29 October 2020

Australia Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

VIA ELECTRONIC SUBMISSION

Envestnet Yodlee response to the Australia Competition and Consumer Commission's (ACCC) draft rules that allow for accredited collecting third parties (intermediaries) to participate in the Consumer Data Right

Dear Commission Members,

Envestnet Yodlee ("Yodlee") welcomes this opportunity to provide feedback on the expansion of rules dated September 2020.

In summation we believe the detailed expansion of the rules to accommodate three levels of accreditation to be overly complex. In essence we see the best model to be as described below:

1. **ADR**
No change to current definition as it exists under the rules. ADR can work with both Intermediaries and TSPs

2. **Intermediary Governance Model** *(resembles the Affiliate model).*

Yodlee are open to sharing its existing policies and protocols in its current affiliate program model and in use in other jurisdictions, working with the ACCC CDR in order to arrive at a more scalable framework. As mentioned on our call with Jodi Ross and the ACCC team on 28 October 2020 we are happy to set aside time to meet for discussion on this topic.

Summary of model
As further explanation of this model we see a "Provider/Sponsor" hold full accreditation into the CDR including liability and access to consumer data on the Data Holders side. The Data Holder knows and trusts the Provider and in some ways the Provider, although having standard agreements across all DHs, has a direct relationship and shares their risk posture and accreditation credentials; with both with the ACCC and Data Holders network. Under this model an entity whom is a client of the Provider (though a potential ADR) does not need to become an unrestricted level accredited ADR (as the liability rests with the Provider). From a regulatory perspective this allows for the regulator to have a single point of recourse rather than concern over chasing multiple parties for breaches and the like.

This is the current business practice in place at Yodlee today. We place requirements on our clients and they sign up to a "Client Governance Framework and Program". This model was built for our US open banking program and UK Open Banking agents. Clients, and prospective clients, must complete an online security questionnaire and provide evidence of the design and operating effectiveness of

their risk, security and privacy controls that support their Yodlee-powered service(s). If our assessment determines that necessary controls are not present, or not designed and operating effectively, a remediation process is initiated to bring the client into compliance with Yodlee's requirements. As mentioned, full liability to the ecosystem is upheld by Yodlee, so it is in the best interest of Yodlee to ensure there are no "bad players".

The Provider/Sponsor, Yodlee, is responsible for and guarantees the compliance and security of the receipt, processing, use and any retention of consumer data by them and its clients who are covered by the "Client Governance Framework and Program". Meeting CDR and OAIC standards and guidelines using in effect the successful "Sponsored" tiered accreditation and multi-party participation models in place in not only other Open Banking Frameworks but the wider global Payments and financial services industry.

Yodlee's Enhanced Client Governance Program is part of our overall Risk Management Program and subject to audit and reporting requirements to Management, the Board of Directors Compliance & Information Security Committee, regulators with standing and data providers with whom we have contractual agreements. We believe this will release the burden on Principals/Affiliates holding all assurances and liabilities plus the cumbersome and costly task of having to gain unrestricted level accreditation as it exists in draft currently.

3. **Technical (or Outsourced) Services Provider (TSP)**.

This is not accredited so in essence sits outside this ruling however stricter rules are required for governance of data practices being a non-accredited body. We believe there are many providers in the ecosystem currently utilizing services of Outsourced or Technical Service Providers where the policing of who collects, holds and enhances this data is not transparent due to a lack of ruling (or policing) that exists.

Consultation Questions

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

No issue with timing of Mid-December when rules can be finalised.

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.**

We refer back to our submission in July where we proposed several levels of accreditation. Whilst it seems the ACCC have taken into account a model similar to our first level (Affiliate) we believe the other proposed levels in the current rules expansion are over complicated and extraneous to the objectives; open the CDR up to those entities that don't want nor can afford a full level of accreditation.

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**

We believe that any access to consumer data on a consumer's online banking platform is high risk and accreditation based on levels of risk of consumer data is too broad and complex and can be, as noted when combined with other forms of data, highly subjective in definition. To use the example the ACCC has given on low levels of risk data; any data that has PII would be considering high risk for Yodlee and again we reinforce that all data on consumer's online banking interfaces is high risk and when it comes to PII we treat extremely sensitively and have strict practices in de-identifying for this reason.

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

Noted above where we believe all consumer data is high risk.

5. **Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?**

No. Disagree with model.

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?**

We do not believe so.

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 CDR rules expansion amendments 15 future CDR sectors.**

There is no need for this under the Governance model Yodlee is proposing. We believe the Affiliate/Intermediary Governance model would encompass this level of accreditation.

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?**

As above

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

n/a

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.**

Yes, the affiliate restriction level, as currently presented, will increase participation in the CDR by providing a safe reliable regulatory option for innovative entrants to the Open Banking ecosystem. A challenge with the unrestricted ADR accreditation has been that while the requirements are reasonable for handling the full set of CDR Data, the maturity and rigor required are out of reach for new market entrants whose capital is focused on growth or small establish firms that have appropriate practices, but not the rigor to pass assessment. The former reduces competition and innovation, while the latter can result in the shuttering of existing firms which will leave their customers without essential services.

