AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

12 October 2018

ARCA submission on the ACCC Consumer Data Right Rules Framework

Thank you for the opportunity to provide a submission on the Consumer Data Right Rules Framework.

The Australian Retail Credit Association (ARCA) is an industry association with the objective to promote both the integrity of the credit reporting system and best practices in credit management, enabling better lending decisions. In respect to the 'credit reporting system', this includes the system as established under *Part IIIA* of the *Privacy Act* (Part IIIA) and also the broader range of data available to credit providers to assist with credit management.

The Consumer Data Right (CDR) and, in particular, the Open Banking regime will provide credit providers access to additional sources of data that will support better credit risk and responsible lending decisions.

Our submission is separated into two parts:

(i) Standardised use cases – see Appendix 1, and
(ii) General comments on the Rules Framework – see Appendix 2.

Our comments on Standardised use cases propose a new concept to be introduced in respect of the CDR, which we believe with have significant benefits for consumers, accredited persons and regulators. Our General comments provide our feedback to the issues raised in the Rules Framework.

In our submission to Treasury in respect of the second stage consultation on the CDR Bill and draft Designation Instrument we identified a number of interactions between the CDR and the credit reporting system established under Part IIIA. In that submission we have suggested several changes to the CDR regime to ensure the regimes complement each other. We have further recommended that those changes be reflected in the Bill, however, we note that Treasury may elect to defer some of the issues to the Rules. For your reference, we included a copy of our submission to Treasury as Appendix 3.

If you have any questions about this submission, please feel free to contact me or Michael Blyth.

Yours sincerely,

Mike Laing
Executive Chairman

Appendix 1 - The need for standardised use cases, including consents

The CDR is expected to bring increased competition and innovation to the Australian economy by allowing consumers to give businesses access to their data in a secure and convenient manner. Such data should allow both existing and new businesses to develop innovative products and services – types of which are not even currently contemplated.

However, it must be recognised that there are already uses for CDR data that are well known, high-value and common to many businesses. Using Open Banking data for risk and responsible lending purposes is one of the clearest examples of such uses.

Risk and responsible lending use cases involve lenders obtaining a better understanding of a customer's existing financial situation prior to providing credit and in the subsequent management of that credit. That is, the data is used in processes that help to ensure that providers lend responsibly, the prudential strength of Australia's authorised deposit-taking institutions is maintained, and that credit is made available on competitive terms to those who need it.

Community and regulatory expectations of credit providers when assessing a customer's suitability to be granted credit, and in the subsequent management of that credit, are clearly increasing. This has most dramatically been shown through the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry where the need to enhance responsible lending, and the importance of using data specific to an individual borrower, have been key take outs.

Financial services regulators have already imposed additional obligations and expectations that will require lenders to have, and use, better data about the customer.

For example, in ASIC's recent work on credit cards, the regulator has:

- Expressly stated its expectation that lenders develop tools to help consumers choose credit cards that reflect their actual needs and use – where Open Banking will provide the data used in the tool. See Issue 6, Report 580 *Credit card lending in Australia* (REP 580).
- Imposed an expectation on lenders when assessing *all* consumer credit applications to assume a higher repayment amount on existing credit cards, such that the payments would repay the full credit limit within three years. To do this assessment properly, the credit provider would need to understand the features, particularly interest rates, of those other products. See Report 590 *Response to submissions on CP 303 Credit cards: Responsible lending assessments* (REP 590) [1]
- Highlighted the problems with consumers using a balance transfer offer on a new card to pay off old debt but failing to close the old card – such that the consumer's overall

[1] This assessment will require credit providers to have a verified understanding of the limit of the credit card, the applicable interest rates and how those rates apply. In REP 590 , ASIC notes that it is appropriate to use an assumed rate, rather than the actual rate. This does not recognise that some lenders' rates are significantly higher than the assumed rate. This assumption may also have a distorting impact on competition as a lender that holds the credit card (and who will have actual information about the card) may be able to offer higher credit limits on other credit facilities (i.e. if the credit card rate is less than the industry assumed rate). To properly make the assessment suggested by ASIC, lenders will need to have actual data about the customer's other credit cards.

indebtedness increases. To address this risk, credit card providers would need to have a better way of understanding whether the old card has been closed. See, for example, Findings 7 – 8, REP 580 which discussed the risk of balance transfer creating a 'debt trap'.

Consent as a precondition of the provision of a service

Considering their risk and responsible lending obligations, lenders will make consent to access Open Banking data conditional on making an application for credit. This *is* consistent with the Rules Framework principle that consent should be 'freely and voluntarily' given, despite the fact refusal to provide consent is likely to inhibit a consumer's ability to access credit from lenders. This is consistent with the approach taken in the United Kingdom, which has similar provisions to those proposed in Australia, such that any consent that is conditional on the provision of the service must be restricted to only that data necessary for the provision of the service.

Given the CDR framework is based on a consent model it is a tautology that businesses will require consent as a precondition for a service to be provided. The question is then whether the consent is 'related to' the service being provided.

In most cases it is likely that the question of whether the consent is related to the service being provided is reasonably clear. Where those cases are common across accredited data recipients, it makes sense to standardise the approach (including consents) to those uses. This provides benefits to consumers, data recipients, and also the regulator.

Standardisation would also benefit situations where the delineation between what is acceptable and what is not may be unclear. For example, if a customer applied to Bank A for a home loan of $500,000, would it be permissible to use the data obtained for risk and responsible lending purposes to offer a limit of $520,000 – where the extra $20,000 was to refinance an existing credit card with Bank B? Could the use of the data for that assessment be bundled with the overall consent, or should it be a separate consent – which cannot be presented as a condition of applying? We note that Part IIIA, which regulates credit reporting, would not permit the use of credit reporting data for such a purpose. As noted above, in the absence of a standardised approach, this will require significant regulator oversight.

Hence, standardisation would have benefits for regulators, in that they could be confident that common uses of open banking were consistent with the rules, and they would need to spend less resources on monitoring data recipients using the standard approach. Standardisation would also have advantages for data recipients, in that they could have confidence that their consents and practices will be treated as consistent with the Rules.

Consumer impact

Standardisation of use case and consents across industry participants for some purposes will have significant benefits for consumers, who will not be required to interpret differing consent requests for potentially identical services from different service providers.

