AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

18 January 2019

Comments on the Treasury's Privacy Impact Assessment

Thank you for the opportunity to comment on the first version of the Privacy Impact Assessment (PIA).

We have the following feedback:

1. We are concerned with the example given on page 71 in relation to an imbalance of power with service providers. The PIA earlier notes that the CDR is intended to support improved compliance with regulations, including responsible lending processes (p20). It is concerning that a lender who requests consent to access CDR data for these purposes could be an example of an 'imbalance of power' that could mean the consent is not freely given and voluntary. There is no requirement for a lender to approve a loan in any circumstances, and it has long being accepted that at least in terms of loan applications, the information balance of power rests in favour of the consumer. It is because of this that governments on most countries have legislated to enable credit reporting systems to emerge to address part of this power imbalance. Secondly, the example appears to be inconsistent with the earlier statement regarding the intent of the CDR regime. We suggest removing that example or, at a minimum, clarifying that it may only be a problem if the bank requested access to data that went significantly beyond that which is required to assess and manage the loan, i.e. data that had no relevance to the loan.

2. In addition to whether authorisation is "genuine" and "complied with", the description of 'authorisation risk' (p.46) should recognise that this also incorporates the risk of the authorisation being understood to mean different things by the consumer and the accredited data recipient (ADR).

3. We suggest that Risk 2.1 (p55) include an example of a consumer consenting to data being used to "assess a policy of insurance" without realising that the insurance provider may use the data to assess the consumer's price sensitivity, rather than the simply pricing for risk. In respect of the purchase of an insurance policy this could involve several hundred dollars a year in higher premiums to the customer. However, if this example was followed across other financial products, the loss could be higher. On that basis, we suggest that the Risk Severity be increased to Moderate.

4. We suggest that the Risk Likelihood of Risk 2.6 (p56) should be upgraded to Almost Certain as some businesses will almost certainly decide that acting outside of the CDR regime (i.e. by asking the consumer to obtain the data directly and then handing it on) is preferable to

being accredited and therefore, potentially, subject to reciprocity. This may be done by both legitimate businesses but also fraudulent parties using the CDR system as a way of 'phishing'. We suggest that the phishing example be include in the PIA, noting that the fraudulent entity may rely on consumers' general lack of financial literacy to convince the consumer to share the data.

5. The description of risks for Joint Accounts (p63) should recognise that, for most personal accounts, each joint account holder is already legally entitled to the account related information (e.g. transactions). For example, s194(3) of the National Credit Code (NCC) requires notices or other documents (e.g. statements) to be given to each joint account holder, unless an account holder elects not to receive the documents (with that election able to be withdrawn at any time). There is nothing to stop that joint account holder from sharing that information with other people without the other account holder's knowledge or agreement. Therefore – at least for personal accounts – this is an existing state-of-affairs and is not a risk associated with the CDR system. In fact, under the NCC, the ability for each joint account holder to receive information regarding their loan independently of the other account holder is a key consumer protection.

   As we have noted before, by overstating the significance of this issue, the CDR Rules may overly complicate the arrangements relating to joint account holders, and may result in data recipients relying on current methods of data sharing – such as screen scraping – which would not involve those limitations.

6. Further to the above point, in seeking to address the perceived risk associated with joint accounts, the system (as proposed) will create an additional, serious privacy risk by giving notice to the joint account holder of the other account holder's attempt to share data. As noted in the example relating to Amanda's family law practitioner (p64), there is a risk that an abusive partner could block the sharing of data. However, of more importance is the risk that an abusive partner could become aware of Amanda's attempts to obtain legal advice in relation to the relationship, which could prompt further violence. At a minimum, this risk example should be included in the PIA.

7. We disagree with the comments made on page 66 regarding the limited potential for Non-Accredited Entities applying "pressure to individuals to provide their personal information outside of CDR frameworks as a condition of receiving a service". Likewise, we do not agree that ensuring data holders are not required to provide the direct-to-consumer access through APIs will prevent unscrupulous entities from taking advantage of the direct-to-consumer process (p110). As noted, the data holder would still be required to provide a mandated and standardised set of data in a "user-friendly digital format". It would not be hard for an entity seeking to work outside of the CDR system to establish a system to automatically read that data (at least for the larger data holders). Entities seeking to profit from consumers' data – both legitimate and illegitimate – will innovate and will look for the easiest way to do that. Based on the structure of the CDR system, there will be significant advantages and – at present – little disincentive to act outside of the CDR Rules. As we have noted in previous submissions, we are not suggesting that the consumer be prevented from accessing their data directly. Rather, we think the legislative framework should give the ACCC greater power to intervene if it identifies that entities are inappropriately seeking to avoid the CDR Rules by exploiting the direct-to-consumer process.

8. Further to the above point, there may be some valid products that give consumers the ability to manipulate and utilise their data themselves (e.g. budgeting and financial management tools), without that data being shared with the provider of the product. Those products would be more efficient if they could tap into the APIs, rather than requiring the consumer to download and import the data through an Excel spreadsheet (or like). Inserting "friction" into the direct-to-consumer right to discourage third parties from exploiting that channel may discourage the legitimate development of those DIY tools and give consumers fewer choices that don't involve sharing of their data. In addition to our suggestion regarding the ACCC's powers, it may be appropriate to consider how such tools could operate under the CDR system.

Consumer education

We welcome the focus on consumer education in respect of the CDR system. ARCA – through its industry funded CreditSmart program – is undertaking a similar education campaign in respect to the comprehensive credit reporting reforms. The CreditSmart campaign aims to educate and inform Australian consumers about the nature of the changes and the potential impacts to the consumer. As with the CDR, the CCR reforms involve complex changes that did not involve a straightforward, one-off message to the consumer. CCR is being implemented in stages over a multi-year timeframe reflecting the varying degrees of different participants to join the system, and their own priorities in terms of when various products enter the system. CDR will also involve a staged rollout by different participants and products. This is unlike other consumer education programs, such as the 'PIN@POS' campaign, which had to convey simpler messages, i.e. that a PIN would be required on all cards at all POS terminals from a particular date.

Based on our experience, we provide the following observations regarding the process to educate consumers about the CDR system:

- The education campaign must be a multi-year process – ideally over a period of up to 7 years. It is our experience that consumers are unlikely to engage with the message until they find themselves directly impacted by the change. Given that the CDR will be subject to a reasonably 'soft-launch', an education campaign that does not continue for a significant time beyond that launch will not succeed. The campaign will need to be reviewed and relaunched when additional sectors are added.
- The campaign should include a public relations component to ensure that the media is also providing a consistent message to consumers.
- The education campaign must recognise that the financial literacy level of Australian consumers is often not high. As noted in the PIA this will provide additional challenges for some vulnerable parts of the community.
- Each participant (i.e. data holders and ADRs) will need to provided consumer education to their own customers. It is important that the messages given across industry is consistent. In addition to educating consumers directly, as part of the process, the ACCC and OAIC should ensure that standardised messaging is provided to participants for use in their campaigns – such messaging should be developed in conjunction with relevant stakeholders.

We would be very happy to meet with the Treasury, the ACCC and OAIC to provide further insights from our experience. We note that the CreditSmart website has a 'contact us' section through which we receive regular queries from consumers. This may be of particular use in

designing the CDR education campaign as it gives valuable insight into the types of concerns consumers hold and the level of existing financial awareness.

If you have any questions about our feedback, 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
Executive Chairman