Treasury

CDRRules@treasury.gov.au

17 September 2024

Dear Sir/Madam

**CDR rules: consent and operational enhancement amendments**

Thank you for the opportunity to provide a submission in response to the CDR rules: consent and operational enhancement amendments consultation paper (the 'consultation paper').

Arca is strongly supportive of the Consumer Data Right (CDR) and the Government's stated intent to improve the operation of the CDR, with a specific focus on the lending use case. However, Arca's view is that changes to the CDR are necessary to enable our Members to use CDR data to aid lending and credit management. There are three fundamental issues with the proposed rule changes which will continue to inhibit the effective roll-out of CDR, namely:

- Operational enhancements: the proposal to expand the circumstances in which an ADI can hold CDR as a 'data holder' needs to be expanded to include holders of an Australian Credit Licence (ACL) or their credit representative and service providers, such as credit reporting bodies. (**ADI restriction**)
- Consent review: standardised consents for lending which are reasonable and necessary and presented as 'take it or leave it' ought to be enabled under the rules (**standardised consents**)
- Consent review: data minimisation rules which currently restrict collection of collected CDR data to uses relevant to a specific customer and otherwise impose onerous restrictions on obtaining consent to use data for other purposes ought to be expanded to enable broader uses beyond a specific customer. Similarly, de-identification consents should be able to be included in a bundled, standardised consent, rather than remain a standalone consent. (**credit assessment and management issues**).

We have set out below a comprehensive explanation of each of these issues, with a focus as to why these issues will inhibit the effective use of CDR by our Members. We have further set out a series of illustrative use cases for CDR, alongside an explanation as to the further changes needed to the CDR rules to ensure these use cases can be applied by Arca Members.

**ADI restriction**

Arca considers the expansion of the circumstances to enable ADIs to act as 'data holders' rather than 'data recipients' in respect to CDR data is an important enhancement to support a lending use case. However, restricting this enhancement to only ADIs would have a significant effect on the ability of smaller non-ADIs to compete with larger ADIs[1], particularly considered alongside the prospect of future changes to force all businesses off screen scraping. We would emphasise that enabling an entity who would otherwise be classified as a data recipient to act as a data holder is a positive step. It will significantly limit the risk that the CDR data

[1] That is, larger ADIs are more likely to be able to use the CDR data as an *input* into their existing algorithms to calculate an outcome (e.g. 'score') for a particular customer (where those algorithms have been developed using other data sets, such as from the ADI's transactional facilities including transaction accounts and credit cards). Smaller non-ADIs have more limited access to existing data sets with which to develop the algorithms (due both to their smaller customer bases and product types) and would rely on the data received through the CDR to develop and refine those algorithms (whether themselves or using the services of third parties, such as a credit reporting body).

is required to be quarantined (and therefore, unable to be used effectively to support lending or credit management); for this reason this change is critical for all lenders seeking to rely on CDR data.

However, the limited expansion to ADIs-only would mean that it is then only ADIs who could effectively use CDR data to support lending or credit management. For non-ADIs, including those who currently use screen scraping to enable access to transaction records, this creates a considerable disadvantage (which will only be worsened where these businesses are forced off screen scraping). For service entities, such as credit reporting bodies, who currently provide screen scrapping services to assist lenders in their lending decisions, this would also inhibit these activities and support provided to these lenders.

For example, in a future state where (a) the expanded rule was restricted to ADIs only; and (b) screen scraping was prohibited it is conceivable, the following could occur:

- A large ADI, which already had access to considerable customer transaction records (gained through its existing large customer base and provision of transaction accounts), could implement processes to roll out the use of CDR data to support its lending decisions and processes. Both the use of existing transaction records, alongside a comprehensive set of data (both comprehensive credit reporting (CCR) and CDR) would significantly enhance the quality and speed of the lending decisions made by the large ADI;
- By comparison, a small non-ADI fintech, which does not hold transaction accounts and has a smaller customer base, and no longer has access to screen scraping data, would be unable to effectively use CDR data, i.e. in respect of the CDR, they would be in the same position as they are currently in (which has already been acknowledged as unworkable and is the reason why the relevant rule is proposed to be expanded) and in a worse position in respect of other data collection methods (assuming screen scraping is no longer available). As such, this small non-ADI fintech would become reliant on manual processes (production of customer account statements) to verify income and expenses, which would reduce the effectiveness and efficiency of their lending process and therefore add significantly to lending costs. Further, the small non-ADI fintech would not have access to the CDR with which to develop their credit algorithms or use existing algorithms (where the algorithms would otherwise allow the lender to significantly improve the quality and speed of lending decisions) and place those smaller lenders at a significant competitive disadvantage. Moreover, this manual process is far more fallible (with the manual provision of PDF versions of account statements creating similar (possibly higher) security risks as the current screen scraping processes) and the small non-ADI fintech has greater risk and regulatory/ dispute exposure as a result (due both to the heightened data security risks and the less effective responsible lending processes they would be able to undertake). While the small non-ADI fintech may have access to CCR data under Part IIIA of the Privacy Act to aid the lending decision, this assists verification of undisclosed liabilities but does not otherwise support verification of income and expenses. The lending decision made by the small non-ADI fintech and the efficiency/speed of that process are both therefore far inferior to that made by the large ADI.
- The same outcome would be true of a entities providing supporting services to credit providers, such as a credit reporting body (upon which smaller lenders are often more reliant due to their reduced internal capacity compared to larger ADI lenders).