While many stakeholders have identified the need for an effective consumer education program on the benefits, risks and responsibilities arising from participation in the CDR regime (see Farrell review, p100), it must be recognised that existing levels of financial literacy in Australia

are low. The Farrell review noted that, "[w]hile Open Banking is a simple concept … there are a number of complex aspects" (p.100). We believe that this statement understates the difficulty in conducting an effective consumer education campaign. The Open Banking concept is *not* a simple concept for many Australians. ARCA's own experience in undertaking a consumer education campaign in respect of comprehensive credit reporting has demonstrated the challenges in trying to inform and educate the Australian public about changes to the way consumers' data is managed. The Australian public – often fuelled by critical media coverage - has a long history of treating changes to the way their data is handled with suspicion. This has also been recently demonstrated by the attention given to the introduction of My Health Record.

Given the complex ways in which data recipients will want to analyse and use data, there is a high likelihood that many consumers won't understand the process and – contrary to the expectation set out in the Rules Framework – will be surprised by how their data is being used. Of course, given the broad range of potential uses for CDR data – many of which are currently unknown – there will invariably be some trade-off between consumer understanding and innovation.

However, this simply increases the need to ensure that for use cases that are common across many providers every effort is taken to remove complexity and ensure transparency – particularly as those types of use cases are more likely to be a consumer's first introduction to the sharing of their data under the CDR.

Given the above, we believe that in order to maximise consumer acceptance and engagement with the services that might be created through Open Banking, it is imperative that the Rules contemplate the creation of 'standardised use cases'. Such use cases would, for Open Banking, include the mattes set out it Table 1. In some cases, it may also be appropriate for such standardised use cases to apply the Privacy Safeguards in a manner that is specific to those use cases.

To be clear, we are not suggesting that the creation of standardised use cases limit the circumstances in which an accredited person can access CDR data through a separate unique consent defining the types of data accessed and the uses to which that data is put. Rather, it will provide a set of default uses where stakeholders – government, CDR regulators, financial services regulators, industry representatives and consumer representatives – have agreed that it is appropriate to develop certain protocols based on the types of data accessed and the purposes for which it is used.

Even where the standardised use case is established, we expect that it may be possible for an accredited person to go beyond the use case by *explicitly and clearly* advising the consumer prior to obtaining additional consents.

Standardised use cases will benefit consumers, accredited persons, data holders and regulators by establishing some well-known, controlled forms of data sharing. We believe that a key benefit of the standardised use cases would be to make it possible to have simplified and consistent consents.

This is particularly important in relation to risk and responsible lending use cases as there is a high likelihood that many consumers' first interaction with the Open Banking regime will be when they apply for credit and the lender seeks consent to verify data through the framework

(see the examples in Item 1 of Table 1, below). Ensuring those consents are simple and straightforward – and consistent between lenders – will increase the chances of successful adoption of the Open Banking regime by the public.

The technical approach to enabling open banking also supports the need to develop standardised use cases

It is our understanding that the initial data standards are being developed based on 'coarse-grained' authorisation, which will grant access to a broad data set. This means that an accredited data recipient is likely to receive data that goes beyond what is needed for the provision of the service. For example, a lender may need to understand the value of a consumer's spending to verify the consumer's general expenses when assessing a loan application. To make this assessment, the lender may need to know the value, type and date of a transaction, without needing to know the merchant's name (which may, depending on the consumer's spending habits, include highly sensitive information).

From a privacy perspective, granting access to data that is not needed is not appropriate. Further, lenders are subject to significant compliance risk if they do not use data in their possession in a responsible lending assessment. This risk will increase if Open Banking delivers additional data sets that a lender is not capable of using in those assessments (noting a lender's practices are continually evolving and that it is not possible for a lender to update their practices as soon as they get access to numerous new data sets).

A further benefit then of a standardised use case would be to define which data sets should, by default, be deemed redundant as soon as they are received (again, without limiting what can be done on an exception basis).

Table 1 - What would a standardised use case look like?

We expect that the standardised use case would establish the following matters.

Use case content	Comment
1. The purpose for which the CDR data is being obtained	Ideally, the purpose would include a level of granularity. For example, the purpose should not be simply described as 'assessing your application'. Instead, it should be in the form of, for example, 'verifying the value of income'. Some examples of risk and responsible lending uses cases include: • Verifying the value of income • Verifying the value of living expenses • Verifying the value of existing debt obligations, including outstanding balances • Verifying the payment history in respect of existing debt obligations, including payment amounts, due dates and payment dates • Providing a customer a tool to assess credit card actual needs and use (see Issue 6, REP 580) • Understanding obligations on existing credit facilities – credit cards (see REP 590) • Understanding obligations on existing credit facilities – fixed vs variable; balloon payments etc • Verifying the closure of a refinanced loan (see REP 580) • Assessment prior to progressive drawdown on a construction home loan • Ongoing risk assessment of the loan portfolio tied to the ongoing provision of the loan or to a discount or other feature of the loan.
2. The types of data that will be obtained by default – without limiting the additional data that may be specifically requested by the authorised data recipient	The types of data should be limited to what is necessary for the purpose. As noted above, this could also designate what data should be deemed as redundant immediately as it is not necessary for the purpose (that is, data received under the coarse-grained authorisation but which is not needed).
3. How CDR data may be used and disclosed.	This would set the boundaries for how data could be used or disclosed under the standardised use case.

