

Consultation on facilitating participation of intermediaries in the CDR regime

Intuit has been a long-time supporter of Open Banking in Australia and we appreciate the opportunity to provide input into the ACCC’s consultation on facilitating participation of intermediaries in the CDR regime. We look forward to continued collaboration with the ACCC to implement the CDR for the benefit of Australian customers.

Question 1	Intuit’s response
<p>If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?</p>	<p>At the outset, Intuit wishes to differentiate between the terms “intermediary” and “outsourced service provider”. The CDR regime does not currently reflect any distinction between these two terms, but Intuit ascribes the following meanings to them in the context of CDR.</p> <p>An “intermediary” would sit between an Authorised Data Holder (“DH”) and an Accredited Data Recipient (“ADR”) and would offer a technical integration between the ADR and DH by collecting, and passing through CDR data and possibly also storing and modifying the CDR data on behalf of the ADR. An intermediary would be liable, in its own right, to all CDR Participants for the services provided and would need to have its own CDR-compliant infrastructure.</p> <p>Intermediaries may either offer a:</p> <ol style="list-style-type: none"> 1. technical integration solution on behalf of the accredited person, who collects the consumer consent and provides “under cover” access to the DH’s API; or 2. complete turn-key data aggregator service to the accredited person, where the aggregator collects the consent when linking the consumer of an application to the data holder. <p>In the UK, Intuit uses the first option above - a technical integration and our intermediary is not consumer facing, enabling Intuit to control the user experience. However, consumers are informed that Intuit does use an intermediary.</p> <p>Under the second option above, the aggregator collects the</p>

	<p>consent from the customer of the application requesting the data from the bank</p> <p>The aggregator owns the user experience with the customer, disclosing that the application uses the services of the aggregator</p> <p>The aggregator stores (“persists”) the data and can, for example do the following with the consent and data: “reuse” the connection to the bank for another application requested by the consumer and create derivative, anonymized analytics for sale to third parties</p> <p>Intuit believes there is a role for both the above intermediary functions in the CDR ecosystem.</p> <p>We consider an “outsourced service provider” (OSP) to be more akin to a software provider, that would be engaged by an ADR to provide software, or code, that would form part of the ADR’s own environment to enable them to participate in the CDR regime. An OSP would be liable only to the ADR that engaged them, not to CDR Participants more generally. It would be the responsibility of the ADR to ensure that the software or code provided conforms to CDR standards (including ASAE 3150).</p> <p>Intuit intends to utilise the services of an intermediary to support our integrations with non- major financial institutions. Intuit does support connections with the major financial institutions, which the majority of our customers use, however by using an intermediary to manage the connections to the various smaller financial institutions, we greatly reduce the number of connections Intuit is required to establish and manage. Intuit’s intermediary currently collects, stores and modifies the data we obtain through it.</p> <p>Generally, we are of the view that there is a space for both intermediaries and OSPs in the CDR environment as these would both play a role in greatly reducing the costs and time involved for many organisations to participate in the CDR regime. For many participants, the costs of compliance and resources needed would be prohibitive. By being able to obtain the services of an intermediary or an OSP, there would be a faster, more cost effective option for such parties, resulting in wider participation, which in turn will result in greater innovation and benefits for consumers.</p>
<p>Question 3</p>	<p>Intuit’s response</p>
<p>How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an</p>	<p>Intuit’s view is that there should be an accreditation model for all intermediaries, as these will sit between the DHs and ADRs and under the proposed model, would have access to the open banking APIs of all parties as well as all consumer data. This is more preferable than the situation where the</p>

<p>accreditation model, or both and, if so, and in what circumstances each model should apply.</p>	<p>intermediary would be relying on the accreditations of the DHs and ADRs to participate. Accreditation requirements for an intermediary should be to the same standard as an ADR, however they should not be accredited as an ADR because they play their own role.</p> <p>So that the intermediary can be identified in the system, they should also have their own hybrid access tokens, rather than use the access tokens of the ADR, which we consider should be kept secure and not disclosed. This is so API calls they make can be clearly identified and traced back to the intermediary who is acting on behalf of an ADR to access CDR data from a particular DH. Such visibility and traceability goes hand in hand with accountability.</p> <p>Having an accreditation of intermediaries is crucial because it would give all CDR Participants greater comfort that any party accessing the open banking APIs are well placed to protect against the misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure of CDR data. On the other hand, Intuit considers there should be tiered accreditation of ADRs who may work with intermediaries depending on what kind of CDR Data they wish to obtain. This is discussed in further detail below.</p> <p>Given an OSP would only be providing an ADR with code or software that would form part of their own CDR environment, the ADR itself would be responsible for ensuring such code/software’s compliance with the CDR regime (including the data assurance standards afforded by ASAE 3150), so we do not propose that an OSP would require accreditation.</p>
<p>Question 4</p>	<p>Intuit’s response</p>
<p>What obligations should apply to intermediaries? For example, you may wish to provide comment on:</p> <ul style="list-style-type: none"> A. if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current ‘unrestricted’ level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards; B. if intermediaries are regulated under an outsourcing model, the 	<ul style="list-style-type: none"> A. Similar accreditation to ADRs should apply to intermediaries for accreditation at an unrestricted level - including in relation compliance with ASAE 3150 and reporting obligations. B. Intuit’s view is that OSPs and ADRs should be able to freely contract without regulation, given the ADR will ultimately need to assume responsibility for the software and code provided by the OSP. As outlined above, intermediaries however, should be accredited participants by the ACCC. C. Intuit’s view is that all intermediaries should be accredited at an unrestricted level. However the ACCC may consider introducing tiered levels of accreditation for ADRs depending on the CDR data they may wish to consume. Having lower compliance obligations for ADRs, such as ADRs who may not actually need to obtain CDR data, but data that is derived data from an intermediary. Also for ADRs that don’t store data, but simply use it for a one-off application for example, a

