AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

21 October 2019

By email

Dear

Draft PIA report for the initial implementation of the CDR regime

Thank you for the opportunity to provide a submission in response to the draft privacy impact assessment (PIA) of the proposed consumer data right conducted by Maddocks.

ARCA is the peak industry association for businesses using consumer information for risk and credit management. 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.

We have been closely involved with the development of the consumer data right and, in particular, the initial Open Banking implementation. Our feedback in relation to those reforms has focused on balancing the need to ensure the consumer remains in control of their data, while also developing an Open Banking regime that supports better risk and responsible lending decisions by credit providers using the data that will be made available through that regime.

On that basis, we provide the following observations and recommendations.

1. Ability to explain to a customer how their data will be used

We are concerned that the undefined and uncertain extent of a lender's obligation to forensically analyse a consumer's transaction (i.e. expense) history when assessing a loan could result in poor privacy outcomes for consumers.

Under the *National Consumer Credit Code* (NCCP) a lender must, amongst other things, make reasonable inquiries about a consumer's financial situation and take reasonable steps to verify that information. The lender must then make an assessment as to whether the consumer will likely be unable to comply with the their financial obligations under the contract, or could only comply with substantial hardship.[1]

It is likely that lenders will look to include Open Banking data into their responsible lending assessments.[2] In doing so, the lender will probably want to use the data for straightforward purposes such as verifying a consumer's income, verifying certain expenses that were disclosed by the consumer on the application form and, potentially, identifying whether the consumer has failed to disclosed any material expenses or liabilities.

These purposes should be reasonably straightforward to explain to a consumer in a way that allows the lender to obtain the consumer's genuinely informed and specific consent and comply with the CDR Rules.

However, ASIC has noted in Consultation Paper 309 *Update to RG 209: Credit licensing: Responsible lending conduct* (CP 309), that it considers that it is "not sufficient merely to obtain verifying information but not have regard to it, or to use a source of information to verify only one aspect of the consumer's financial situation it contains other (potentially inconsistent) information about other aspect of the consumer's financial situation".[3]

This has been interpreted by some stakeholders as potentially requiring a lender to forensically analyse the consumer's transaction history to identify any potential issues that may impact on whether the consumer is 'likely' to be able to afford the loan (even where the consumer has declined to provide that information to the lender directly). As noted in ARCA's submission to CP 309[4], this could extend to looking for issues such as whether it was likely the consumer was pregnant (i.e. through medical costs and baby-related purchasing) or undergoing cancer treatment (i.e. through medical costs).

Overall, we are hopeful that ASIC would not expect lenders to use the data in this way and we have asked that further clarity be provided in the revised responsible lending regulatory guide, RG 209 (which is expected by the end of the year). We also note that consumer advocates do not expect this form of forensic analysis to be done. During the recent ASIC

---

[1] Part 3-2, National Consumer Credit Protection Act 2009

[2] The Treasury has noted that the consumer data right was, in part, intended to support improved compliance with regulations, including responsible lending processes; see Privacy Impact Assessment Consumer Data Right, version 2, March 2019, p32. Likewise, ASIC has noted the ability of Open Banking data to improve responsible lending practices; see, for example, Consultation Paper 309 Update to RG 209: Credit licensing: Responsible lending conduct, paragraph 20.

[3] Page 11, CP 309, https://download.asic.gov.au/media/5008524/cp309-published-14-february-2019.pdf

[4] See, in particular, paragraphs 194 – 215, ARCA submission to CP 309, https://download.asic.gov.au/media/5159844/australian-retail-credit-association-cp309-submission.pdf

hearings into responsible lending, a representative of the Financial Rights Legal Centre noted that, in relation to the suggestion that lenders should analyse whether a consumer is pregnant or ill, this was "completely inappropriate and I think that if people thought that was happening there would certainly be resistance".[5]

Nevertheless, the position is currently unclear. This places a lender in a difficult position; if they seek the consumer's consent in simple terms (i.e. for the straightforward processes described above), they will not be permitted under the CDR Rules to analyse the data in the 'forensic' manner that could be inferred from ASIC's comments. Alternatively, if ASIC's expectation is that the lender forensically analyses the data in this unlimited and undefined manner, the lender would be forced to obtain consent under the CDR Rules in such broad terms that a consumer is unlikely to generally understand the extent of the consent.

Accordingly, we recommend that the PIA note the need for ASIC to provide appropriate guidance on the limits to which a lender (as a licensee under the NCCP) is expected to use data obtained under the consumer data right, in particular in relation to issues such as pregnancy or illness (such that lenders may structure their consent under the CDR Rules in a meaningful and clear way).

