside with the provider. This would imply the provider needs to manage consent. In addition, in some instances, the provider uses federation for login and the bank manages authentication. Several ABA members seek further discussion on how these arrangements could be handled.

Australian Banking Association

10. Providing consumer data to consumers

Summary of proposed Rules

The ACCC proposes to make Rules that require data holders to:

- provide consumers with the ability to make requests for direct disclosure of their CDR data in a manner that is timely, efficient and convenient.
- allow consumers to nominate specific CDR data as part of their request, consistent with the data standards that will specify the product descriptions and information taxonomy.
- disclose the requested CDR data to the consumer in a variety of electronic formats, as provided for by the Data Standards Body, potentially at the election of the consumer.

The ACCC welcomes views about the specific rights and obligations that should be imposed to give effect to the right for a consumer to directly access their CDR data from a data holder.

ABA Response

The ABA supports a customer's right to request their CDR data of the data holder.

We would support that this data is delivered by a file download direct to consumer data sharing rather than through APIs in order to protect customer's security.

Further consultation is required with consumer groups to fully understand issues this may pose as far as security as well as potential for predatory behaviour if the customer chooses to then pass this data along to a third party directly.

Australian Banking Association

11. Making generic product data generally available

Summary of proposed Rules

The ACCC proposes to make Rules that will require data holders to make generic product data available via an API in accordance with standards made by the Data Standards Body.

ABA Response

The ABA supports this Rule.

12. Use of data

Summary of proposed Rules

The ACCC proposes to make a rule requiring accredited data recipients to identify to a consumer the uses to which the consumer's CDR data can be put, and obtain express consent to specific uses according to the consumer's wishes.

The ACCC proposes to make a rule requiring that CDR data can only be used in accordance with the consumer's express wishes, as governed by the consent process.

The ACCC proposes to make Rules requiring accredited data recipients to transfer data to a non-accredited entity if directed by a consumer and with their specific express consent, after notifying the consumer that the entity is not accredited and disclosure is outside the protections of the CDR system.

The ACCC proposes to make Rules which would allow an accredited data recipient to disclose data to an outsourced service provider, provided the outsourcing arrangement is disclosed to consumers during the consent process and other obligations relating to outsourcing are complied with. The ACCC is also considering other Rules in relation to this scenario to limit the increased risk to consumers' data, and welcomes stakeholder views on this issue.

The ACCC welcomes stakeholder comment on a model based on use of an intermediary, to assist in determining to what extent the utility of the CDR would be limited without the ability to operate in this way.

ABA Response

12.1 Disclosure of consumer data to other parties

ABA members strongly oppose data holders being directed by customers to share CDR data to non-accredited entities, as outlined in section 12.1.1 through until 12.1.3.

The ABA notes that data sharing should be allowed to occur outside of the CDR.

But this data sharing should not be solely customer directed, given customers are not equipped to assess the risks associated with a non-accredited third parties. Customer-directed data sharing outside of the CDR should only take place against a backdrop of a bilateral agreement between the data holder and the data recipient, where the data holder has ensured that the security, privacy and liability protections will protect the customer's data. Existing arrangements between banks and accounting software providers are examples of this type of data sharing that should continue to take place outside of the CDR.

Australian Banking Association

13. Rules in relation to privacy safeguards

Summary of proposed Rules

A number of proposed Rules in other sections of this framework will build upon and give effect to the privacy safeguards. For instance, Rules in relation to consent, authorisation and use of CDR data will give effect to privacy safeguards on data collection, use and disclosure, and notification.

The ACCC also proposes:

- in relation to privacy safeguard 1, to make Rules to the effect that the CDR participant must make the policy about its management of CDR data available via its website and mobile app, in a readily accessible location and provide a copy of the policy to consumers electronically or in hard copy if requested.
- in relation to privacy safeguard 2, to make Rules to the effect that the use of a pseudonym by a consumer is prohibited for Open Banking.
- in relation to privacy safeguard 9, to not make Rules to provide exceptions to the prohibitions relating to government related identifiers (GRI) in the initial version of the Rules.
- in relation to privacy safeguard 10, to not make Rules in relation to the quality and accuracy of data in the initial version of the Rules.
- in relation to privacy safeguard 13, to make Rules to the effect that the steps the relevant persons should take should be in accordance with the steps outlined by the OAIC in relation to APP 13.

In relation to privacy safeguard 4, the ACCC welcomes stakeholder views on scenarios that may need recognition in the Rules in relation to unsolicited data.

