

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600
Via email: data@treasury.gov.au

7 September 2018

Thank you for the opportunity to provide a submission on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (the draft Bill).

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.

ARCA supports the concept of Open Data and considers that it will promote competition that benefits consumers. In doing so it will also enable access to additional, valuable data to a wide range of credit providers when assessing credit applications from consumers.

However, as noted in [our submission](#) to the *Review into Open Banking in Australia* (Farrell Review), in order to ensure that these benefits are fully realised, any data sharing arrangements require careful design:

- To maintain the integrity and reputation of the system
- To ensure participants don’t abuse their access to consumer data
- To protect consumers
- To make the system efficient and to operate at a low cost
- To provide certainty to participants around what behaviours are acceptable
- To ensure fairness between participants

In respect of the above principles, we note that the adoption of the consumer data right by consumers – and the success of the entire framework – is dependent on consumers having trust in the system. We note the significant reliance under the proposed CDR framework on the concept of obtaining the consumer’s ‘express consent’ to the disclosure and use of data through the consumer data right. We wish to reiterate our comments contained in our submission to the

Farrell Review regarding the limitations of ‘consent’ – regardless of whether it is express – as a means of consumer protection.

This is particularly the case given that it is likely that businesses will begin to make the provision of a product or service conditional on the provision of consent by the consumer. In respect of the provision of consumer credit, we fully expect that some lenders will make the provision of consent under the consumer data rules a condition of applying for the product – where this is done in a way that would still meet the standards for consent outlined in the briefing materials accompanying the draft Bill.

ARCA recognises that the draft Bill establishes the framework for the general consumer data right and that the detail applying to individual sectors, such as Open Banking, will be set out in Rules and Data Standards. We understand that to the extent that the draft Bill diverts from the policy positions taken in the Farrell Review and accepted by Government (e.g. in relation to fees for supply and value-added data), the Rules will apply those policy positions to the Open Banking regime.

In the main body of this submission we set out higher-level policy observations on the consumer data right framework as established by the draft Bill. In *Annexure One* we set out some feedback in respect of specific elements of the draft Bill.

Applying appropriate reciprocity obligations

We note that the draft Bill itself does not establish a reciprocity requirement. We understand that this will be established through the Rules developed by the ACCC under the subsections 56BC(a) and 56BD(a).

Nevertheless, we note that the Explanatory Materials (at 1.46) state:

When in possession of a consumer’s CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants. This is known as the principle of reciprocity.

This concept of reciprocity is unusual.

The principle of reciprocity is generally understood to mean that *in order to obtain data through the data sharing system, an entity must make its own data available to others in that system*. In the context of the draft Bill, this would mean that an ADI which acts as an accredited entity – but which is *also* a data holder in respect of its own created or collected data – must make the information for which it is a data holder available to other participants in the system.

The principle does not ordinarily mean that a data recipient must pass on data that it has obtained through the data sharing system to a third party. In fact, we caution against requiring an accredited entity to pass on such information to a third party. As noted in our comments regarding the interaction with the credit reporting system, requiring an accredited entity to pass on ‘second-hand’ information to another accredited entity raises the risk that the data will not be ‘accurate, up-to-date and complete’ – it would ordinarily be better to require the data holder that initially created or collected the data to directly disclose it to that second accredited entity.

Separately, we note the challenge of identifying the sectors and information (in respect of those sectors) that should be designated under the consumer data right. We understand that an accredited entity will not be subject to the reciprocity obligations unless that entity's sector has been designated.

To ensure the competition benefits of the consumer data right are fully realised, we suggest that in deciding which sectors should be designated, consideration should be given to which as-yet undesignated sectors are regularly obtaining data under the consumer data right – such that, those sectors that are benefiting from the consumer data right should also be amongst the first to be designated. We recommend that this be added to the list of factors to be considered by the Ministers or the ACCC when considering which sectors to designate (as set out in subsection 56AD(1)).

Further, we note that in designating which information must be supplied in the sector – and which would be subject to the principle of reciprocity – consideration should be given to what information *is of value in that newly designated sector*, rather than whether that data is 'equivalent' to the data being made available through other designated sectors.