We appreciate that the restriction to ADIs is intended to reflect the stringent data security restrictions placed on APRA-regulated entities (and stems from a desire to ensure that CDR data is sufficiently protected in the event of a possible data breach). However, our view is that the better approach in the rule design would be to remove the ADI-only restriction, and directly address the data security concern separately. For instance, it is possible that the entity who holds the data could agree to treat that data 'as if' it was credit reporting information, therefore applying the same use and disclosure and data security obligations[2] to the data (and derived data) as would apply under Part IIIA of the Privacy Act.

[2] These obligations are set out in sections 20Q and section 21S and require a credit reporting body or credit provider to take reasonable steps to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure, as well as requirements to destroy or de-identify information once no longer needed or required to be held.

**Standardised consents**

Arca notes the consent review proposes to remove the restriction on the bundling of consents in rule 4.10. However, the consent framework otherwise continues to operate to allow consumers choice in respect to various elements of the consent. Arca has previously proposed the concept of standardised consents, under which industry would agree to a set of consents (covering data sets and uses/disclosure permission) that were considered reasonable and necessary for the provision and management of credit. Those consents would be approved by the Office of the Australian Information Commissioner (OAIC) and/or Australian Competition and Consumer Commission (ACCC), and would be subject to a bespoke set of rules that could override elements of the 'standard' rules. For example, bespoke rules would explicitly allow bundling of consents (i.e. that are reasonably necessary for the use case) and could apply a different set of CX rules (to simplify the consent process).

The consents could then be presented on the basis that the application for credit could not proceed without the consent (i.e. it is a 'take it or leave it' consent).

To confirm, Arca's recommendation to allow for standardised consents would be an optional process that applies to nominated use cases only (e.g. the lending use case) and would not limit other use cases (which would then be subject to the ordinary CDR rules). In this way, the consumer protections applying to those nominated use cases could be refined to reflect the importance and risk-profile of that specific use case, while maintaining the strong protections applicable to all other potential use cases. Likewise, data recipients would be able to determine whether the use of the standardised consent (rather than the ordinary rules) was appropriate for their business.[3]

In essence, our recommendation for standardised consents adopts the concept of consent bundling but goes further to involve adjusting how the rules would then apply to the nominated use case (which may involve either relaxing *or* tightening how the data recipient may use the data received under the standardised consent).

Standardised consents for lenders and service entities are critically important to developing lending processes which rely on the use of these consents. For example, if a standardised consent requires that, for every credit application, a potential customer is required to consent to sharing of all current CDR account data, this enables a lender to build a lending process based on the assumption that the CDR data is comprehensive. In this context, it should be noted that access to all current CDR account data is critical to support the lender's accurate verification of that customers' income and expenses (i.e. a credit provider cannot create an efficient and effective lending process based on inconsistent and uncertain access to data).

In the absence of a standardised consent model, the customer would retain the ability to pick and choose which CDR account data was provided to the potential lender (and the purposes for which it can be used). A customer who was intent on both obtaining credit, and hiding those accounts and transactions which may highlight a possible lack of suitability for that credit, may simply refuse to provide consent to sharing the CDR data for those particular accounts. This compromises the credit provider's ability to conduct appropriate due diligence and lend responsibly, with the potential for negative impacts to borrowers who are approved for credit which should not have been granted.