ABA Response

The ABA believes that the dual system of APPs and CDR Privacy Safeguards poses significant challenges to data holders, data recipients and customers. Dual systems create uncertainty around the obligations and responsibilities borne by data holders and data recipients, but more importantly, the likely confusion that will be faced by consumers when seeking to understand their rights.

Some specific issue relating to the Rules framework proposed by the ACCC are discussed here.

- **Privacy Safeguard 6 – Use or disclosure of CDR data**

ABA members believe Privacy Safeguard 6 places a restrictive scope of permitted disclosure.

PS 6 permits an entity to disclose CDR data only if permitted by the Rules, even if the consumer has provided a valid consent. Limiting the use of CDR data to where such specific active consent has been obtained will effectively require banks to build and maintain separate structures to hold and maintain data.

- **Privacy Safeguard 7 – Prohibitions on on-selling and direct marketing**

ABA members believe that direct marketing using CDR data should be allowed provided express, specific and informed consent has been given.

PS 7 outlined in Treasury's exposure draft enables the use of CDR data for direct marketing only when permitted by the Rules and where a valid consent has been provided in accordance with the Rules. However, the ACCC state that direct marketing is prohibited under the Rules. This is stricter than APP 7, which allows for direct marketing, provided the customer is given an opportunity to opt-out of their data being used for marketing.

- **Safeguard 8 – Cross-border disclosure of CDR data**

Requiring all CDR data recipients to be accredited, as outlined in Privacy Safeguard 8, poses issues for those banks that use outsourced service providers, including those that are domestically based but with offshore support.

ABA support the ACCC's requirements that outsourced providers be subject to minimum safeguards. We believe that these safeguards should provide a stringent framework that protects customers' data but also enables for the possibility that data may be accessed offshore.

14. Reporting and record keeping

Summary of proposed Rules

The ACCC proposes to make Rules requiring CDR participants to keep and maintain records relating to the participant's compliance with the privacy safeguards, the Rules and the standards for a period of six years.

The ACCC also proposes to make Rules requiring CDR participants to keep and maintain information about complaints for a period of six years and to provide regular reports of this information to the ACCC and the OAIC.

The ACCC also proposes to makes Rules requiring accredited data recipients to notify the Data Recipient Accreditor of material changes in circumstances relevant to their accreditation.

ABA Response

The ABA supports these Rules.

Australian Banking Association

15. Dispute resolution

Summary of proposed Rules

In relation to internal dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants have in place internal dispute resolution procedures that comply with the requirements specified in the Rules.

In relation to external dispute resolution, the ACCC proposes to make a rule requiring that all CDR participants be a member of the external dispute resolution scheme recognised by the ACCC for Open Banking. The ACCC proposes to recognise the Australian Financial Complaints Authority (AFCA).

In relation to complaints by larger businesses or disputes between CDR participants, the ACCC does not intend to make Rules relating to alternative dispute resolution in these situations in the first version of the Rules. However, the ACCC welcomes stakeholder views on this issue.

ABA Response

The ABA supports AFCA's role in the CDR as well as mechanisms for internal dispute resolution.

We also support not making Rules relating to alternative dispute resolution in relation to complaints by larger businesses at this stage.

Australian Banking Association

16. Data Standards Body

Summary of proposed Rules

The ACCC proposes to make Rules that set out the process by which standards are developed by the Data Standards Body, including specified principles for developing standards to which the Data Standards Body must have regard and requirements that draft standards be publically available for stakeholder testing and feedback.

The ACCC proposes to make Rules that require the Data Standards Chair to review the operation of a standard where directed to do so by the ACCC, and Rules that facilitate urgent or purely technical changes to the standards being made without undertaking the usual consultation processes.

The ACCC proposes to make Rules that require the Data Standards Chair to establish and maintain at least one Advisory Committee, as well as a consumer experience consultative group.

ABA Response

ABA supports the ACCC's Rules on Data Standards Body and the Advisory Committee.

ABA members support the ongoing maintenance of the advisory committees, and believe that each industry involved in the CDR should have its own advisory committee to advise on industry-specific issues.

ABA members support the introduction of the consumer experience consultative group, and believe this work should begin as soon as possible on customer education on open banking.

ABA members support the principles for guiding the development of the technical standards.

Australian Banking Association

About the ABA

With the active participation of 24 member banks in Australia, the Australian Bankers' Association 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 to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.