AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

9 April 2020

Inquiry into Future Directions for the Consumer Data Right

Thank you for the opportunity to provide a submission to the Inquiry.

ARCA is the peak industry association for businesses using consumer information for risk and credit management. Our purpose is to improve the availability of credit through responsible and efficient credit management policy and practice. We do this by working with stakeholders to develop and advocate for best practice in credit management and better availability and use of data.

Our Members include Australia's leading banks, credit unions, finance companies, fintechs, and credit reporting bodies. Collectively, ARCA's Members account for well over 95% of all consumer lending in Australia.

Our submission identifies:

(i) ways to ensure that the Consumer Data Right (CDR) promotes innovation, and better compliance outcomes, in the provision of consumer credit in a manner that is inclusive of the needs of vulnerable consumers – particularly through the development of a standardised 'consent taxonomy' combined with a bespoke rules regime that recognises the limitations with, and provides alternatives to, the current 'consent-based' framework; and
(ii) issues to consider when implementing a 'write access' regime.

(i) Standardised consent taxonomy with bespoke CDR rules

A key question that the Inquiry needs to answer is the extent to which the Consumer Data Right (CDR)/Open Banking regime is intended to support the efficient and responsible provision of credit. The Treasury has noted that the consumer data right was, in part,

intended to support improved compliance with regulations, including responsible lending processes.[1]

If this is the case, the CDR/Open Banking regime would:

- Give credit providers efficient and certain access to data that was 'reasonably' required to allow verification of a consumer's financial situation, and to permit that data to be used in ways that are necessary for the proper assessment and management of the credit; and
- 'Raise the bar' on what forms of verification are 'reasonable' under the *National Consumer Credit Protection Act* (NCCP) by providing an improved verification tool and, in doing so, improve compliance outcomes for Australian consumers.[2]

However, the current rules framework does not support the above outcomes.

The CDR Rules are highly restrictive and do not adequately support credit providers accessing and using data that is necessary for responsible lending and credit risk. In particular, the strict and complex rules place significant blocks on the access to, and use of, the data by credit providers. For example, the rules relating to:

- the **data minimisation principle** do not permit the credit provider to use CDR data to develop or maintain lending-related algorithms as this use is not related to the product being offered to the consumer[3];
- **consent** requires the credit provider to obtain itemised consent which does not give the credit provider certainty of access to the customer's accounts or data clusters that it requires; and
- **redundant data** which permit the CDR customer to determine whether their redundant data will be deidentified or deleted will mean that the data available to develop or maintain lending algorithms will be patchy and unrepresentative. This, in turn, will cause the algorithms to be flawed (assuming the data can even be used for the purposes of developing or maintaining the algorithm, given the data minimisation principle). This risk will likely impact smaller lenders more acutely as larger lenders may have enough data to compensate for the patchy data coming through the CDR/Open Banking regime.

As a result, a credit provider is unlikely to be able to consistently rely on the CDR/Open Banking regime to supply it with access to data that it needs to complete 'reasonable' verification steps under the NCCP. This has two impacts: (i) a credit provider is more likely to continue using other options to access that data that give them greater control and certainty, such as digital data capture, aka "screen scraping" (or even much less secure methods such

---

[1] Privacy Impact Assessment Consumer Data Right, version 2, March 2019, p32.

[2] ASIC notes, in RG209.23, that the responsible lending obligations "are not static - what is 'reasonable' will be affected by the broader professional and regulatory environment in which you operate. For example, legislative developments (e.g. open banking and comprehensive credit reporting) and other developments and innovations adopted by the credit industry will affect the measures you could reasonably be expected to undertake".

[3] That is, the CDR data may be used to create a 'credit score' (by using an existing algorithm) in relation to the customer's application, but cannot be used to help improve that algorithm. Importantly, as the OAIC has noted (Privacy Safeguard Guidelines, C.43) the process for obtaining consent for deidentification "necessarily involves explaining how de-identification and disclosure of the consumer's CDR data is reasonably needed to provide the goods or services to the consumer". It is difficult to see how the credit provider could even deidentify the CDR data for the purposes of improving the algorithm as that process is not "reasonably needed in order to provide the requested goods or services".

as email); and (ii) any data provided under such other manner will not be subject to the protections provided under the CDR Rules. This means that the restrictions in the CDR Rules will therefore undermine one of the key objectives of the CDR regime which was to reduce the need to rely on alterative means of data sharing.

Importantly, the CX Guidelines state that data recipients "SHOULD avoid making consent a precondition of services". This means that a small, fintech lender is unlikely to be able to establish their business using only the CDR/Open Banking regime as their verification tool. That is, they will be expected to establish other means of obtaining verification data. In reality, there would be little reason for the fintech lender to take part in the CDR regime at all, as they are more likely to rely on other means of obtaining the data, such as digital data capture, which are not subject to the same restrictions.