Further, without the standardised consent model, many of the benefits of CDR will be eroded and the customer may not appreciate that by not providing their full consent any lender will still need the customer to provide alternative verification material (e.g. PDF statements etc) rather than obtaining this information through CDR (where the sharing of that information would not be within the secure framework of the CDR and the use and disclosure of that information would not be subject to the Privacy Safeguards that would apply if it was received through the CDR). In this sense, standardised consents could be an advantage, particularly for information where customers may not appreciate how the information is used by lenders and the consequences of not providing CDR consent (e.g. more paperwork to provide, slower application turnaround). From a lender's point

[3] Some Members have noted concern that a mandated use of a standardised consent for a particular use case could potentially increase costs. For that reason, we would suggest that their use be optional (although we also think that such standardised consents are more likely to reduce costs).

of view, they have the investment costs of CDR without the benefits, including competitive ones (e.g. time to decision, time to provide credit/funds).

Finally, the absence of standardised consents makes it difficult for a lender developing a single lending process, given the process will need to change dependent upon the consents provided. In some instances, it may also lead to arbitrary outcomes i.e. a lender may develop policies to decline credit to those customers who do not provide full CDR data (with such an outcome warranted in some, but not all instances).

**Credit assessment and management issues**

There are two further elements of the consent framework which remain problematic when applied to a lending use case:

- The data minimisation principle (rule 1.8), which restricts the data that is collected to that which is used to provide the requested goods or services to the specific customer (and which otherwise imposes problematic restrictions on obtaining consent to use that data for other purposes). That principle does not reflect how data is collected and used in practice by credit providers. For example, a credit provider's existing algorithm will use data that the credit provider has already identified as being relevant to their credit decision (i.e. the data has predictive value). Under the data minimisation principle, the credit provider would be permitted to collect that data to feed into its existing algorithm (assuming the customer's consent is obtained). However, the credit provider will also need to refine and improve that algorithm. Part of that process is to identify *other* information that may be predictive, i.e. they would collect other information which they suspect may be predictive (but which is currently not incorporated in their algorithm) and retrospectively assess whether the information would have been predictive (i.e. by comparing the performance of the loans provided to the specific customer(s) and seeking to identify whether any of that other information would have helped predict how the customer ultimately performed in respect of the loan). This important and necessary step in refining and improving credit algorithms is currently prohibited under the data minimisation principle.
- The inability to bundle a de-identification consent alongside multiple CDR consents relevant to lending will substantially limit a lender's ability to use CDR data for developing credit score algorithms, credit strategies and verification tools.[4][5]

The lending use cases below set out in some detail how lenders undertake this activity, and why it is necessary that CDR data can be collected and used, in a de-identified format, beyond a single customer, in order to adequately aid the lending process. In that context, it is important to understand that effective use of CDR data can be an involved, lengthy process, including:

- Developing credit assessment policies/ risk strategy: Policy may be derived based on limited data, however for risk strategies more data is required, and for models even more data is required. Robust models require a minimum 12-18 months' performance window (e.g. accounts

[4] In addition to the need to use CDR to develop and refine credit scoring algorithms, a credit provider would need to use the data to verify the effectiveness of their (more basic) income and expense verification tools. For example, income verification is typically undertaken by checking incoming credits to a customer's account from their employer. However, those credits do not distinguish between base income, overtime, commissions, bonuses etc. The credit provider will need to apply certain assumptions to the credits to the account. For example, the credit provider may assume that customers within the travel industry receive high bonuses and commissions and, due to the unstable nature of those types of income, apply a discount to the credit amounts as part of their verification processes. That credit provider will subsequently need to validate whether those assumptions are inappropriate by. for example, checking whether the expected default rate for customers within the travel industry was within the expected range. A higher than expected default rate for that customer segment could suggest the income verification assumptions were incorrect.

[5] We note that there may be concern that once the data has been de-identified it would be beyond the scope of the Privacy Safeguards and therefore could be used for purposes that are not directly relevant to the provision of credit products. To be clear, we are concerned with allowing appropriate de-identification to support purposes that are directly relevant to the efficient and responsible provision of credit. An alternative to broadening the ability to de-identify CDR data is to ensure that the other purposes are properly allowed for. That is, rather than allowing de-identification to support necessary credit-related activities, it may be possible to directly allow that credit-related activities which – if deemed appropriate by the credit provider – could involve deidentification.

opened during a six month time period Jan-Jul '24 and account performance as at Jul '25) with CDR data. It is preferable to have longer performance window e.g. 18-24 months; the lower the volume of accounts with CDR data the longer the account open window required (to get enough volume of accounts to determine performance by score/strategy).

- Furthermore, account performance is required alongside CDR data for an account to assess the model/strategy, this means that whilst de-identified data can be used for the assessment, it must be possible for the lender (or a third party on behalf of the lender) to match the CDR data with the account performance (thus data can't be completely de-identified up to this point).

