# ACCC consultation on proposed changes to the CDR Rules

## Submission from Finder

Thank you for the opportunity to provide input into this consultation on the proposed changes to the Consumer Data Right (CDR) Rules. Finder continues to be very supportive of the CDR, which we believe will empower Australians to take control of their personal data and use this information to make better financial decisions.

Finder.com.au (Finder) is Australia's most visited comparison website, with more than 2.6 million Australians using our site each month[1]. We help consumers to compare products across more than 100 categories, including credit cards, home loans, transaction accounts, savings accounts, insurance products, superannuation, telecommunications and energy. Our purpose is to help people make better decisions, and our guides, calculators and comparison tables enable better decision making across a range of complex products and services. Finder is proud to be an Australian-owned fintech business that has succeeded in growing internationally. We now have offices in Sydney, New York, London, Toronto, Manila and Wrocław.

In this submission we have focused on a limited number of the proposed changes from the consultation paper where we have formed a view or where we think we can add value. Given more time we would have provided a more complete submission. Where possible we would welcome further consultation on the proposed changes before implementation.

[1] 2.6 million average unique monthly audience (Oct–Dec 2019), Nielsen Digital Panel

## **Section 3:** Increasing the number and types of businesses that can participate in the CDR

Finder is supportive of the ambition to introduce more businesses into the CDR regime. We also strongly agree with the principle that any changes that lower the requirements to become accredited for the regime need to be carefully balanced against privacy, information security and user experience considerations. Our primary recommendation on this topic is that more consultation should be undertaken to reach an optimum outcome for both consumers and organisations interested in lower levels of accreditation. We would advocate for workshops forming part of this consultation process to ensure more voices can contribute to the conversation. Below we will provide our initial views on each model outlined in the consultation paper.

### 3.1. Restricted level: limited data restriction

Finder is broadly supportive of this type of restricted data access. Lowering accreditation requirements relative to the risk of particular data in scope is a sensible approach and is aligned to the "risk-based accreditation" outlined in the original Open Banking report from February 2018. We also agree that transaction data is the highest risk banking dataset from a privacy standpoint and should be out of scope for this kind of restricted data access.

Our understanding from the consultation paper is that the requirements for the proposed restricted accreditation would be largely the same to those for an unrestricted accreditation with the exception that an independent assurance report would be replaced by a self-assessed attestation statement for the information security obligations. For many providers the cost of the independent assurance report will be less than the costs of meeting the information security requirements. As such, it is not clear to us how attractive this level of accreditation would be to potentially interested parties that will still be required to do much of the same work for a lower level of access to the CDR data.

We also note that replacing the independent assurance report with an attestation statement signed by an executive from the data recipient may introduce a risk of adverse outcomes for the CDR regime. The information security obligations are complex and we can envisage a scenario where an interested party and/or its authorised representative do not fully understand the obligations before completing the attestation statement. A scenario like this could lead to lower levels of information security being present within the CDR ecosystem and this may increase the risk of a data breach that undermines the rest of the regime.

### 3.2. Restricted level: data enclave restriction

Finder would require further information on the data enclave model before taking a position on whether we are supportive or not. We do think that the ability to access CDR data with only a subset of

the information security obligations will lower costs for interested parties and could make participation in the CDR regime attractive to more participants.

However, we do worry that this model could introduce further complexity to the messaging required to explain the CDR to consumers in a data sharing arrangement that is already not well understood and is difficult to explain succinctly. We also note the same potential risk for the data enclave model as outlined above in section 3.1 in relation to self-assessed attestation statements for the information security requirements.

In future consultations we would welcome more clarity on which party would be responsible for consent requests and if there would be a requirement to explain the data enclave model to the CDR consumer. We would also welcome further information on the potential commercial agreements that would be possible under the data enclave model.

### 3.3. Restricted level: affiliate restriction

In line with our comments in section 3.1, we are not sure how attractive this level of accreditation would be for potentially interested parties if they are still required to do most of the work that could get them unrestricted access to the CDR regime. We would also welcome more clarity for this model on which party would undertake consent requests and the extent to which the consumer needs to be made aware of the affiliate relationship.

### 4.2 Transfer of CDR data between accredited persons

Finder is broadly supportive of the notion of enabling the transfer of CDR data between accredited persons. We think this could enable some interesting use cases that would help customers make better financial decisions. On this point we would welcome more clarity on whether this proposed rule would also enable an accredited data recipient to share CDR data with an accredited data holder as well as other accredited data recipients.

On the consent for this type of data sharing, we'd recommend that a second request is presented to the consumer at the point of possible data transfer between accredited persons. Differentiating this consent request from the initial CDR data sharing consent request should help the consumer to better understand what data is being shared with which accredited persons and why.

### 5.2. Disclosure of CDR insights

Finder is broadly supportive of the proposed rules to permit accredited parties to share insights derived from the CDR data to any person with a consumer's consent. We agree that this may help with certain use cases like the ones outlined in the consultation paper. Similarly to the transfer of CDR data

between accredited persons, we would recommend that a new consent request is sent to the consumer before CDR insights are shared.

### 7.2. Amending consents

Finder is supportive of a simplified approach to amending consents and we are particularly supportive of the proposed rules to allow for pre-selected options during the consent amendment process. We would also welcome a similar simplified approach where pre-selected options are permitted when a consumer is renewing CDR consents that have expired.

### 7.5. Improving consumer experience in data holder dashboards

Finder is supportive of this proposal as we believe it will help the consumer to understand which data sharing agreements are linked to which applications or products they are using (or not using). We would welcome further consultation from the Data Standards Body on the metadata that could be provided by accredited data recipients for inclusion in data holder dashboards.