SUBMISSION PAPER:

Submission to The Treasury, Australian Government Privacy Impact Assessment v.1 - Consumer Data Right

January 2019

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 170 FinTech Startups, VCs, Accelerators and Incubators across Australia.

Table of Contents

About this Submission

This document was created by FinTech Australia in consultation with its Open Data Working Group, which consists of over 120 company representatives. In particular, the submission has been compiled with the support of our Working Group Co-leads:

- Melissa Mack, Money Place
- Rebecca Schot-Guppy, Fintech Australia

This Submission has also been endorsed by the following FinTech Australia members:

- CertifiedBy
- ID Exchange
- On Deck
- Prospa
- EzyPay
- Reinventure
- Zip Co

Submission Process

In developing this submission, our Open Data Working Group held Member roundtables to discuss key issues relating to the Privacy Impact Assessment. Given the constricted timelines of release and response to this submission over the Christmas / January holiday period, our Members have not had the opportunity to fully consider all of the issues presented by the Privacy Impact Assessment. Further submissions are therefore likely to be forthcoming and/or presented by our Members in later rounds.
We also particularly acknowledge the support and contribution of DLA Piper and K&L Gates to the topics explored in this submission.

Context: Open Banking in Australia

FinTech Australia has been a consistent advocate for policy reform to drive the implementation of an Open Financial Data framework in Australia before the end of 2018. We have made numerous submissions to Federal Treasury, the Productivity Commission, the Open Banking Inquiry and Data 61 on the need for an Open Financial Data framework and on the details of that framework.

FinTech Australia will continue to engage on these broader issues, including by liaising with the Australian Competition and Consumer Commission (**ACCC**) in relation to the development of the Rules Framework including Privacy Safeguards, and Data 61 in relation to the underlying Consumer Data Standards.

Privacy Impact Assessment - Consumer Data Right

FinTech Australia welcomes the opportunity to put forward its position on behalf of its members in relation to the privacy implications of the introduction of the Consumer Data Right and, specifically in this submission, the Privacy Impact Assessment ('**PIA**') released by The Treasury on 21 December 2018.

1. PIA Recommendations

Fintech Australia broadly supports the nine overall Recommendations of The Treasury as outlined in the draft PIA to address the privacy risks in the CDR system as set out in this review and to adequately protect CDR participants. Many of our Members have been strong advocates of, the need for an open and transparent regime which protects the individual privacy rights of CDR consumers.

We have highlighted below a selection of key issues which we believe are important to finalisation of the Recommendations and the PIA.

Consent based Mechanism

We support, in particular, Recommendation (No 3) that the ACCC and OAIC continue to work together to ensure that the key framework underpinning this regime is one that supports express consent from CDR consumers, and protects vulnerable individuals.

Key to the success of the CDR regime - for all sectors and all participants - is an easy to use and to understand consumer consent framework. We acknowledge references to the attempts made by the Treasury to assess similar consent-based regimes (e.g. the EU GDPR) and the complexity of obtaining and validating, in practice, express consent particularly in cases where there may be an imbalance in power between the consumer and the entity holding the data, whilst at the same time balancing the need for consent to be informed without over-loading the consumer with information on the scope, purpose, duration etc. of this consent. We strongly advocate for a simple, seamless and

cross-sector consent mechanism. On this specific issue, our Members have raised some further issues which we believe are important to address in the PIA:

- **Non-Sectoral approach** - Our Members appreciate that the intent and scope of the CDR is to ensure insofar as feasible consistency across sectors. We also acknowledge Treasury's statement and rationale that the Rules are the most appropriate mechanism to ensure adoption of a sector-based approach. However, there is continued concern from our Members that consistency across sectors will not be achieved on such critical areas, such as the definition of what constitutes 'valid' express consent' for the purposes of the CDR Bill, where the form and nature of this consent is enshrined in the Rules only. The PIA acknowledges that the current ACCC Rules framework are based on the risk levels for financial information only - with an implication that differing standards could apply for newly designated sectors (e.g energy & telecoms). Given the ubiquitous nature of innovative technologies and the ability to export from one market sector to another, enabling trade in data to occur cross-sector and cross-industries, having a common framework and basis for consent will be vital to ensuring this cross-sector innovation can be seamless. Having a legislative regime in place which allows for the potential for different consent thresholds to be applied cross-industries or for the nature and form of consent to be different across sectors, significantly hinders data portability & interoperability - core objectives of this regime. To this end, we advocate that the CDR Bill is the more appropriate place to incorporate a properly defined consent model. Considerations as to necessary appropriate exemptions, on a per sector basis, could be captured under the relevant sector Rules, but these should be on an exceptions-only basis.