Use case content	Comment
	In respect of the example given above, the use case could establish whether the lender could use the data to 'upsell' the customer to the $520,000 loan. Again, if the use case did not contemplate the use of the data in this way, the lender would be required to obtain a separate consent. In the case of risk and responsible lending use cases, we note that it may be appropriate for certain use and disclosure purposes, that go beyond the main purpose, to be permitted either by default (i.e. a form of permitted 'secondary' purpose) or using a simplified form of express consent. For example, the proper operation of a lender's risk and responsible lending practices, and its broader credit business, may require the lender to use and disclose the data in circumstances that go beyond the main purpose of obtaining the data to, for example, verify the consumer's disclosed income. This could include: • Disclosure to securitisation entities, providers of lenders mortgage insurance or prospective guarantors • Use of the data to assess the performance of the lender's risk and responsible lending processes. Such examples of use and disclosure are recognised as necessary and appropriate in Part IIIA. In respect of the second point, this process is consistent with ASIC's expectation that a lender regularly monitor and review its use of systems and tools that are used to satisfy its responsible lending obligations (see RG 209 *Credit licensing: Responsible lending conduct*). Likewise, ADIs are expected by APRA to regularly review their credit risk management systems (see Prudential Standard APS 220 *Credit Quality*). If, under the consumer data rules, a lender was required to obtain explicit consent for each of these forms of use, the form of consent presented to the consumer would be complex and lengthy. Providing for a standardised use case with standardised consents would enable such consents to be simplified. We note that the Rules Framework proposes that a withdrawal of consent would require an accredited data recipient to treat any data already received as redundant. We have set out of concern regarding this in our General Feedback (see our comments in respect of Section 13 *Rules in relation to privacy safeguards*). However, if this is to be accepted as a principle, the standardised use cases could identify specific exceptions to this rule where it is necessary for the proper operation of a business. For example, as noted

Use case content	Comment
	above, Part IIIA recognises that a lender may use data obtained through the credit reporting system to assess the performance of their risk and responsible lending practices (this is permitted based on the 'internal management purposes' use; see s21H of the Privacy Act).
4. The form of customer consent required.	A benefit of standardised use cases would be the ability to have simplified consents as the parameters for use and disclosure would be established in the use case. Additional consents would only be required by exception if the CP wanted to go beyond the standardised use case. We note the Rules Framework suggests that consumers should not cross-reference other documents (p.36 Rules Framework). We set out our comments in respect of this in our General Feedback (see our comments in respect of 8.3 *Consent provided to accredited data recipients*). In respect of standardised use cases, we consider that it is appropriate to be able to have a simplified form of consent presented to the consumer, while allowing the limited number of consumers who want more detail to be able to obtain that detail by a straightforward click-through – particularly where the parameters of the use cases have been recognised by relevant regulators (which, for risk and responsible lending purposes, would include the financial services regulators). For example, where data was obtained for a specific risk and responsible lending purpose, it would be appropriate to obtain consent to use the data for 'purposes related to optimising the lender's responsible lending practices' (i.e. a simplified description), while also giving the consumer the opportunity to understand more about those purposes on an exception basis (again, noting that those other purposes would be established under the standardised use case with input from stakeholders, including regulators).
5. The implications of the customer not giving or withdrawing consent prior to the data has been obtained. Subject to our General Feedback on Section 13 *Rules in relation to privacy safeguards* – the implications of the	The withdrawal of consent - either prior to the data being obtained or, if the Rules require the data to be deemed redundant, after the data is obtained - will impact on the consumer's ability to be offered, or to continue to be offered, the product or service. In respect of the provision of a credit product, the following are some potential implications:

Use case content	Comment
customer withdrawing consent after the data has been obtained.	• Can a lender accept a credit card application if the consumer does not use the tool described in Issue 6 of ASIC's REP 580? • If a consumer obtains a balance transfer to pay out and close a credit card with another provider, what happens if the consumer withdraws consent before the credit card provider can confirm that the account has been closed? Would this place the consumer in default of their credit contract? Would it allow the credit provider to revert the balance transfer amount to a higher interest rate? • If a customer has a construction home loan that requires progressive payments (based on the stage of the building's completion) and the lender verifies the customer's financial situation prior to each drawdown using CDR data, what happens if the customer withdraws or fails to renew their consent? Can the lender refuse the drawdown? Can the lender place the loan in default? • If the lender offers a discount based on the customer providing ongoing consent to access CDR data, does the withdrawal of consent (or failure to renew consent) allow the lender to remove the discount? The unfair contract terms and credit legislation may limit the ability of the credit provider to take certain action, however there is still the potential for consumers to be significantly and negatively impacted by the withdrawal or failure to renew consent. It is appropriate that stakeholders – including financial services regulators – agree on parameters in respect of the withdrawal or non-renewal of consent.

Appendix 2 - General feedback on the Rules Framework

Rules Framework reference	Comment (and recommendation)
3. CDR consumer – who may take advantage of the CDR	1. **CDR consumer**: a. The Framework is not clear as to whether the concept of consumer is intended to include non-account holders, such as credit card additional card holders. b. We recognise that priority should be given to delivering Open Banking in respect of current, online customers. However, we note that there is a risk that the exclusion of closed accounts could reduce the benefits of Open Banking data for risk and responsible lending purposes and permit some consumers to game the system (e.g. by closing accounts that may demonstrate poor payment behaviour). We suggest that this concern be considered when assessing when data holders will be required to make data available in respect of former customers. 2. **Former customers** – the Framework is not clear as to whether this is assessed at the customer or account level. For example, if a customer has two products – a credit card and transaction account – but then closes the credit card but keeps the transaction account open. Will the bank be required to give access to the credit card? 3. **Offline consumers** – will a bank be required to give access to a particular account, which is not viewable through internet banking, if the customer otherwise is an 'online' customer (i.e. they have other accounts that are viewable through internet banking)?
5.2 Derived data	4. We note that Treasury has proposed changes in relation to the definition of 'CDR data' such that only data within the Designation Instrument is subject to the access regime – while the privacy safeguards and other protections will apply to both the data accessed and data that is derived from that data. Nevertheless, to the extent that the draft Designation Instrument leaves open the scope for derived data to be included in the access regime, we propose the delineation exclude data that results from analysis that includes inputs, calculations or outputs that are derived from data that aggregates or summarises data from multiple customers. This would include, for example, a credit score created by a lender.

