

Frollo's submission to proposed changes to the CDR Rules

29 October 2020

Summary

Frollo Australia Pty Ltd (**Frollo**) has read the materials in the ACCC's announcement of 30 September 2020 relating to the proposed changes to the CDR Rules.

Frollo has structured this submission using the ACCC's questions provided in the CDR rules expansion amendments consultation paper.

Questions

Timeline for proposed rules to take affect and overview of key proposed rules

1. We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

Frollo would like to enable its use cases requiring amended consents earlier than July 2021. Either February 2021 (same time as PAR or 1 March 2021). In particular amending a consent to extend the duration.

The transfer of CDR data between accredited persons timeline is December 2020. The disclosure consent timeline to support this is needed at the same time.

Increasing the number and types of business that can participate in the CDR

2. The proposed rules include three discrete kinds of restricted accreditation (i.e. separate affiliate, data enclave or limited data restrictions). We welcome views on this approach and whether it would provide sufficient flexibility for participants. In responding to this question you may wish to consider whether, for example, restricted accreditation should instead be based on a level of accreditation that permits people to do a range of authorised activities.

Frollo agrees with the ACCC's overall approach to restricted accreditation models on the basis that:

- a. restricted ADRs can leverage existing, CDR compliant technologies built by third party software providers to power their own unique offerings;
- b. it reduces the cost for other organisations who wish to participate in the CDR regime;

- c. it reduces build effort for other organisations who wish to participate in the CDR regime;
 - d. it will increase the number and type of services offered to Consumers;
 - e. Information Security requirements will still be maintained and applied; and
 - f. by not specifying the type of activities a restricted ADR can perform, these amendments have allowed the market sufficient flexibility to create innovative, data driven products that will ultimately benefit the Consumer.
3. We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation.

Frollo notes that the previous ASIC Fintech Sandbox regime is a good example of how customer volume limits can negatively impact market participation in a regime which aims to improve innovation (among other things).

Restricted Level: Limited data restriction

4. What are your views on the low to medium classification of risk for the data set out in Table 1?

Generally, Frollo considers this risk classification appropriate. For Frollo to comment further on this, this will depend on:

- a. the definition of ‘low’ and ‘medium’; and
 - b. how the classifications are used
5. Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?

Frollo considers this appropriate since the CDR data includes medium classified data.

6. Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?

Frollo does think the limited data restriction would encourage participation in the CDR. Some use case might include:

- a. Account verification services;

- b. Buy now, pay later services;
- c. Evaluating building contractors' financial position in relation to being able to provide services during the life of a contract. This may protect projects against builders going broke during a contract and not completing. A full picture is not required, limited data is suitable.
- d. Account balance check for debt collection services

Restricted level: data enclave restriction

- 7. Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR Sectors.

Frollo strongly believes that the data enclave restriction would increase participation in the CDR considerably. Frollo has spoken with a number of organisations who would like to participate in the CDR, however these organisations are unwilling and/or unable to become an unrestricted ADR due to the considerable cost and effort associated with this level of participation.

Frollo has undertaken preliminary market validation (in the banking sector, and associated financial services organisations) of a data enclave type model and interest appears to be very strong.

- 8. Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?

It is Frollo's opinion that some type of reporting is required to show complaints and issues, where a shared responsibility exists.

- 9. Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?

It is Frollo's opinion that no additional requirements are required as the data safeguards cover a data enclave.

Restricted level: Affiliate restriction

- 10. Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.

This may facilitate the mortgage aggregator use case. Consumers could obtain consumer affordability reports through a sponsor collecting the raw data. It is an additional model to the trusted advisor model (where the Trusted Advisor is a broker). Something that replaces the need for consent to individuals where a scalable service can be provided is beneficial.

11. Should there be additional requirements under Part 1 of Schedule 2 for sponsors?

If an affiliate was able to have many sponsors, this would complicate the management of data and the security controls. Data from different sponsors could be separate, overlap or be duplicated.

Which sponsor would be responsible for controls over what CDR data?

12. Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?

In order for the sponsor of an affiliate to take reasonable steps to ensure that the affiliate complies with its obligations as an accredited person, some reporting obligations would need to exist between the affiliate and the sponsor. This may need to cover complaints and incidents (those that affect compliance).

13. The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.

Frollo agrees with distinctions based on risk. Frollo has commented on each of the examples below.

Example level 1: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems.

This is the highest risk, a full schedule of controls would need to apply depending on the data held. If low medium CDR data is held then risk is reduced. Transaction data would need the full schedule.