- **Consistency on definition of 'consent'** - Further, the use throughout the text of the legislative framework, including the Rules, draft CDR Bill and Privacy Safeguards, as well as the PIA draft, of interchangeable terms describing the nature and form of the consent required (e.g. the Rules refer to 'genuine' consent, 'valid' consent and 'explicit' consent, each being used interchangeably throughout), indicates at least some confusion, as well as a lack of clarity on the appropriate consent-based mechanism that should apply. Further clarify on definitions and the form and nature of consent must be incorporated.

- **CDR Policies and Notifiable Information** - We note that part of the requirements for providing fully informed consent to CDR consumers, that a CDR policy (in similar form to an APP privacy policy) must be prepared and maintained by ADR's and relevant data holders. This also includes (at Section 55EF(5) of the Bill as supplemented by Part 8 .4 of the Rules) - in the case of ADR's only - the policy must set out 'listed outsourced service providers, the nature of their services, and the CDR data that has been disclosed to them'. We would submit that individually listing each outsourced provider to whom information be disclosed will be a challenge for many organisation - and this may be further complicated by the use of automated or other technologies in the collection and/or disclosure of CDR consumer data. Analogous to similar positions under the GDPR, (where 'recipients *or category of recipients'* is used) it is submitted that classifications or 'categories of outsourced providers' instead be identified. Further listed details need only be provided where such providers are located outside of Australia / overseas.

- **Balancing Innovation & Privacy**

  We acknowledge Recommendation (No.4) and the need for strong privacy protections to drive up consumer confidence in the CDR system. However, we would not agree with the positioning in this Recommendation of regulators not placing 'undue weight on the benefits of competition and innovation", given the value of competition in this market - and in this regime. There is a need to foster a safe environment to encourage the growth of competition and avoid stifling innovation. There are also privacy benefits to a properly operating CDR (as opposed to screen scraping).

2. Consumer Data Right - Privacy Safeguards

The CDR system provides for the application of the Privacy Safeguards (as minimum protections) to all CDR data and in particular to bind all accredited data recipients (**ADRs**). The Privacy Safeguards are a much more restrictive regime that the Privacy Act and apply to a broader class of data than that captured by the APPs (applying to information that 'relates to' an identified or identifiable person and information 'derived' from CDR data). It is noted also that 'to minimise the complexity of the CDR regime', the Privacy Safeguards will not apply to data holders (who will remain subject to the Privacy Act & APPs, as

applicable) until a request is made, in which case they will apply only to the data being requested.

We understand further that the Privacy Act will apply to protect non-CDR data held by small businesses where that small business is an accredited recipient under the regime - effectively switching-on the APPs for small business previously exempt under this latter regime, with the more restrictive Privacy Safeguards applying to all CDR data. Fintech Australia reiterates some concerns on this approach:

- **Privacy Safeguards v APPs** - As has been highlighted in prior submissions, there is a risk of some confusion between the application of the two privacy regimes, which is particularly pertinent in the case of SME businesses who would have been previously exempt under the Privacy Act & APP regime.

  Further, from a regulatory perspective, it is critical to clearly identify the boundaries of the CDR scheme, and to ensure that all organisations are clear about when the Privacy Safeguards apply, and when APP applies, so as to avoid overlap in the two regimes. Whilst this risk is noted in the PIA it is not clear on how this delineation risk has been mitigated, particularly given the broader scope of CDR data (including by reference to 'derived data'). Further clarity on the hierarchy of the two different regulated regimes is also required - many businesses may be both holders and consumers of CDR related data.

- **Regulator collaboration**: We note that an information sharing agreement / MOU between ACCC and OAIC is one of the recommendations to support clarity on enforcement, but changes to the Bill and the Rules are also recommended as critical to enshrine clarity in the CDR legislative framework.

  Further clarity on the graduated powers of each Regulator is also required - this has not received the attention to detail that we would expect for such game-changing legislation.

  Additionally, on the point of an MOU / information sharing agreement, this should include the views of other interested sector-focused regulators (including e.g.

RBA) as well as the Data Standards Body to ensure that all cross-regulator issues are captured.