For example, if it is identified that social networks were regularly obtaining transaction data from the banking sector (e.g. in order to better target advertising), that sector should be subject to designation as a priority - where the information that is to be made available from that sector would be based on an assessment of the value of the information to consumers (i.e. through better competition, innovation etc) rather than whether it is 'equivalent' to the data obtained from the banking sector.

Interaction between the credit reporting system and the consumer data right

In our submission to the Farrell Review we outlined some observations in respect of the interaction between the consumer data right and the existing credit reporting system established by Part IIIA. While we note that the draft Bill recognises the existence of Part IIIA (see, for example, subsection 56EC(3) and Privacy Safeguard 3), it is still not clear on how the consumer data right will work in conjunction with the Part IIIA credit reporting system.

In particular, we note the following specific issues (some of which may be clarified through the designation instrument or the Rules):

- (i) As noted in Item 8 of our submission to the Farrell Review, an accredited data recipient (which is not a credit provider within the meaning of Part IIIA) that receives CDR data from a credit provider 'for the purposes of, or for purposes including the purpose of, providing an entity with information about the credit worthiness of an individual' may be a 'credit reporting business' within the meaning of Part IIIA (see s6P of the *Privacy Act* and s11 of the *Privacy Regulations*), as . As such, the intermediary will be subject to the Part IIIA restrictions as to the types of data that can be collected, the use of that data and the persons to whom the data (or derived data) can be disclosed. In essence, it appears that such a business would be subject to both the Part IIIA restrictions and also the Privacy safeguards. We understand this is not what was intended.
- (ii) Where a credit provider ('first credit provider') has received credit reporting information through the Part IIIA credit reporting system, it will have data (such as

the credit limit) in respect of a consumer's credit accounts held with another entity ('second credit provider'). Depending on the way in which the CDR data is designated under subsection 56AC and the Rules, that information may be 'CDR data' that may need to be disclosed by the first credit provider upon request of the consumer. This means that 'second-hand' information may be disclosed to an accredited data recipient (who has the consent of the consumer to access the CDR data held by the first credit provider).

We strongly recommend that such data be excluded from the CDR data that must be disclosed, given:

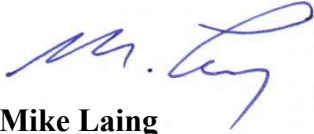
- the disclosure of 'second-hand' data by the first credit provider to the accredited data recipient is inconsistent with the requirements under Part IIIA to ensure that data collected is 'accurate, up-to-date and complete' (see, for example, s21Q of the Privacy Act).
 - it could enable a non-signatory to the Principles of Reciprocity and Data Exchange (PRDE) to receive credit reporting information outside of the reciprocity requirements of those Principles – this is particularly important if a credit reporting body (under Part IIIA) also acts as an accredited data recipient, such that the reciprocity obligations under the consumer data rules would require that credit reporting body to disclose credit reporting information held by it in circumstances that would be contrary to the PRDE (and, subject to the passing of the *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018*, the requirements of that Bill) .
- (iii) As noted in our submission to the Farrell Review, both Part IIIA and the consumer data right enable the sharing of credit-related information between credit providers. However, the consumer data right will significantly broaden out the types of data that may be exchanged, while at the same time removing many of the strict constraints that are placed upon the disclosure and use of information obtained through the credit reporting system. While ARCA welcomes the many benefits that such access to broader data will bring to consumers and credit providers, we consider that the policy implications of allowing such disclosures in the banking sector – which run counter to almost 30 years of regulatory precedence in the credit reporting industry – should be carefully considered prior to the consumer data right becoming operational.

For instance, information relating to the balance of a consumer's loan account and actual repayments made are currently not available through the credit reporting system. Such data is powerful information when assessing a consumer's application for finance. However, that information (together with a large amount of other information) is likely to be available under the consumer data rules. If, as we anticipate, the granting of consent to access open banking data by a consumer becomes a condition of the loan application being assessed, then from a consumer protection perspective, it seems incongruous that a credit provider can't access similar information through the credit reporting system, given the already stringent protections that apply to the use and disclosure of credit reporting information.

We recommend that the interaction between the credit reporting system and the consumer data right be clarified as a priority. We would welcome the opportunity to discuss these matters in-depth with Treasury, the ACCC and the OAIC.

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,

A handwritten signature in blue ink, appearing to read 'M. Laing', is written over a light grey rectangular background.