Example level 2: affiliate is able to access all data sets, but uses some of the sponsor's systems and applications to access or manage the data.

This is very much dependent on the scenario. If transaction data is held by an affiliate, then risk is still high.

Example level 3: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor’s systems and applications to access or manage the data.

Lower risk and therefore a limited number of controls should be specified. Application white listing for example may not be needed. If data held is de-identified or derived data such as insights then there is a case for lower level of controls the sponsor should seek.

Combined Accredited Person arrangements

14. We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.

Frollo agrees, the principal is responsible for defining and ensuring dashboard functionality. Also for customer communications and dispute resolution need to be performed by the Principal. Clarification is required to state if these functions can be outside the enclave.

Transfer of CDR data between accredited persons

15. Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data?

This may confuse consumers if disclosure is not separate. A defaulted disclosure is not ideal. The statement:

‘Where CDR data is transferred between accredited persons and each accredited person is providing a good or service to the consumer, each must independently provide consumer dashboards, CDR receipts and the appropriate notifications’

should refer to the goods or services supplied and not to the transferred data.

- a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate?

Yes.

b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the consumer and, if so, to what extent?

Yes. It is Frollo’s opinion that this arrangement should be transparent and provide the names of the parties and a general description of the type of service offered.

Disclosure to trusted advisors

16. To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession’s regulatory regime in your response.

Generally, Frollo agrees with the ADRs disclosing CDR Data to trusted advisors with consumer consent. Frollo is not in a position to comment on every professional advisor class outlined in the rules, however, Frollo can share some insight on the mortgage broker class.

Frollo strongly supports the disclosure of CDR Data to Mortgage Brokers for the following reasons:

- a. consumers will benefit greatly by allowing their Mortgage Brokers to use their CDR Data to find and recommend the most appropriate mortgage in a fraction of the time;
- b. Consumers already share the data (similar to CDR Data) with Brokers through unsecure methods (eg. screen scraping, statement downloads);

17. Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?

Yes, this measure shows a direct relationship and purpose for the passing of CDR data.

18. Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding ‘raw’ CDR data as disclosed by the data holder)?

Since raw data can be passed to a trusted advisor, treating insights as derived data is useful for other use cases and consistent with a common understanding.

19. What transparency requirements should apply to disclosures of CDR data insights? For example, should ADRs be required to provide the option for consumers to view insights via their dashboard, or should consumers be able to elect to view an insight before they consent for it to be disclosed to a non-accredited person?

Frollo considers this as a restrictive approach. A consent to pass insights for a service should be sufficient.

Specific rules for business partnerships

20. We are seeking feedback on the proposal for enabling business consumers (both nonindividuals and business partnerships) to share CDR data.

Frollo has no feedback on this question.

21. In particular, we welcome comment on the proposal to require a data holder to provide a single dashboard to business consumers which can be accessed by any nominated representative to manage CDR data sharing arrangements.

Frollo has no feedback on this question.

22. Are there other implementation issues the ACCC should be aware of in relation to the proposed rules for CDR data sharing by non-individuals?

Frollo has no feedback on this question.

23. We welcome comment on the proposed approach to require data holders to treat business partnerships in line with the approach for dealing with business consumers? Do you foresee any technical or other implementation challenges with taking this approach for business partnerships that the ACCC should take into account?

Frollo has no feedback on this question.

24. Should additional protections be introduced for personal information relating to business partners who are individuals?

Frollo has no feedback on this question.

25. Are there other aspects of the rules that may require consequential changes as a result of the enablement of business consumers? For example, are the internal dispute resolution requirements appropriate for business consumers?

Frollo has no feedback on this question.

Secondary users

26. We welcome feedback on the proposals for enabling authorised users to share CDR data.

Secondary users would be of benefit to services that allow for someone (with account authorisation) to monitor elderly financial abuse.

27. Should persons beyond those with the ability to make transactions on an account be considered a person with ‘account privileges’ in the banking sector?

Yes, as per answer to 26.

28. How should secondary users rules operate in a joint account context?

This would make it more complex for joint accounts if the secondary person is not one of the joint account persons.

29. As well as having the ability to withdraw a ‘secondary user instruction’, should account holders be able to have granular control and withdraw sharing with specific accredited persons that have been initiated by a secondary user?

Yes

Sharing CDR data on joint accounts

30. We are seeking feedback on our proposals relating to sharing CDR data on joint accounts, including:
- a. the proposed approach to require data holders to allow consumers to set their preferences (a disclosure option) as part of the authorisation process.