- **Burden for SMEs** The proposed regime results in a requirement for all ADRs including SMEs to differentiate and ring-fence internally between (at least) two data sets - CDR data and non-CDR data - with alternate regimes applicable to each. (This could be further complicated for any organisation / SME subject to the GDPR regime and where EU data sets are also required to be segregated). Whilst one option is for the ADR to adopt the more restrictive Privacy Safeguards for the protection of all datasets, aside from the (potentially prohibitive for SME's) additional administrative burden and operational costs this would incur, it is noted that there are divergences between the two regimes that would make this inefficient. This may act as a deterrent for SMEs who were previously exempt under the Privacy Act from engaging in the system - which may result in a stifling of future innovation from the start-up and SME community. There is a need for compliance processes associated with the CDR regime to be able to balance both the need to properly assess data and security risks and safeguard the consumer, whilst allowing innovative new entrants and start-ups to participate and thrive.

3. Impacts on Privacy

- **Screen-Scraping Restrictions** - It is noted in the PIA that the introduction of CDR may also present an opportunity to consider whether other methods of providing access to sensitive financial data, particularly screen scraping, should be restricted in light of the availability of the more secure and protective CDR method. As proposed in earlier submissions on the Open Banking regime, our Members submit that where a direct data connection via the CDR is not yet an option — either for the data holder or ADR — use of other secure, proven data capture technologies (including screen-scraping) should *not* be restricted. Consistent with our previous submissions, our Members believe that customers should be empowered to provide permissioned access of their financial account data to third parties securely and easily, using whatever secure application or technology they wish without charge or restriction. Such charges or restrictions would have the potential of stifling of innovation due to increased barriers to entry for early-stage Australian fintechs. Our Members further note that this has been an allowed back-up service in other markets that are moving towards open

banking and it be unwise for this regime to put in place a regime which is out of step with international markets progress in this area.

- **Non-CDR Recipients** - We note that transfers of data out of the CDR system will be possible, but highly restricted. However, we do not believe that the PIA or Rules Framework has to date properly articulated the process around 'non-CDR recipients' and what 'out of the CDR system" means, either in form or practice. For example, how will usual categories of recipients such as service providers, accountants, Amazon Web Services (AWS) be classified or managed in the CDR system. There needs to be much more clarity provided on what 'out of the CDR system' actually means - for all organisations.

- **Data Deletion / Retention** - We note that the Framework proposes that data 'must be deleted or de-identified upon any use permissions being spent' (as per the PIA). Our Members broadly support this proposition, but submit that there may be circumstances which require relevant data to be retained beyond the specific consent use case. This is similar to the position in respect of personal information which is required to be retained for legal or tax reasons etc. in relevant circumstances, but is also more broad than this, when considering CDR data is a much broader category of information. For example, if raw data is collected as part of an underwriting assessment, a recipient may need to store the records on why a decision was made. Further consideration is required on the exceptions to and circumstances of data deletion / retention.

5. Risk mitigation

- **Supporting a Consumer Education campaign**

  As set out in earlier submission on the Open Banking regime, FinTech Australia and its members strongly support the PIA's recommendation that a consumer education campaign be run in conjunction with implementation to ensure large take-up of the regime by both would-be accredited entities and consumers. Education in particular to consumers on the privacy risks and providing assurance and clarity to consumers to enhance trust must be a priority.

  Further, as noted in the PIA survey results, many consumers favour trust in the banks over smaller financial institutions / fintechs. As such, the education

campaign will be crucial in changing consumer perception and increasing take-up of the open data and CDR regime. The banks, in particular, should pay a larger - and more transparent - role in educating consumers given the trust placed by many individuals in the larger institutions to protect and safeguard their data. This trust must be shared with the SME and fintech community and the banks have a significant role to play in improving the 'trust deficit' with neobanks and fintechs, in particular.

- **Continuous Review**

  It is also extremely important to ensure that the rules and standards initially established throughthe roll-out of the CDR regime are continuously reviewed and updated over time to ensure they are continually in line with global best practice, and are also inter-operable with rules being developed for other designated industry sectors. We are pleased to see a post-Open Banking implementation review will be undertaken with lessons learned to be applied to future designated sectors. Nonetheless, as set out in previous submissions, an annual formal review process for at least the first 5 years should be undertaken by the ACCC and DSB (for the banking sector) around key areas such as the Rules design, Accreditation process, and minimum security standards.

Conclusion

FinTech Australia thanks The Treasury for the opportunity to provide inputs and recommendations on the development of the Consumer Data Right, including in respect of privacy issues and the Privacy Impact Assessment. We will continue to engage on the broader issues in relation to this Privacy Impact Assessment and Open Banking.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech Industry, representing over 120 fintech Startups, Hubs, Accelerators and Venture Capital Funds across the nation.

Our vision is to make Australia one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to drive cultural, policy and regulatory change toward realising this vision.

FinTech Australia would like to recognise the support of our Policy Partners, who provide guidance and advice to the association and its members in the development of our submissions.