Rules Framework reference	Comment (and recommendation)
5.3 Data sets	5. **Transaction data** – We understand that data standards being developed by Data61 will largely deliver the transaction data that is available to account holders through internet banking. If this is the case, we expect that this will deliver a useful data set to lenders for risk and responsible lending purposes. Nevertheless, knowing what transactional data is required is dependent on an understanding of the likely use cases. We recommend that the ACCC and Data 61 conduct further workshops to identify the likely use cases in more detail and is the data that is required for those uses. Those workshops should have representation of those who are making the data available (i.e. major banks, other ADIs – subject to reciprocity) and the likely users of that data. 6. **Product data: account level information** – We note that product data in relation to a consumer's existing obligations is a valuable data set for a lender's responsible lending assessment. Such data allows the lender to better understand the extent of a consumer's existing liabilities – both the value of those obligations and the consumer's repayment obligations. The consumer's existing repayment obligations will impact whether the consumer can repay the new loan without substantial hardship and care must be taken to ensure that the data delivered through Open Banking shows the complete picture of those obligations. For example, it is not simply a matter of knowing that the customer's existing repayment is $X per week – the new lender should ideally know whether that amount can change. To do this, the lender would need to know whether the interest rate was fixed or variable; if variable, whether it is subject to a honeymoon rate or a discounted rate that may change (including the terms that apply to such changes); and, whether the loan subject to a large balloon payment at the end (which would require the customer to have access to a lump sum). In APG 223 – *Residential Mortgage Lending*, APRA (p.12) notes that a sound serviceability assessment model applied to a residential mortgage borrower would include consideration of any existing and ongoing debt commitments and that "good practice is that ongoing serviceability would not rely on longer-term access to 'honeymoon' or discounted introductory rates". Accordingly, it is not simply a matter for the lender to understand the interest rates on the consumer's existing debt obligations, but also whether those rates are likely to increase. Likewise, we note that an important user of Open Banking data will be fintech lenders who often find themselves refinancing debt from larger lenders. To understand whether the refinancing deal being offered to a consumer – and to comply with their responsible lending obligations – the

Rules Framework reference	Comment (and recommendation)
	fintech lender would need to understand the true cost of the existing obligations being refinanced (if the customer's requirements and objectives involved 'saving money'). This is often not simply a matter of knowing the interest rate and fees as the lender would ideally have access to data regarding the terms applicable to those rates and fees (e.g. is the rate a honeymoon rate or dependent on a 'package' discount; are there fees for paying out the existing loan etc).
5.4 Reciprocity	7. We agree that the principle of reciprocity does not require a 'quid pro quo' arrangement as described in the Rules Framework. The principle of reciprocity, as it applies to credit reporting under the Principles of Reciprocity and Data Exchange, can be broadly described as requiring an entity, which benefits from accessing consumers data held by another entity, to make their own consumer data available through the system (subject to whatever preconditions apply) – this is at the organisational level, not on a customer-by-customer basis. Treasury has proposed changes to the draft Bill that clarify the principle of reciprocity and how it could operate. In Treasury's document *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation*, three examples are given of the application of reciprocity. The first two examples relate to entities that operate within the financial services sector (and offer products of the same type as in the designation) and which could be subject to a reciprocity requirement if they choose to access CDR data through Open Banking; (i) 'equivalent data – designated entity', and (ii) 'equivalent data – not designated entity'. Imposing an obligation of reciprocity on entities covered by these two examples will ensure that more consumers (i.e. the customers of those entities subject to the reciprocity requirement) will be able to enjoy the benefits of the Open Banking regime. The third example in Treasury's document involves requiring data recipients to give access to data received under the CDR. We have previously provided feedback to Treasury that such a requirement should be treated with caution given that it would require the sharing of 'second-hand' information – where it would ordinarily be better to require the original data holder to share the information.

Rules Framework reference	Comment (and recommendation)
	Reciprocity is a key principle embedded into most data sharing arrangements. The requirement for reciprocity is seen as essential to create incentives for participation and to ensure fairness between participants. Ultimately, maximising the amount of data in the system and maximising competition between participants ensures that benefits to consumers are maximised. We consider that it is appropriate to impose a reciprocity obligation on entities that hold 'equivalent data' if they choose to participate in Open Banking – this will ensure that the benefits of Open Banking are available to customers of more financial institutions. Experience in other data sharing regimes such as credit reporting indicates that the size of the task and investment required to consume data is substantially greater than the challenge and investment required to supply data into the system – hence if an entity seeks to become a data recipient in open banking the burden of a reciprocity obligation may not be great. The ACCC's decision on whether to impose reciprocity for open banking should be made after testing this assumption.
6.2 Proposed rules for accreditation model and criteria	8. **Lower accreditation levels** – We note the proposal to permit a lower level of accreditation if a data recipient will hold only limited forms of consumer data. We agree that such lower levels of accreditation may be appropriate where the data recipient holds only derived CDR data that does not allow the identification for individual consumers. However, we caution whether it is appropriate to allow such lower standards for data recipients holding any data for identifiable consumers. We note that the Farrell review identified 'account balances' as potentially a type of data set that is lower risk (p25, footnote 41). We respectfully disagree with this view – noting that such data is a valuable type of data and that the Part IIIA specifically excluded balance from being available through the credit reporting system. For example, we note that balance information can be used by banks as part of their customer identification processes for telephone banking. Our view would be that all data recipients receiving data relating to and identifiable for an individual consumer should be subject to identical levels of accreditation.
6.3 ADI accreditation	9. We agree that there should be a streamlined accreditation process for ADIs that are specified by the rules to be data holders. However, we recommend that the ACCC assess whether it would be

Rules Framework reference	Comment (and recommendation)
	appropriate to provide a simplified form of accreditation for certain other entities such as holders of an Australian Credit Licence with a 'credit provider' authorisation which are also a registered finance corporation under the *Financial Sector (Collection of Data) Act*.
6.8 Accreditation and outsourcing	10. ADIs are already subject to detailed APRA obligations in respect of outsourcing of material business activities – see Prudential Standard CPS 231 Outsourcing which requires that all such arrangements are subject to appropriate due diligence, approval and ongoing monitoring. While this Prudential Standard mandates the requirements only in respect of material arrangements, it is common practice for ADIs to apply relevant policies and procedures to all outsourcing arrangements. We recommend that any Rules made in respect of include a recognition that policies and procedures developed by ADIs to comply with CPS 231 – and which are applied to all outsourcing arrangements – will satisfy those rules.
6.9 Security obligations	11. As with Outsourcing, we recommend that, if entities are already subject to APRA prudential standards relating to Information Security, compliance with those requirements should be deemed compliance with the Rules.
8.1 Who can provide consent?	12. **Joint accounts:** a. As we have previously noted in response to the Farrell review, we are unclear as to the reason why the ability to give consent in respect of a joint account is being tied to the ability to authorise a transaction on the account, rather than to a joint account holder's ability to *view* account information. It is important to note that, while a transaction completed on the account by one account holder will deny the other account holder of those funds, the transfer of data authorised by one account holder does not prevent that other account holder from also authorising the sharing of that data. Further, if an account is 'both to operate' either account holder may still share a PDF copy of their statement, (subject to the bank's functionality) download a CSV or other readable format file of their transactions or supply their log-in credentials to allow a screen-scraping service to access the data. – The ability for one joint account holder to share data through the Open Banking system does not, at least if it is limited to information available on statement and through internet banking, impact on the privacy of the other joint account holders. As noted by the

