FinTech Australia

SUBMISSION PAPER:

Submission to Federal Treasury

Proposed Changes to the Consumer Data Right - Version 3 of the Rules

August 2021

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.

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 developing this submission, our Open Data Working Group held a series of Member roundtables to discuss key issues relating to the proposed changes.

We also particularly acknowledge the support and contribution of K&L Gates to the topics explored in this submission.

Context: Consumer Data Right

FinTech Australia has consistently supported the implementation of Open Banking in Australia, and strongly supported the CDR Intermediaries proposals of July 2020. In the past, we have made submissions to the Federal Treasury, the Productivity Commission, Open Banking Inquiry, the Australian Competition and Consumer Commission (**ACCC**) and Data 61 on the need for an effective and efficient Open Banking framework.

Now, in July 2021, we are avid supporters of the proposed changes to the Consumer Data Right (**CDR**) framework that will increase access to and participation in the CDR regime.

During the consultation phase for Version 3 of the CDR Rules (**Draft Rules**), we have sought insight from FinTech Australia's members and key players who will implement the Rules in practice.

We find these Draft Rules to be a productive step towards increasing access and participation to the regime. We envision that the Draft Rules can achieve the intended rates of CDR utilisation and provide Australian consumers with innovative products to support their financial health. We have outlined below areas where we consider the Draft Rules require further modification to deliver on these aims. In particular, FinTech Australia considers that the Draft Rules need to provide for a broad spectrum of models for accessing the CDR, enabling consumers and industry to design compliant and practical solutions. This is how innovation is best fostered.

1. CDR Access Models

FinTech Australia are supportive of tiered levels of accreditation that work to significantly increase use cases and participation in Open Banking.

While there is considerable overlap and similarities between the proposed access models, FinTech Australia is comfortable that industry will decide which model is most suitable for their business structures and level of participation in the CDR regime.

1.1 Sponsorship Model

Access

FinTech Australia supports the inclusion of the Sponsorship model, alongside the other access models.

The Affiliate accreditation process, as currently proposed, is only slightly less burdensome than the accreditation process for unrestricted accreditation. As such, FinTech Australia questions whether this marginal benefit will justify the additional requirements which come with the Sponsorship model.

We anticipate that Sponsors using this model will need to establish an assessment framework to ensure a prospective Affiliate is compliant. FinTech Australia considers that it would be useful for the Draft Rules to contain more detail about the expectations on Sponsors in this regard. Similarly, the Draft Rules should clearly define the levels of liability of a Sponsor in connection with its Affiliates. For example, FinTech Australia members seek confirmation that a breach of the CDR Rules by an Affiliate will not necessarily be regarded as a breach of the Sponsor's obligations under the Draft Rules. In particular, Rule 2.2 refers to the Sponsor taking "reasonable steps" to ensure the Affiliate complies with its obligations and Schedule 2 Part 2 Requirement 7 refers to a third party management framework which is to include "post-contract requirements".

Process

Under the Draft Rules, it is contemplated that an Affiliate would obtain accreditation from the ACCC first and then seek a Sponsor. We consider it would be preferable for sponsorship to be obtained first. This would reduce the likelihood of Affiliates undertaking a forum shopping exercise to identify prospective Sponsors with weaker controls. This would also enable the ACCC to get comfort from confirmation that a Sponsor has examined the prospective Affiliate and become satisfied that it could be compliant.

Branding

The Draft Rules do not adequately outline the requirements surrounding branding under the Sponsor/Affiliate model. As liability is shared under the model, members may assume that a Sponsor/Affiliate would be jointly branded, while a CDR representative would use their own branding. Further clarity is required in this space.

1.2 Representative model

Access

FinTech Australia supports the inclusion of the Representative model, alongside the other access models.