Mike Laing
Executive Chairman

ANNEXURE ONE:

ARCA’s Submission on the draft Treasury Laws Amendment (Consumer Data Right) Bill

	Issue	ARCA Comments	ARCA’s Submission
1.	<p>Application of the definition of ‘CDR data’ to derived data</p> <p><i>Subsection 56AF(1) Meaning of CDR data</i></p>	<p>The definition of ‘CDR data’ – which is central to both the disclosure obligations and the Privacy Safeguards – applies <i>automatically</i> to all data that is derived from information that is designated under subsection 56AC(2). For instance, if the credit limit in respect of credit cards is designated information, then all information that is ‘wholly or partly derived’ from that information is deemed to be ‘CDR data’.</p> <p>While this may be appropriate when applying the Privacy Safeguards to information held by an accredited data recipient (i.e. so that all the derived information is protected by the Privacy Safeguards), it is not appropriate when considering whether a data holder is obliged to disclose data under the customer data rule.</p> <p>For example, the credit limit on a credit card is almost certainly going to be used to develop various forms of value-added data by the data holder – including the customer behavioural score. Further, when considering the range of data that is going to be designated in respect of the banking products (e.g. balance, transactions, payment history etc), it is likely that virtually <i>all</i> value-added data held by an ADI will, in some form, be ‘derived’ from that designated data.</p>	<p>The definition of ‘CDR data’ be split into two components – one that includes the data designated under subsection 56AC(2), which may include derived data held by a data holder if that is specifically designated, and another that covers data that is derived from that first type data. In this way, the provisions of the draft Bill applying to the ‘disclosure’ of designated data by data holders can be limited to that first type of data, while the Privacy Safeguards applying to accredited data holders can apply to both types of data.</p>

		<p>Based on the current drafting, it appears that data holders would be required to disclose all of that value-added data. This is not the intended outcome (see Recommendation 3.3 of the Farrell Review).</p> <p>While it may be possible for the Rules – in respect of a data holder’s obligation to disclose data – to then <i>exclude</i> derived data (other than derived data that has been explicitly designated), it appears to be an unnecessary complication.</p> <p>Further, the power to require disclosure of data is given to the Minister. If the Minister’s designation automatically applies to all data derived from that designated information, the decision to limit the application of the definition of CDR data by Rules is left in the hands of the ACCC. This is not consistent with the role of the Minister and ACCC as established by the draft Bill.</p> <p>For completeness, we note that paragraph 1.50 of the Explanatory Materials states CDR data will be data outlined in the designation instrument and “any information that is <u>subsequently</u> derived from that data” (<i>emphasis added</i>). This appears to confirm the intention that derived data only be regulated as ‘CDR data’ once it passes through the system established by the consumer data rules – however, this does not appear to be reflected in the proposed drafting.</p>	
2.	<p>Implications for existing data sharing arrangements</p> <p><i>Subsection 56AF(1) Meaning of CDR data</i></p>	<p>It appears that the impact of subsection 56AF(1) is that, once a sector and relevant information has been designated under subsection 56AC(2) then that information is subject to the requirements of the draft Bill – particularly the Privacy Safeguards – regardless of whether or not a particular element of datum has been subject to a consumer data request.</p>	<p>Further consideration should be given to this issue.</p> <p>For instance, it may be possible to limit the definition of ‘CDR data’ to only apply to particular information if and when there has been a request (or purported request) from a CDR consumer for the data holder to disclose that data. In this way, it would be clearer that the draft Bill does not limit or restrict current business-to-business disclosures.</p>