Rules Framework reference	Comment (and recommendation)
	Farrell review, a key measure of success of Open Banking is how other methods of data sharing are actively used (see Recommendation 1.1). Linking the Open Banking regime to the account holder's ability to transact will place the regime at a disadvantage to those less secure means of sharing account data. b. We are concerned with the suggestion that the joint account holder may be notified of any data transfer and be given the ability to readily terminate any data sharing arrangement initiated by other joint account holders. Such a proposal appears to be inconsistent with protecting the privacy of the account holders. For example, an account holder may elect to share their data with an intermediary which passes that data onto a family law firm. Notifying the other account holder of that sharing is likely to put that account holder on notice that the first account holder is seeking advice regarding their marriage or other sensitive personal matters. Even if the data sharing is with a credit provider, this will give the other account holder notice that their joint account holder is seeking finance. This is not consistent with protecting the privacy of individuals. Secondly, giving the power to a joint account holder to terminate a data sharing arrangement authorised by the other account holder, gives that account holder the power to terminate the other account holder's acquisition or use of a service that is dependent on that Open Banking data being shared. In the family law example above, the joint account holder could interfere in the other account holder's ability to seek legal advice (or, at least, force the other account holder to share their data in a less secure manner). c. We recommend that the proposed treatment of consent and authorisation on joint accounts be reconsidered. The starting point – at least for less complex forms of account ownership, such as with most consumer accounts – should be that an account holder's ability to share data be tied to that account holder's ability to view data (or, to put it another way, their right to receive account statements or log-in to internet banking). While some adjustments may be necessary (e.g. in the case of family violence; in respect of data that would not be readily viewable by all joint account holders, such as financial information disclosed in the loan application), these should be applied on an exception basis. We note that further consideration should be given to the sharing of data in respect of more complex, commercial accounts.

Rules Framework reference	Comment (and recommendation)
	13. **Minors** – We recognise that minors should be able to get the benefit of sharing their data. However, there is a greater risk of predatory practices or providers seeking to exploit the relative lack of financial awareness or literacy amongst young Australians. Noting our earlier comments in respect of the benefits of standardised use cases, we suggest that consideration be given to permitting access to minor's Open Banking data only on the basis of approved standardised use cases.
8.2 What does the consumer consent to?	14. **Extent of consent** – We note that there is an expectation that the accredited data recipient will have to obtain the consumer's preference as to the scope of data involved. However, on the basis that the granularity of authorisation will be at a 'coarse-grained' level, in many cases it will not be in the power of the data recipient to dictate what specific data it will obtain (based on the data that it needs). It would be confusing for the consumer if the data recipient had to obtain the consumer's consent to obtain data and, in obtaining the consent, advise the consumer that the data is not being obtained for any relevant purpose. We recommend that the ACCC consider whether the Rules should permit accredited data recipients to obtain specific consent in respect of the data that it requires, with a generic statement that any unnecessary data that is collected will be immediately destroyed.
8.3 Consent provided to accredited data recipients	15. **Nature of consent -** We agree with the proposal that consent must be freely and voluntarily given, and that accredited data recipients cannot make consent to share data a precondition to obtaining other services not related to, or dependent on, the sharing of CDR data. However, we note our earlier comments in relation to *Consent as a precondition of the provision of a service*. Again, we note that the creation of standardised use cases would mean that, where there are common use cases between data recipients, the standardised approach may be followed, leaving the regulator to focus on entities not following that standardised approach. 16. **Outsourced –** See our comments below (at XX) in respect of outsourcing. Based on those comments, we do not consider it is reasonable or necessary to require disclosure of the identity of the outsourced service provider. For comparison, Part IIIA does not require such disclosure in relation to credit reporting information, even though such information is generally considered to

Rules Framework reference	Comment (and recommendation)
	require a high degree of consumer protection. We recommend that the ACCC look to the requirements of Part IIIA in respect of disclosure to outsourced service providers. 17. **Purpose -** We agree the description of the purpose should be generally specific, rather than generic (although note our comments in respect of standardised use cases for the potential to describe some associated purposes in more generic terms). However, we note that this could still prove to be problematic. For example, we note that a provider - such as an insurance provider - could seek the consumer's permission to access CDR data for the 'purposes of assessing your application and setting the premium'. This consent is specific and would be understood by most consumers as relating to assessing the risk of the consumer making a claim. However, it is possible that the insurer could also use the data to assess the consumer's price sensitivity and, based on that assessment, increase the premium offered to the consumer – this activity would still be within the purpose described in the consent. If the purpose stated that the data was to be used to assess the consumer's propensity to pay a higher premium, it's likely that the consumer would not consent. We note that the use of standardised use cases would assist with setting the parameters on how CDR data may be used for purposes that are common across data recipients. 18. **Degree of specificity** – We note that it is better to describe the matters referred under "Specified information to be provided" on page 36 of the Rules Framework with an appropriate degree of specificity. However, what is appropriate for each of the matters listed may be different. For example, it may be possible to describe the period for which the data recipient will access data with a high degree of specificity – it may even be possible to state the number of days, or even hours. However, a data recipient may not be able to describe how long it will use or store the data in such detail (e.g. where it could be based on how long the customer holds the resulting product or service, or how the data recipient's document retention obligations apply). In this case, the Rules should recognise that the matter may be described in more generic terms. 19. **Cross-references** – We do not agree with the proposal to prohibit cross-referencing to other documents. The amount of information that is likely to be required under the Rules Framework to be given to the consumer is significant. Many consumers will not be particularly interested in the detail and it may be appropriate to provide a limited set of 'must know' information – while giving other consumers the ability to easily click-through to more detail information. At a minimum, we recommend that this issue be assessed as part of the user experience testing.