2. Use of standardised consents in relation to common use cases

We have previously noted the benefits that could be obtained from developing 'standardised consents' for critical and potentially sensitive uses of CDR data that are common across many data recipients, including risk and responsible lending use cases.

We described the benefits of standardised consents in the following way in our submission to the ACCC CDR Rules Framework in October 2018[6]:

> *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.*

[5] Page 92, https://download.asic.gov.au/media/5243788/asic-public-hearings-on-responsible-lending-sydney.pdf

[6] [XXX – Link to the online reference if available.]

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 [not included in this extract]. 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.

We further noted:

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.

We understand that our proposal for the use of standardised consents has been received positively by Treasury and the ACCC. The Treasury has recognised the purpose of such

standardisation as aiding in "consumer comprehension by creating a short-hand and shared understanding of common uses."[7]

However, given the work required to implement the CDR regime, we understand that the ACCC has not had the resources to investigate this issue further. Nevertheless, we consider that the initial work to develop the standardised consents should be given to industry, rather than Treasury, ACCC or OAIC. ARCA has commenced initial work to begin developing certain lending related use cases, however this work would be assisted if there was documented support for the development of the standardised consents from the relevant regulators.

Accordingly, we suggest that the PIA include a recommendation that the ACCC encourage industry to develop, in consultation with relevant stakeholders, appropriate standardised consents – starting with those relating to the use of Open Banking data for risk and responsible lending purposes.

3. Joint account holders

We welcome the proposed recommendation 6 to review the approach taken to joint account holders.

ARCA has previously noted our concern regarding the fundamental approach taken to joint account holders that restricts an account holder's access to, and use of, their own data (i.e. as the framework is currently proposed allows the other account holder to control whether that data may be shared by the account holder under the CDR regime). The Farrell report recommended that "[a]uthorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from the joint account".[8] We consider that this misconstrues the nature of the data sharing; unlike the sharing of money, the sharing of data by one joint account holder does not deprive the other account holder of the ability to share that data.

Further, under the financial services laws, a consumer has the right to their data, regardless of whether the account is held jointly or singularly. For example, the NCCP provides that account statements must be provided to all account holders. There is a specific process to be followed if the account holders wish to nominate only one account holder to receive those statements – and, if such any nomination is made, any account holder may withdraw the nomination at any time.[9] This is essentially the opposite approach to that taken under the CDR legislative framework.

We recommend that, in considering whether the CDR legislative framework implements an appropriate policy balance between the protection of the privacy of joint account holders, against the need to facilitate access to information by victims of family violence, consideration be given to changing the current fundamental approach to joint account holders. That is, consideration should be given to allowing a joint account holder to authorise the sharing of the CDR data without the consent or knowledge of the other joint account holder. This is more consistent with the current approach in the financial services laws, will

[7] Privacy Impact Assessment Consumer Data Right, version 2, March 2019, p131.
[8] Recommendation 4.7, Review into open banking: giving customers choice, convenience and confidence, December 2017.
[9] See section 194, National Consumer Credit Protection Act

avoid the concerns identified in relation to family violence and will simplify the design of the data standards.

4. Other matters

We note:

- In respect of the complexity discussed in paragraph 23. 7, certain data could also be regulated as 'credit eligibility information' under Part IIIA as well as CDR data if it was data was that derived from both credit reporting information (obtained from a credit reporting body) and CDR data (which could include forms of credit or behavioural score calculated by a lender). We note that this could increase the complexity identified in the PIA.
- In respect to Recommendation 4, we note policy reasons for not including a right for CDR Consumers to access their CDR Data whilst it is held by the Accredited Data Recipient are that (i) the data held by the Accredited Data Recipient (ADR) will not be the most up to date version of that data (and any data derived from that data is most likely to be 'value-added data'). Rather, the most up to date version will be held by the Data Holder; and (ii) on that basis, requiring the ADR to develop and maintain a further 'business-to-consumer' process to exchange data appears to be unnecessary cost to impose on the ADR (many of whom will be smaller enterprises).
- In respect to Recommendation 3.1, we note that any such extension of the Rules should recognise the requirements already imposed upon many data holders in relation to security obligations (and, in particular, those already imposed on authorised deposit-taking institutions under the prudential framework).

If you have any questions about this submission, or would like ARCA to share any previous submission made by us in relation to the CDR framework, please feel free to contact me or Michael Blyth.

Yours sincerely,

Mike Laing
Chief Executive Officer
Australian Retail Credit Association