<p><i>Section 56EF Privacy Safeguard 3 – collecting solicited CDR data</i></p>	<p>For instance, if a credit card’s credit limit is designated to be information that is subject to the draft Bill, information relating to the credit limit for <i>every</i> customer of the ADI is ‘CDR data’ regardless of whether there has been any request by the customer under the customer data rules.</p> <p>This has the potential to limit the handling of data by a data holder in ways that are not intended.</p> <p>For instance, Privacy Safeguard 3 prohibits a ‘person who holds an accreditation’ from soliciting ‘CDR data’ unless the data is collected in a manner consistent with the consumer data rules or under “an Australian law, other than the Australian Privacy Principles” (we note that this would permit disclosure under the Part IIIA credit reporting system).</p> <p>We expect that many organisations, including banks or other credit providers, will hold an accreditation under subsection 56CE(1) in order to gain access to the data made available under the consumer data right. However, those organisations will want to continue to share consumer related data between each other <i>outside</i> the regimes established under the consumer data rules.</p> <p>For instance, we expect ADIs, lenders and other organisations would continue to share customer related data for reasons such as:</p> <ul style="list-style-type: none"> • Bank B asking Bank A for information regarding a customer’s existing accounts (i.e. a ‘bank reference’); • Bank A seeking credit reporting information from a credit reporting agency in respect of non-consumer accounts; • Bank B undertaking due diligence on Bank A’s portfolio prior to purchasing Bank A; • Bank A sharing information about a customer’s accounts with a related body corporate. 	<p>Alternatively, it may be possible to limit Privacy Safeguard 3 to only apply when the accredited data recipient is acting, or purporting to be acting, upon a request from a consumer exercising their rights under the consumer data right.</p>
--	---	---

		<p>These activities are currently permissible, subject to having the appropriate consents under the Australian Privacy Principles. The disclosures are not ‘required or authorised’ under any other Australian law.</p> <p>Based on the current drafting, it appears that such disclosures would be prohibited – because the recipient of the data <i>incidentally</i> holds an accreditation under subsection 56CE(1). We don’t believe that this is an intended outcome.</p>	
3.	<p>Receiving unsolicited ‘CDR data’ outside the consumer data rules</p> <p><i>Section 56EG Privacy Safeguard 4 – dealing with unsolicited CDR data</i></p>	<p>Similar to the issue identified in Item 2, entities that hold accreditation may receive account-related information from consumers in circumstances unrelated to the consumer data rules. For example, a credit provider may receive a hardship application assistance form from a customer which details that customer’s banking and credit relationships with other entities. Based on the proposed definition, that data appears likely to be ‘CDR data’ – where the provisions of Privacy Safeguard 4 appear to require the credit provider to destroy that ‘unsolicited’ data.</p> <p>For completeness, we confirm that this Privacy Safeguard would not apply in circumstances where an accredited entity receives CDR data (with the consumer’s consent) for the purposes of providing a product or service to the consumer – but the consumer does not proceed with that product or service.</p>	See Item 2.
4.	<p>Notifying of the collection of CDR data</p>	<p>We note that Privacy safeguard 5 applies to data collected in ‘accordance with section 56EF’. This would appear to include data (which would otherwise meet the definition of CDR data) that is collected in accordance with other Australian laws (as per paragraph 56EF(b)).</p>	Clarification that the requirements of Privacy safeguard 5 do not apply to data (which otherwise meets the definition of CDR data) collected in accordance with paragraph 56EF(b).

		This contrasts with the similar provision in Privacy safeguard 6 which applies the requirements of subparagraph (b) only to data collected in accordance with paragraph 56EF(a).	
5.	Third parties exploiting consumer's right to data	<p>As noted in our submission in relation to the Farrell Review (see Appendix 1, item 3) an unaccredited party could circumvent the consumer protections in place under the draft Bill by encouraging a consumer to access their own CDR data directly for the purposes of passing that data on to the unaccredited party.</p> <p>In this way, the third party would gain access to that data without the restrictions under the Privacy Safeguards and without meeting the security requirements that will apply to an accredited data recipient. This places at risk both the consumer's privacy and the security of the data holder's business. It would be unacceptable for an unaccredited third party to develop a large, unsecure database of sensitive information relating to the customers of a data holder.</p> <p>While we recognise that a consumer should be free to access their own data without unnecessary restrictions, this should not prevent the Bill from addressing this risk.</p>	<p>The Bill should include a rule making power that, in relevant circumstances, enables the ACCC to apply the requirements of the Bill (including the accreditation requirements and the Privacy Safeguards) to entities that actively solicit CDR data directly from a consumer (e.g. where the business encourages the consumer to exercise their rights to request disclosure of that data from a data holder for the purposes of passing it onto the unaccredited third party).</p> <p>In this way, the consumer's own right to access the data is not restricted. However, businesses that may potentially receive significant amounts of consumer data will be appropriately regulated (and the incentive to act outside of the consumer data rules is minimised).</p>