Rules Framework reference	Comment (and recommendation)
	20. **90-day time limit** – We recognise the reasons for introducing a default period for authorisation. However, there will be instances where this period is insufficient and is likely to cause detriment to consumers – for example, if the consumer has taken out a credit product which is dependent on the ongoing supply of CDR data and the consumer fails to renew the consent because they are on holiday. In such circumstances, the data recipient may have no choice but to terminate the product and, potentially, place the consumer in default of the loan. At a minimum, the Rules should permit the period be extended or removed based on the use of standardised use cases. 21. **Withdrawal without detriment** – We note our comments in respect of the potential implications of withdrawing consent set out in Item 5 of Table 1. Where a data recipient has advised the consumer of the implications of withdrawing consent at the point of obtaining consent, this exercise of such an outcome cannot be deemed a 'detriment' to the consumer (subject to the unfair contract provisions). 22. **Prohibition of on-selling of data and direct marketing** – We are unsure as to why these purposes would be explicitly prohibited. Such purposes seem to be within the main objective of the CDR regime. For example, subject to obtaining the consumer's consent, a comparison website may first obtain the consumer's CDR data, provide a recommendation and, subject to the consumer choosing a service provider, on-supply (for a price) that CDR data to the entity that will supply the service. Likewise, a consumer may sign-up with a service that, on an ongoing basis, monitors the consumer's CDR data and sends relevant offers to the consumer from time-to-time.
9.6 Granularity of authorisation	23. See our comments in respect of 8.2 *What does the consumer consent to?*
10. Providing consumer data to consumers	24. In our submission to Treasury on the draft Bill, we noted that there is a risk that a requirement to give consumers the ability to have their CDR data directly disclosed to them may be exploited by businesses to access data outside the CDR regime. This risk will increase if data holders are required to allow consumers to access CDR data via an open API (as suggested in the Rules Framework). To be clear, we agree that consumers should have the right to access their CDR data directly. However, the ACCC should be given power to make Rules applying to such businesses if it becomes necessary. This is to protect both consumer and data holders, which could otherwise find large parts of their sensitive consumer data records are extracted out of the secure CDR

Rules Framework reference	Comment (and recommendation)
	regime. Based on our review of the draft Bill, there does not appear to be any power granted to the ACCC to make rules in respect of such businesses.
12.1 Disclosure of consumer data to other parties	25. **Disclosure of data to a non-accredited entity (e.g. accountant) -** See discussion below under paragraph 27. In essence we see this model as a specific instance of a disclosure to intermediaries that could be accommodated in generic rules. 26. **Disclosure to outsourced provider of data recipient:** a. The suggested requirements relating to the disclosure of CDR data establish an unreasonable and unnecessary compliance framework that will disrupt businesses' standard outsourcing arrangements. The Rules Framework (p.50) notes that "the accredited data recipient would provide the primary service to the consumer, and will be the party with which the consumer contracts, it may utilise an outsourced service provider to assist in doing so". From the consumer's perspective, the accredited data recipient provides the *whole* of the service and, in most cases, the outsourced service provider is invisible to the consumer. The accredited data recipient would remain liable for the actions of the outsourced service provider. Requiring the disclosure of the identity of the outsourced service provider will simply confuse the consumer as to the identity of the business offering the service and which business is responsible for any misconduct. b. Accredited data recipients are likely to have multiple outsourced arrangements for different functions, such as data centres, communications providers (e.g. statement printers) and software suppliers that may incidentally receive CDR data as part of the service being provided. It would be confusing and unnecessary for the consumer to be told the names of each of these providers – particularly as the data recipient will be required to maintain appropriate risk management plans and processes (under the Rules and, if it's an ADI, under CPS 231) and will remain responsible and liable for compliance with all obligations under the legislation, rules and standards. c. For completeness, we note that the paragraph on page 50 beginning, "As provided for in section 8, the accredited data recipient…" appears to suggest that the consent obtained from the consumer need not include the details of the actual outsourced service providers

Rules Framework reference	Comment (and recommendation)
	(rather these are to be contained in the policy about the management of CDR data). This is not consistent with the requirements for specified information set out on page 36. d. While it may be better to include the names of outsourced service providers in the policy only – provided that the policy can be updated without invalidating consent already obtained – we consider that this still places an unnecessary compliance burden on accredited data recipients. e. We note that in many outsourcing arrangements, it may be possible for the outsourced service provider to themselves outsource certain components of the service. For example, an analytics service provider may use the service of a cloud provider. It is common for the primary outsource arrangement to not include the details of secondary service providers (although it will establish the parameters for such secondary outsourcing and, for ADIs, will be subject to the requirements of APRA – see our comments in respect of 6.8 *Accreditation and outsourcing*, above). This will mean that the accredited data recipient is unable to comply with the requirement to name all outsourced service providers. f. Further, the suggestion to restrict the ability to disclose to an outsourced service provider 'once removed' would interfere with the operation of such common outsourced arrangements. 27. **Disclosure to intermediary through whom data passes on its way to data recipient:** a. We are concerned that the suggested Rules described in 12.1.3 is seeking to address one particular type of business model and risks interfering with common outsourcing arrangements. b. The 'intermediary model' described in this section is simply a form of outsourcing arrangement. That is, the business offering the service to the consumer and obtaining the consent of the customer ('pr imary entity') utilises a third party to actually 'call' the API. As noted above the service provider in this case is likely to be invisible to the consumer even if they are the one who actually calls the data through the Open Banking system. In most cases, the primary entity would require the relevant accreditation and be liable for the actions of its outsourced service providers. c. We recognise that the Rules Framework is seeking to provide for a different outsource model – such that the outsourced service provider would hold the accreditation and permit