To be clear, to use CDR effectively lenders will need to use CDR data to be able to both verify the customer's financial situation and to assess the credit worthiness of the customer via a credit scoring algorithm. CDR data should therefore be capable of being used both to verify and assess a customer effectively but also to build the lenders' credit assessment and management database. This enables activities such as validating and improving credit assessment tools, product development, risk management reporting. These uses are vital to the management of an efficient and responsible lending business.

**Examples of lending use cases**

To better understand how lending processes work, and what difference CDR rule changes will make to the lending use cases, we have set out a number of examples below (and within each example sought to illustrate the impact of rule changes).

The first example is a theoretical illustration of the use of the effective use of CDR which would be possible if the above changes were made to the rules (in addition to the other improvements in the proposed consent and operational enhancements amendments). The second example reflects feedback from a Member that has actively considered using the CDR for an income verification use case (including the reasons why it determined the CDR was not currently effective to support that use case).

We appreciate that the use of data by a credit provider (and by entities that support those credit providers) can be complex. We would welcome the opportunity to workshop these issues with you in further detail.

**(i) Use of CDR data – new to lender customer, full CDR participation**

- Customer applies for new credit with CP1 that the customer doesn't have an existing relationship with (this could be for a number of reasons, better interest rate, product features etc.). This means CP1 has no existing records for this customer.
- CP1 is a CDR participant, and all the credit providers that the customer has existing relationships with are CDR participants. The customer consents for all data to be provided to CP1.
- CP1 has sufficient applicants/customers with CDR data that means they have policies and strategies in place to leverage the CDR data, including in automated decisions.
- CP1 receives the information and can use the information (alongside CCR and other information) to verify the customer's financial situation (e.g. income, expenses and existing liabilities) and otherwise assess their credit worthiness (through use of a credit scoring algorithm), and therefore determine what product and product features they can offer the customer.
- CP1 retains the CDR data and use the information to monitor and develop policies, models and strategies. The CDR information is also available for CP1 for review and audit purposes of the credit decision.

*To confirm, the above process is not possible under the current rules (and would remain so even with the changes in the proposed consent and operational enhancement amendments). To give effect to the above scenario, each of the three fundamental rule changes Arca has identified would need to be resolved.*

For instance, the following are potential issues which could arise if 'ideal' situation above doesn't play out:

- Absence of standardised lending consent If the customer doesn't provide full consent for all information to be provided (either not all CP information, or not all account information) that could impact the decision of CP1, or the appropriateness of the decision. If the information passed from

the data holder to CP1 is not an accurate reflection of the customer's account and product offering then that could impact the decision of CP1.

- Credit assessment and management issues remain unresolved

  CP1 cannot develop strategies based on CDR data if 1) it is not possible for CP1 to use CDR data for analytical/modelling purposes; 2) if CDR data has to be de-identified too soon; or 3) it is not possible for CP1 to retain the CDR data for sufficient time to assess historical decisions that include CDR data. In addition, CP1 will have difficulty developing policy and strategy considering CDR data if insufficient applicants/customers have CDR data at point of decision.

  CP1 will have difficulty reviewing decisions that were made considering CDR data if CDR data cannot be retained for sufficient time (e.g. in-house review, audit purposes).

**(ii) Use of CDR data – income verification**

A non-bank Member has sought to test an income verification use case to understand the impact CDR data (under the current rules) would have on this aspect of its lending process.

The feedback from this Member is that the current process would be insufficient to provide efficient income verification, noting:

- The customer experience is unsatisfactory. The onus is placed on the customer to provide this information, they are linked to a portal and required to scroll through 8 different screens and find each of their banks and related accounts.
- The customer is not required to share every account, and for a lender this provides a real challenge as there is no certainty that the information provided represents the complete picture for that customer. Using this income verification tool to aid responsible lending obligations creates challenges.
- For a lender, there is no visibility of what a customer does and what they can't complete in the process. This lack of visibility means this use case, in its current form, is not viable at scale.

Changes which would be necessary to make this use case work effectively are as follows:

- Improved processes to identify customers and link all CDR products to that customer
- Customer sharing all information as part of a standardised lending consent, with necessary validation of that information and the customer's identity. The standardised lending consent requires provision of complete information by the customer.
- The lender is able to receive back summarised views of income, and fluctuations in income based on a 365 day period. The lender can also rely on a third party aggregator to match information alongside CCR framework to provide full view of liabilities.

We would welcome an opportunity to discuss this submission further. Please contact Arca's General Manager, Policy & Advocacy, Michael Blyth.

Yours sincerely,

Elsa Markula

Chief Executive Officer