Given the uncertain and inconsistent access to data that the CDR/Open Banking regime will give to credit providers, it will not change what are 'reasonable' verification steps, as suggested by ASIC.[4] . It is unfortunate that the current CDR Rules framework which offers greater security and other protections may play a limited role in supporting responsible lending because its rules are too restrictive, and will therefore not promote an improvement of compliance outcomes for Australian consumers. –

Please note that we are not suggesting that the current 'consent' based rules framework is fundamentally wrong. However, the very fact that the current CDR Rules are so 'strict and complex' appears to recognise the fact that a pure consent-based framework is, unless very tightly drafted, open to manipulation and exploitation given the limits on relying on a consumer's *informed and voluntary* consent. In seeking to protect consumers interests by relying almost exclusively on a consent-based model, the legislative 'bar' has been set so high that it risks reducing the effectiveness of the CDR/Open Banking regime.

We consider that there is an opportunity to take a different approach for certain critical and potentially highly sensitive uses of CDR data that are common across many data recipients – such as those relating to the assessment and management of credit. That is, the Rules could recognise certain 'standardised consents' (or 'consent taxonomy' as referred to in the Issues Paper) that establish the types of data required for the use case and set out the way in which the data is used – where those standardised consents are supported by their own bespoke Rules that are more tailored to the particular use case.

For example, the bespoke Rules relating to lending-related standardised consents would better recognise the need to give credit providers more certain access to, and use of, data (such as for the purposes of developing and managing lending related algorithms). The bespoke Rules would provide more flexibility to credit providers to do things that are necessary for the provision of credit, while imposing stricter prohibitions on other uses (e.g. this could potentially involve a prohibition on using the information for the purposes of marketing).[5] This would be similar to the approach taken under the Privacy Act to the disclosure and use of credit reporting information.

[4] This should be contrasted to the comprehensive credit reporting developments that have provided credit providers with clear rights to access additional credit reporting information when assessing credit contracts.

[5] Noting that a credit provider would still be able to separately seek consent for other purposes (that are permitted by the CDR Rules). However, those consents would be subject to the ordinary CDR Rules.

We have previously raised this possibility with the ACCC and attach an extract of our submission to the ACCC CDR Rules Framework consultation dated 12 October 2018 (see Appendix A). In its Privacy Impact Assessment, Treasury previously recognised the purpose of such standardisation as aiding in "consumer comprehension by creating a short-hand and shared understanding of common uses."[6]

Accordingly, we suggest that the Inquiry include a recommendation that the ACCC allow for bespoke rules within the CDR Rules that support the development of standardised consents (or taxonomies) for certain critical and sensitive use cases where the use of CDR data is likely to be common across many data recipients, such as those relating to the assessment and management of credit.

(ii) Issues to consider in relation to write access

Given ARCA's interest in the use of the CDR/Open Banking regime for credit assessment and management purposes, we do not have extensive comments in relation to the proposal to allow 'write access', however we do make the following observations.

Using write access to close accounts – responsible lending implications

When assessing a loan that will consolidate (i.e. pay out) an existing loan, credit providers must currently consider whether it is appropriate to treat the existing loan as closed for responsible lending purposes as, for many products, there is no way for the credit provider to effectively or efficiently confirm the closure of the existing loan. For example, if Bank A is assessing an application for a credit card that will be used to pay out an existing card with Bank B (via a balance transfer), there is currently no way for Bank A to ensure that the credit card with Bank B is subsequently closed (or even to test whether it has been closed). This often means that Bank A will, when assessing what credit limit the customer can afford, treat the existing credit card as a continuing liability of the customer.

This may be helped if the ability to close an account is included as part of the write access. However, we note that this ability would need to recognise that the consent/instruction to close the account is likely to be obtained some time prior to the instruction to close being transmitted by the accredited data recipient to the data holder (i.e. the entity which holds the account to be closed). For example, it would be problematic if, in the credit card example above, Bank A obtained an instruction to close the credit card with Bank B and assessed the credit limit on that basis, and the customer withdrew their consent/instruction prior to the account with Bank B being closed (i.e. the customer could be left with more credit than they could afford and Bank A may be at risk of being judged as being in breach of the responsible lending obligations).

Potential for using (or misusing) write access to collect debts

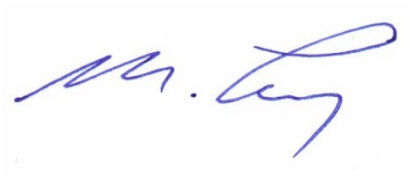
While not directly related to the provision of credit, we note that the potential for the CDR regime with write access to be used in ways that may be considered unfair. For example, a debt collector could seek consent (potentially in a way that is not consistent with the CDR Rules requirement that consent be 'voluntary') to undertake real time monitoring of a consumer's transaction account and, if it identified funds being transferred into the account, immediately withdraw those funds to their own benefit without consideration of the needs of the consumer.

[6] Privacy Impact Assessment Consumer Data Right, version 2, March 2019, p131.

We suggest that consideration be given to whether this is a desired outcome. Additional rules may be required to protect against outcomes such as this if the CDR regime is extended to allow write access.

If you have any questions about this submission, please feel free to contact me on 0414 446 240 or at mlaing@arca.asn.au, or Michael Blyth on 0409 435 830 or at mblyth@arca.asn.au.

Yours sincerely,



Mike Laing
Chief Executive Officer
Australian Retail Credit Association

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.