Rules Framework reference	Comment (and recommendation)
	the primary entity to avoid holding accreditation or allow it to hold a lower level of accreditation. This may be an appropriate model in some cases, however it should not interfere with ordinary outsourcing models. d. We note that genuine intermediary models also exist, where the consumer has the direct relationship with the intermediary. For example, this could be a model where the consumer directly engages an intermediary to hold a single view of the consumer's financial situation, that is then able to be passed to a lender when the consumer applies for a loan (noting that the intermediary in this case would be working for the consumer, not the lender). In this case, the intermediary would clearly need to be accredited. Such arrangements are not addressed in the Rules Framework other than to a limited extent in 12.1.1 (being a particular example) and incidentally in 12.1.3. **e.** This issue highlights the potentially broad range of business models that may exist under the CDR, and the dangers of trying to create specific rules for every possible model. We recommend that further consideration be given to this issue to ensure the "rulebook" does not become overly complex and prescriptive - as the ACCC notes the objective is for the CDR to be flexible enough to allow the development of alternative business models – a set of generalised rules that apply to all business models is more consistent with this objective and is possible.
13. Rules in relation to privacy safeguards	28. **Safeguard 11: withdrawal of consent –** We note that section 8 (p.38) of the Rules Framework states that, "if a consumer withdraws consent, the consumer's data becomes redundant … see discussion above and section 13". With respect, the preceding sections of the Rules Framework do not seem to address this point or section 13. We note the discussion in *Consent should be time limited* notes that, "once data is no longer needed for the purposes permitted under the rules … it is 'redundant data'". Likewise, the discussion regarding Privacy safeguard 11 in section 13 states that "the ACCC proposes to make rules to the effect that data should only be kept by an accredited data recipient for as long as is necessary to provide the uses consented to by the consumer". Both of those second two passages relate to whether there is still a valid use of the data, notwithstanding the consumer has withdrawn their consent to the data recipient accessing further

Rules Framework reference	Comment (and recommendation)
	data. It is possible for a consumer to withdraw their consent to the data recipient accessing further data, while still wanting to use the service provided based on the data previously obtained. If the ACCC does intend for data to be deemed redundant merely because the consumer has withdrawn consent, we note that this is both unnecessary and places an unreasonable burden on data recipients. Given the requirement to obtain explicit consent to specific purposes and the obligation to treat data as redundant once it is no longer needed for a valid use, it is not necessary to automatically deem data to be redundant as soon as the consumer withdraws – the consumer's original consent (i.e. which set out the valid use for the data) would continue. Further, as noted in Table 1, lenders will have valid uses of the data that extend beyond the initial granting of a loan, such as for assessing the performance of the lender's risk and responsible lending processes. Requiring the lender to make the data redundant when the consumer withdraws consent will interfere with those processes.

Appendix 3 – ARCA submission to Treasury on Provisions for further consultation

Kathryn Wardell
Structural Reform Group

Via email

12 October 2018

Thank you for the opportunity to provide a submission on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation* and *Designation Instrument for Open Banking*.

We appreciate having had the opportunity to discuss those documents with Treasury on 2 October 2018.

Impact of Provisions for further consultation

In our earlier submission, we identified issues relating to:

- Reciprocity under the consumer data right
- Interaction between the credit reporting system and the consumer data right
- The automatic application of the definition of 'CDR data' to derived data held by a data holder
- The definition of 'CDR data' and how it would apply to matters not within the scope of the consumer data right (e.g. data exchanges outside the CDR regime)
- Third parties exploiting the consumer's right to data

Subject to our comments in respect of the credit reporting system, we think that the provisions for further consultation address most of these issues. We note that the amended provisions do not appear to address our concerns regard third parties exploiting the consumer's right to data. In respect to this issue, we note that it may be appropriate to include an ability for the Rules to designate certain words or phrases as protected, so that they cannot be used by non-authorised businesses. This could include the phrases, 'consumer data right'; 'accredited person'; 'accredited data recipient' and 'open banking'.

In respect to the concept of reciprocity, we note that to give effect to the examples for 'equivalent data – designated entity' and 'equivalent data – not designated entity' outlined in *Proposal 3: Reciprocity*, the ACCC will need to review their current position of not making rules regarding reciprocity in the first version of the rules. Our view is that the effective and fair operation of the Consumer Data Right (CDR) requires the ACCC to develop rules creating reciprocity obligations, and our separate submission to the ACCC's draft framework will include an outline for how this might operate.

Interaction between the credit reporting system and the consumer data right

When assessing an application for credit, the credit provider's ability to successfully undertake a risk and responsible lending assessment is dependent on the availability and accessibility of relevant, accurate, and up-to-date data about the customer. The credit reporting system established under Part IIIA of the Privacy Act provides such data in respect to consumer's existing consumer credit arrangements. The consumer data right – in particular, the Open Banking regime – will provide access to additional data sets in respect of those consumer credit arrangements, together with other data relevant to the risk and responsible lending assessment (e.g. data for income and living expense verification). Importantly, the Open Banking regime will ensure such data is obtained via a secure, reliable and efficient process that represents a significant improvement in current approaches to obtaining similar data (e.g. copies of paper statements, or "screen scraping" internet banking websites that require disclosure of customer internet banking credentials).

On that basis, the CDR/Open Banking regime and the credit reporting system will operate in a complementary way with similar levels of data quality and data security.

Regarding our comments in our earlier submission about the interaction between the credit reporting system and the consumer data right, we note:

- CDR intermediaries being caught by the definition of 'credit reporting body' (CRB) – subject to making the actual regulations, this has been addressed through the introduction of a regulation making power to vary the application of Part IIIA.

  Recommendation: Treasury should consult on the drafting of the relevant regulation.

- Credit reporting information obtained by a credit provider from a CRB being caught by the definition of 'CDR data' and, so, being subject to access under the consumer data rules – the Designation Instrument identifies information "that was observed or provided by the person". It appears that the reference to "observed" refers to being observed by the data holder when establishing the product. This could mean that the credit reporting information obtained by the credit provider from a CRB would be captured by the Designation Instrument.

  Recommendation: That the Designation Instrument be clarified on this point and, if the intent is to generally include information 'observed by the data holder', that there be a specific exemption of credit reporting data (for the reasons outlined in our earlier submission).

We note the following additional ways in which the credit reporting system and the consumer data right overlap. Where we consider this to raise problems, we have recommended a solution. Otherwise, we have simply noted the interaction for completeness.

1. Paragraph 5.1 of the Privacy (Credit Reporting) Code 2014 (CR Code) prohibits a credit reporting body from collecting "personal information about an individual's activities in relation to consumer credit that is not credit information". To the extent that the data available through the consumer data right involves collecting data in relation to a credit account (which would include certain products offered businesses such as telcos and

utilities) that goes beyond the meaning of 'credit information', this appears to limit a CRB's ability to participate in the consumer data regime.