Liability

FinTech Australia acknowledges the need for the Principal under this model to be responsible for the conduct of its CDR Representatives. This risk can be appropriately managed by Principals in their commercial arrangements with CDR Representatives. However, FinTech Australia seeks confirmation that the civil penalty provisions in the CDR Rules would not apply to a Principal in respect of the conduct of its CDR Representatives. While it is necessary for Principals to be liable to consumers in respect of the conduct of their CDR Representatives, the civil penalty regime should only punish a Principal for its own conduct (even where that conduct is a failure to adequately supervise its CDR Representatives). This would align this model with the authorised representative model utilised in financial services, where the licensee is fully responsible to clients, but only exposed to civil penalties and criminal offences for its own conduct.

Consent

FinTech Australia assumes that the intention would be for the CDR Representative under this model to collect the consumer's consent. We seek further feedback about any disclosure which will be required about the CDR Representative's status and whether this will involve disclosures concerning the Principal. While FinTech Australia fully supports transparency, we are also keen to ensure that the process does not confuse consumers.

1.3 Trusted Adviser

Access

FinTech Australia supports the inclusion of the Trusted Adviser model, alongside the other access models.

Principles-based definition of Trusted Advisers

The current approach to the definition of Trusted Advisers narrowly confines it to listed occupations. We are concerned that this approach will eliminate people performing equivalent functions for consumers. The genesis of the CDR Regime lay in giving consumers control over their data. Under the Draft Rules, consumers will still not have the ability to share their data with persons who they wish to share it with. Downloading the data into a spreadsheet and emailing it will remain a preferable option for many. This has the potential to undermine a key use case for the CDR.

For example, a number of small businesses employ the help of bookkeepers and family or friends for doing vital business tasks. The current approach to Trusted Advisers cannot accommodate these arrangements.

Instead, FinTech Australia considers a principles-based approach to defining Trusted Advisers will better achieve the intended effect.

In order to ensure that CDR delivers on its aim of providing consumers with greater control of their own data, we consider that a principles-based approach to defining Trusted Advisers provides the needed flexibility in this regard.

Due diligence under the proposed approach

Even if the current approach to defining Trusted Advisers is retained, FinTech Australia consider it is impracticable to impose due diligence obligations on Data Holders and ADRs seeking to share data with Trusted Advisers.

We presume it would be necessary to seek confirmation that the Trusted Adviser is on one of the professional registers mentioned in the definition. There are a number of registers currently referred to and not all of them are capable of interrogation in an automated way. It is not clear how often it is expected that the registers would be checked to ensure the Trusted Adviser remained on the relevant register. Further, if Data Holders and ADRs are required to verify a Trusted Adviser's status, this would also necessitate verifying the identity of the Trusted Adviser.

By way of contrast, when an AFSL holder seeks to rely on a wholesale client certificate from an accountant, ASIC has made it clear that it does not expect the AFSL holder to verify the accountant's credentials. An equivalent approach should be adopted here.

Additional categories

Again, if the current approach to defining Trusted Advisers is retained, FinTech Australia seeks the inclusion of additional categories of person. For example, our members consider the following should be included:

- insolvency practitioners;
- actuaries;
- business consultants, farm advisers, etc;

- bookkeepers; and
- stock brokers.

Liability

FinTech Australia anticipates that, once data has left the CDR Regime (by being disclosed to a Trusted Adviser), any entities which had been involved in providing the data to the Trusted Adviser would no longer have liability for how that data is held or used. FinTech Australia seeks confirmation in the Draft Rules that liability ceases at this point.

Trusted Advisor Consent

The Trusted Advisor (**TA**) Consent can be a one time or periodic consent. If there is periodic consent, it is not clear how the validation of the TA will occur. Given the TA may leave the profession. FinTech Australia seeks further clarity in this area of the Draft Rules.

1.4 Other models

FinTech Australia has previously been supportive of a data enclave model of access. The Draft Rules contain a number of access models and FinTech Australia considers that it may be preferable to retain the data enclave model as a separately recognised model under the Draft Rules.

1.5 Other issues

Assurance reports

FinTech Australia seeks clarification of the scope of the 2 yearly assurance reports for Principals under the CDR Representative model. Specifically, we seek clarification in relation to the CDR data environment boundary in respect of CDR Representatives which will not be accredited in their own right.