Disclosure consents do not impact data sharing from a Data Holder. Duplicating and synchronising these across ADRs and DHs creates more build and friction for consumers. If the suggested approach simplifies the lifetime consent processes then this may outweigh other considerations but it is not clear with the information available.

- b. the proposed approach of allowing ‘joint account holder B’ to withdraw an approval at any time

Frollo agrees with this approach.

- c. the expansion of the rules to include joint accounts held by more than two individuals

Frollo agrees with this approach.

- d. the proposal that joint account holder B does not have to ‘approve’ amendments to authorisations

Frollo agrees with this approach.

- e. the proposed approach that the rules do not require (but do not prohibit) the history of disclosure option selections being displayed to consumers as part of the joint account management service or data holder consumer dashboard.

Frollo agrees with this approach.

- 31. Do the benefits of requiring data holders to display on-disclosures to ‘joint account holder B’ outweigh the costs?

It is Frollo’s opinion that the benefits do not outweigh the costs, complexity, support or possible customer experience impacts.

Amending consents

- 32. Should accredited persons be required to offer consumers the ability to amend consents in the consumer dashboard, or should this be optional?

Yes. Offering through the consumer dashboard will simplify and allow a summary or aggregated view of consents to be seen by the consumer.

- 33. We are seeking feedback on the proposed rules about the way accredited persons are able to invite consumers to amend their consents. Should a consumer be able to amend consent for direct marketing or research in the same way as amending consent for use of data in the provision of goods and services?

This type of consent may be only with the ADR and not Data Holder. It should not require the equivalent full authorisation required as a consent for collecting CDR data.

- 34. Should the authorisation process for amending authorisations also be simplified?

Yes. The proposal which does not enable a technical amendment to an existing consent creates further complexity. Amending the duration of a consent should be a simple attribute change, that does not require authorisation or withdrawal to effect the change. Amending the duration of a consent should be brought in earlier than 1 July 2021.

Separate consents approach

- 35. We are seeking feedback on the proposed approach of separating the consent to collect from the consent to use CDR data (rather than combining consent to collect and use).

This would be useful for loan applications and Frollo would like this earlier than 1 July 2021. Either February 2021 (same time as PAR or 1 March 2021). It would also simplify changes if

separate use consents did not require the Data Holders to keep track of, given the data holder does not control the use consent. ADRs are required to continue notifications to the consumer which protects against misuse of the use consent.

36. Should accredited persons be able to offer disclosure consents only after an original consent to collect and use is in place (with the effect that combining a use and collection consent with a disclosure consent would be prohibited)? See also the consultation questions in section 7.2 above.

Combining disclosure consents with collect and use would overload the consent at the time of the consent. Consumers may feel the disclosure consent is not optional.

A ‘point in time’ redundancy approach and the impact of withdrawing authorisation

37. We are seeking feedback on the ‘point in time’ redundancy approach.

If the rationale for making this change is that it is difficult to tag data associated with a consent, then it is not correct. It is quite simple and all participants that come in prior to these rules will need to deal with this ‘tagging’ as do the current participants. A change for these participants will also cost (understand it is left optional, but this will create differences in the ecosystem that are unnecessary). This will also create further complexities where existing consents continue to be extended/re-authorised.

38. We are seeking feedback on the proposed approach where a consumer withdrawing their authorisation for a data holder to disclose their CDR data results in removal of the ADR’s consent to collect only.

This would align to the joint account’s scenario where a joint account approval is removed by joint account holder B (although a specific notification of this authorisation removal would be beneficial and as it would not require interpretation when data ceases to be shared under this scenario). Many use cases will rely on data sharing to continue for joint accounts. The consent to ‘use’ can be explicit and incorporated into the overall customer education, dashboard and CDR policy. To create a default consent to use through a DH withdrawal would be more confusing as the number consents grow.

39. We are seeking feedback on the collection consent expiry notification and permissible delivery methods.

The 2 channel approach makes sense as the dashboard will require customers to be logged in to see the dashboard, this will usually apply even when there is an in channel notification. That way the message can be delivered by the consumers channel preference.

Improving consumer experience in data holder dashboards

40. We welcome any comment on the proposed rules to improve consumer experience in data holder dashboards.

A very short description of the service being authorised may be a good customer experience.

Application of product reference data rules to ‘white-labelled’ products

41. We are seeking feedback on whether the proposed amendments place the obligation on the party best placed to meet the obligation.

Yes, the obligation for PRD should lie with the entity responsible for the T&C’s for the product and changes to it.

42. Are there any technical or other implementation issues of which the ACCC should be aware?

This would be new to brand owners, where new maintenance processes would be required.