2. Subject to the above comment, if a credit reporting body collects information under the consumer data rules that meets the definition of 'credit information', that information would be subject to the requirements of both the consumer data right regime and Part IIIA.

3. Data that is derived by a credit provider from data obtained under the consumer data rules and through credit reporting system will be both 'CDR data' and 'credit eligibility information' (referred to below as 'dual derived data') – a key example would be a credit score created by the credit provider that utilises both types of data. We note that this will create several overlaps between the provisions of Part IIIA (and the CR Code) and the Privacy Safeguards. These include:

    - Privacy safeguard 5: For completeness, we note that a credit provider that has dual derived data will required to notify the consumer in accordance with Privacy Safeguard 5 and sections 21B and 21C of the Privacy Act. Based on the matters below, that notification may be confusing to the consumer.

    - Privacy safeguards 6 and 7: These safeguards and the use and disclosure provisions of Part IIIA (and the CR Code) will apply to the dual derived data. Part IIIA prescribes the circumstances and purposes for which credit eligibility data may be used or disclosed – unlike the consumer data right, this regime is generally not based on the consumer's consent.

      The restrictions on use and disclosure under both regimes are, however, subject to uses and disclosures that are "required or authorised by or under an Australian law"[2] On this basis, the dual derived data will be *permitted* to be used and disclosed in the circumstances set out in Part IIIA. Given the careful and restricted design of the Part IIIA use and disclosure regime, we consider this to be appropriate.

      However, it will also mean that the dual derived data may be used or disclosed in circumstances not permitted by Part IIIA, subject to satisfying the consumer data rules – most notably, by obtaining the express consent of the consumer. This would permit credit providers to use credit eligibility information (provided it is dual derived data) for marketing purposes – subject to obtaining consumer consent. This is contrary to one of the key principles of Part IIIA.

      Recommendation: That the use and disclosure of dual derived data be made subject to the restrictions in Part IIIA – notwithstanding that sub-paragraphs 21G(2)(d) and (3)(f) of the Privacy Act may permit the use or disclosure based on the consumer data rules.

[2] See: sub-paragraphs 21G(2)(d) and (3)(f) of the Privacy Act for CP's use or disclosure of 'credit eligibility information'. We note that both the consumer data right and Part IIIA establish circumstances in which the data 'must not' be used, rather than directly authorising the particular uses and disclosures. We suggest that Treasury consider whether the two regimes genuinely 'authorise' the relevant uses and disclosures. If the regimes do not 'authorise' the relevant uses and disclosures, the restrictions of both regimes will apply – significantly impacting on the ability of a credit provider to use or disclose dual derived data.

- Privacy safeguard 8: Part IIIA permits cross-border disclosure of credit eligibility information in certain circumstances. We note that, unlike Privacy safeguards 6 and 7, this safeguard is not qualified by the reference to 'required or authorised' under an Australian law.

  Recommendation: This safeguard be qualified to permit cross border disclosures where required or authorised by an Australian law (noting our comment in footnote 2 regarding the meaning of 'authorised by or under an Australian law').

  Further to the above, we note that where Part IIIA permits the disclosure of credit eligibility information to a person without an Australian link, the Act deems the credit provider to be responsible for acts of the recipient that would constitute a breach of the relevant law.

  Recommendation: Treasury consider whether the Bill should include a rule making power that would permit the ACCC to deem the disclosing entity responsible for the acts of the overseas recipient (where they would be inconsistent with the consumer data rules) if they are not accredited or do not meet the other conditions specified (if any).

- Privacy safeguard 11: For completeness, if a credit provider (i.e. accredited data recipient) discloses dual derived data in accordance with Part IIIA (as contemplated by s56EI(1)(c)(i)), we understand that this will not be a disclosure 'required by the consumer data rules' – as per s56EM(2), such that this Privacy safeguard won't apply to that disclosure.

- Privacy safeguard 12: The requirements of this safeguard and s21S of the Privacy Act will both apply to dual derived data. While the requirements are broadly the same, we recommend that for simplicity credit providers be subject to one regime only.

  Recommendation: Credit providers be exempt from the requirements of Privacy safeguard 12 in respect of dual derived data (on the basis that s21S provides equivalent protection).

  Further to the above, to the extent that a credit reporting body obtains CDR data which is 'credit information' within the meaning of Part IIIA or creates dual derived data, there will be an inconsistency in the obligations under this Privacy safeguard and the retention periods set out in s20W of the Privacy Act. While the safeguard provides an exemption where the accredited data recipient is 'required' by law to retain data, the retention regime under Part IIIA imposes destruction/deidentification requires, rather than a requirement to retain.

  The retention periods in Part IIIA have been carefully chosen based on the nature of the data. It seems incongruous to require a credit reporting body to destroy or de-identify data that was obtained under the consumer data rules, where that data may be more up-to-date than credit information obtained under the framework set out in Part IIIA.

Recommendation: That CRBs be exempted from the requirements of s56EN(2) of the CDR Bill, where it is otherwise subject to retention periods set out in s20W of the Privacy Act.

- Privacy safeguard 13: A credit provider which holds dual derived data will be subject to this Privacy safeguard and s21V of the Privacy Act. Part IIIA and the CR Code set out a comprehensive process for the correction of credit eligibility information by credit providers, which is tailored to the nature of the data (e.g. it includes requiring the credit provider to consult with other credit providers or credit reporting bodies as required). It would not be appropriate to then overlay a separate process on top of that.

  Recommendation: That credit providers be exempt from the requirements of Privacy safeguard 13 in respect of dual derived data.

4. For the recommendations made in respect of Privacy safeguards 6, 7 and 13, we believe that the changes suggested should be incorporated into the Bill, rather than relying on the ACCC rules making power. This would be consistent with how the interaction between the consumer data right and the APPs is addressed. In addition, the issues raised in respect to those safeguards are not limited to the Open Banking regime and will apply to all sectors that involve 'credit providers' under Part IIIA (such as telcos and utilities).

If you have any questions about this submission, please feel free to contact me or Michael Blyth.

Yours sincerely,

Mike Laing
Executive Chairman