Access models linked to data flows

Currently, the Affiliate / Sponsor and CDR Representative / Principal models couple the concepts of access and data flow. An Affiliate can only collect data through their Sponsor and an CDR Representative can only collect data from their Principal. We consider this to be unnecessarily restrictive and not something which needs to be mandated by the Draft Rules.

A key example of a scenario where this would stifle innovation relates to derived data. As derived data is classified as CDR Data, once an ADR has generated derived data, that data can only be shared in accordance with the CDR Rules. Under the proposed access models, additional complexity would be involved for a CDR Representative or Affiliate seeking to

collect and aggregate derived data from more than one source (or from a source which is not willing to appoint CDR Representatives).Rather than prescribing this linkage in the Draft Rules, we consider that this could be left to the relevant parties. For example, in an Affiliate / Sponsor arrangement, it would be a matter for the Sponsor to decide whether to allow the Affiliate to receive CDR Data from other sources. Similarly, for a CDR Representative / Principal, the Principal could decide whether they were to be the only source of CDR Data or if the CDR Representative could also receive data from others.

This prescriptive approach may also create issues as CDR expands outside the banking industry, as it may make it more difficult for businesses to access and aggregate cross-industry CDR Data.

Furthermore, the Draft Rules lack clarity surrounding the role of resellers of CDR solutions. For example, the Draft Rules do not adequately cover a scenario where an accredited ADR has a commercial arrangement with another business who then white labels the intermediary CDR solution to resell to other businesses.

Deidentified data

While this is not directly raised in the current consultation, FinTech Australia wishes to also highlight a potential discrepancy between the definition of de-identified data in the Act and the Rules. In the Act, data is regarded as de-identified if not able to be reidentified by the particular entity. However, in the Rules, data is de-identified only if it is not able to be reidentified by any person.

2. CDR Insights

FinTech Australia supports the proposal to allow free sharing of CDR Insights. Our members consider that there is a significant difference between the real-time raw data obtained directly from a Data Holder and discrete point-in-time insights. This change could substantially improve and broaden the use cases for CDR data.

FinTech Australia, however, has some concerns about the current definition of CDR Insights. Firstly, prescriptive requirements for CDR insight data are likely to be too narrow and thereby reduce useability and innovation. In particular, references to "income" and "expenses" may not translate appropriately for business accounts. Our members recommend also referring to revenue. In addition, the explanatory materials currently contemplate that CDR Insights would provide a "yes/no" confirmation. While insights of this kind will often be useful, for many use cases, additional information would also be required. For example, a lender seeking to use CDR Insights to make a lending decision is likely to require details of the amount and nature of the relevant income and expenses. To accommodate this use case, we suggest expanding the definition of CDR Insights to include data based on analysis that includes contextual status, comparisons, financial targets or more, generally any derived data for the purpose of the consent.

In addition, a specific issue arises in the context of accounting information. An accounting platform which consumes CDR Data would use that data to prompt end users to create ledger entries (ie a bank transaction relating to $100 of spending at Officeworks may prompt an end user to create a ledger entry of $100 of expenses). Under the current approach to derived data, we understand that those ledger entries created by the end user would be treated as derived data and, hence, only able to be dealt with in accordance with the CDR Regime. This creates significant barriers for this sector, as accounting information is not currently subject to CDR protections and can be freely shared. If this limited use of CDR Data to prompt end users would result in all accounting information being treated as CDR Data, we anticipate that accounting platforms would not be able to participate in the CDR regime, without further adjustment. One possible avenue of adjustment would be to treat ledger entries created by an end user as CDR Insights. These entries are not raw data obtained from a Data Holder, but have been created by end users in light of such data. Furthermore, accounting information is prepared for the purpose of being shared (to a range of stakeholders which can include directors, shareholders, ASIC, ASX, etc). As such, we consider that it is an appropriate balancing of risk and efficiency to afford accounting information with this treatment.