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

Yes. Sponsors must have a demonstrably mature third-party governance integrated with their overall risk management program. Effective third (and fourth) party risk management focuses on both safeguards on CDR data as well as governance in the management of those safeguards and over the handling of the data. To be clear, this is not simply a point-in-time assessments or attestations, but rather a comprehensive set of preventative, detective and response controls implemented in the initial due diligence, onboarding and duration of the affiliate relationship. These arrangements can provide significant benefit to the affiliate as the sponsoring organization as a backstop and accelerator to their maturing controls program.

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?**

Yes, coordinated incident response is essential to protect the consumer and the broader CDR ecosystem. This should also include incidents/complaints where a DH has declined a consent request from an ADR sponsor or affiliate which at present is not allowed for. Only consumer complaints/incidents are required to be reported upon by DH.

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.**
    a. **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.**
    b. **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.**
    c. **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**

We don't believe a distinction is necessary on access to data sets. The affiliate can access all CDR data and use the systems and applications available under CDR as long as the Sponsor has undergone a level of due diligence that complies with the governance model mentioned above. If Yodlee (or any Sponsor for that matter) was to place different levels of risk across what data is being accessed as well as the use or not of our systems and applications this would lead to a huge amount of complexity in our pricing and contractual arrangements. As well it needs to be considered that the more complex these arrangements are, the more complex the inherent risk becomes.

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.**

Disagree. If liability is shared then this is what the Principal is paying for in their contractual arrangements with the Provider

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

The commercial arrangements should not be transparent to the consumer only as currently required whom the data may be transferred and for what use.

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.**

It is difficult to limit specific professional classes or entities. The description in the rules may be better described as those parties consented to by the consumer that provide product or services that provide or use the consumer's data.
The prior comments in relation to accreditation and responsibility and liability of the ADR/intermediary that has received the data from DH should apply. And not rely on the professions regulatory regime which is outside of the ability to assess whether they meet required standards, ability to monitor that they do meet required standards and if the entity is currently certified as compliant with them.

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?**

Based on our earlier accreditation and governance model additional measures would not be required to put in place to prevent ADRS from operating as a conduit. As it is built on the principal of consumers being aware of a consenting to the data being provided.

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)?**

This should not be the case as it restricts the scope of potential benefits to be gained from CDR. As long as supporting data security and consumer consents are gained.

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?**

Overly complex and operationally impossible. Insights (de-identified data) are often "onsold'. What and where this data goes is not always commercially an option to manage.

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

More details on use cases and proposed safeguards and scope of entities are needed. Is this their CDR Business data and if so yes. Otherwise more use case and examples need to be provided to enable comment.

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.**

Most Data Holders already have this however there needs to be a minimum standard on what is available on a consumer's dashboard versus what's available on business banking/Corporate account dashboard and the latter needs to be shared via CDR so all accounts (e.g. business transaction accounts and business loans) must be available as an API through both online interfaces (e.g. Netbank and CommBiz). Access to the more corporate accounts is through similar methodologies as constructed for the business account ownership (e.g. Company Director, accountant, etc.)

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? CDR rules expansion amendments**

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?**

This should be handled much like the proposal on joint accounts. Both business partners need to consent in order to share data

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

The liability and ability to confirm authority to give consent and maintenance of consent will need to be added. The mechanism to support its inclusion in sending of a consent to a DH will also need to be addressed

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?**

Yes, disputes and the current dollar value and other criteria limits to be eligible to use the external disputes body will need to be addressed. Along with what current commercial dispute resolution processes exist today.

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

Refer as commented above including guideline for doing so.

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, those that provide guarantees or other direct liabilities

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

They should operate as they do today as far as permitted account operation and use authorised for secondary users.

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, they should have that control

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 b. the proposed approach of allowing 'joint account holder**
    b. **to withdraw an approval at any time**
    c. **the expansion of the rules to include joint accounts held by more than two individuals**
    d. **the proposal that joint account holder B does not have to 'approve' amendments to authorisations**
    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.**

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

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

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?**
Yes, they should provide consistent consumer experience and confidence in the CDR ecosystem and support of it use

34. **Should the authorisation process for amending authorisations also be simplified?**
Its still being finalised so difficult to comment.

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).**

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**

37. **We are seeking feedback on the 'point in time' redundancy approach.**

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 should be explicitly stated to the consumer if to be the case, so they are aware. They should then also have opportunity to make further withdrawal of authorisation if they required.

39. **We are seeking feedback on the collection consent expiry notification and permissible delivery methods.**
This should be the same existing methods of delivery of other notifications to the consumer by their product or services/entity provider, and not only via the dashboard.

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

Current functionality on the CBA dashboard to send an OTP to the Netbank inbox needs to be improved. Expectation is to be in the form of a mobile text (as they do currently with online banking) NOT buried down in the inbox of the online dashboard. Very counterintuitive.