Finally, once data is regarded as CDR Insight, the Draft Rules permit that data to be disclosed outside the CDR ecosystem. However, it would still be CDR Data in the hands of the relevant ADR or if disclosed to another ADR. This means the ADR would still need to treat the CDR Insight as CDR Data (and any data derived from it as CDR Data, for example), whereas the recipient would not. This result, if intended, significantly reduces the useability of CDR Insights for ADRs (although they would still be very useful for non-ADRs) and creates the situation where an ADR is constrained more than an unaccredited person for the same CDR data. This is a more general problem with derived data that should be addressed. For example, if an ADR obtains consent to collect CDR data as input to a credit decision, the CDR rules would seem to dictate that data must be deleted once that credit decision has been made. This means that the ADR will have no record of the basis on which it made a credit decision / responsible lending assessment, cannot use the data as input to credit modelling, or as a basis if a complaint were later to arise. While CDR Data can be retained where required by law (eg by credit laws or responsible lending requirements), this is a relatively narrow carve out to the deletion requirements and would not extend to other data also considered as part of the credit decision. Additionally, if an ADR uses CDR insight data to perform a credit check, such as verifying a customer's income, then the output is considered derived CDR data. This derived data is subject to data minimisation and deletion rules that make it unworkable in a credit risk management context.

3. Outsourced Service Providers

The amendments in relation to unaccredited outsourced service providers (**OSPs**) appear to be intended to address the issue identified by the Office of the Australian Information Commissioner (**OAIC**) in relation to SaaS models widely used in the industry. The OAIC's

approach had been to treat the SaaS host as collecting CDR Data and passing it on to the entity using the SaaS host's services.

While we support the Treasury's efforts to address this anomaly, we consider that the proposed amendments in the Draft Rules may have gone too far. In particular, the Draft Rules would now appear to permit any unaccredited entity to:

- collect CDR Data from multiple Data Holders and store; and
- provide ADR's with access to CDR Data, either through APIs which directly interface with Data Holder or by accessing CDR Data stored by the unaccredited OSP.

Under this model the OSP is required to comply with security, standards and data privacy, however the liability for not complying rests with the CDR Principal. The additional capability of collection, requires the OSP to participate in the ecosystem where they have access to CDR data, information as to the performance of DH systems and generally far more information by virtue of having access to DH systems than a representative would have. This level of access should require accreditation. We understand that this model may suit a parent organisation with a subsidiary providing IT services but it extends to a far greater audience. In any event, these arrangements could be dealt with through the Principal / CDR Representative model, without creating the risks associated with unaccredited OSPs collecting data.

This seems to create significant risk and run counter to the extensive efforts which are being taken to protect CDR Data. For example, the narrow definition of Trusted Advisers ensures that CDR Data can only be passed outside the CDR ecosystem to persons who are subject to existing professional obligations. However, these changes to the outsourcing arrangements would permit unaccredited entities to have direct access to Data Holder APIs and to store CDR Data in any way they choose.

Finally, the Draft Rules do not provide clarity surrounding outsourced service providers (OSPs) that have commercial arrangements with ADRs that are not authorised deposit-taking institutions (ADIs). Whilst the ADI will assume the liability of the OSP under its own information security, assurance and attestations, the only supervision of unaccredited OSPs for non-ADIs may be at accreditation and then again at each 2 yearly assurance report. FinTech Australia is concerned that this may not be sufficient.

4. Joint Accounts

FinTech Australia and its members are overwhelmingly supportive of these proposals. We consider that they address what has been a practical barrier to uptake of CDR by joint account holders. This feedback has been affirmed through practical experience from the ADRs which are active within the CDR ecosystem.

However, in relation to the implementation, we make the following comments.

- Where a customer chooses not to disclose information about a joint account (i.e. under the nondisclosure option in Rule 4A.4(1)(c)), it would be preferable if this decision was visible through the CDR regime. It would also be preferable to have visibility where a consumer has selected the co-approval option.
- It would be useful for a Data Recipient to know whether an account is a joint account or not as currently that information is not shared with the Data Recipient. This information would help with use cases for a range of consumer-centric services including Personal Finance Management, loan affordability assessment, and lending (Financial Passport), but also verifying account ownership.
- We would like to see Data Holders implement joint account sharing well in advance of the proposed 1 April 2022 compliance deadline.