<p>extent to which contractual obligations should be regulated between accredited persons and intermediaries;</p> <p>C. if the obligations should differ depending on the nature of the service being provided by the intermediary.</p>	<p>lower level of accreditation should apply. For ADRs who store data, and may want to use it for other purposes, then a higher level of accreditation should apply. Having the option of tiered accreditation would encourage more participation in the CDR regime and discourage practices such as screen scraping etc that would not fall within the regime.</p>
<p>Question 5</p>	<p>Intuit's response</p>
<p>How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.</p>	<p>Intuit believes that the current proposal under the CDR Rules for disclosure about the use of intermediaries both in the consent workflow and in an ADR's CDR Policy to be sufficient where the intermediary is not offering a turn-key service as described in our response to question 1 above. Intuit notes the current rules make provision for CDR consumers to request further information about an ADR's intermediary should they desire it. Intermediaries offering turn-key services would manage the relationship with CDR consumers on behalf of an ADR.</p> <p>Intuit does not propose that intermediaries who offer technical assistance to access DH's APIs and who do not collect consent to be consumer facing as this may lead to undue confusion or concern on the part of a consumer and would serve little utility given the consumer is already consenting to the ADR obtaining the CDR data. Nonetheless, consumers should be informed about the use of an intermediary.</p>
<p>Question 6</p>	<p>Intuit's response</p>
<p>How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.</p>	<p>Intuit considers all accredited persons should be subject to the same regime regarding the disclosure of CDR data- ie with consumer consent. However if an intermediary does not need to obtain CDR consumer's consent directly, but may rely on the consent obtained by the ADR, then there would be different rules regarding the intermediary's obligations to maintain consent dashboards, provide CDR receipts and also actioning revocations for that intermediary. Intermediaries who offer technical integration only, should be allowed to leverage the consent a CDR consumer gives DHs and ADRs, where that intermediary provides services to the particular DH and ADR.</p> <p>Further, the CDR Rules should provide that all intermediaries (irrespective of their role) have their own digital access key so there is traceability, visibility and ultimately, accountability.</p>
<p>Question 7</p>	<p>Intuit's response</p>

<p>Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?</p>	<p>In line with our response to question 3 above, Intuit is of the view that lower tiers of accreditation for ADRs is appropriate depending on the type of CDR data they wish to consume. This is to reduce any unnecessary compliance burden and to provide greater optionality to all parties. In terms of liability, Intuit considers intermediaries should bear full liability for the services they provide that are within the scope of their engagement.</p>
<p>Question 8</p>	<p>Intuit's response</p>
<p>If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to:</p> <ul style="list-style-type: none"> A. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers; B. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers. 	<p>We believe there should be tiered accreditation for ADRs, which should encourage more parties to form part of the CDR regime.</p> <p>The accreditation tiers should be determined according to the types of CDR data the ADR would like to consume. As a minimum, all parties receiving CDR data should have in place CDR policies regarding the management of CDR data, a CDR consumer consent process in place, reporting requirements, obligations to delete or de-identify data on the revocation of consent in accordance with CDR Privacy Safeguard 12.</p> <p>If an intermediary is used, then a basic or mid-tier accredited ADR should be entitled to rely on the intermediary's compliance with more onerous standards such as an audit of compliance with ASAE 3150.</p>
<p>Question 9</p>	<p>Intuit's response</p>
<p>What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?</p>	<p>Consumers should be empowered to give permission access to their financial account data securely and easily, using whatever secure application or technology they wish. To do this, consumers must provide explicit consent for access to and use of their data. Consumers must also be able to easily view, modify and revoke consent for data sharing.</p>
<p>Question 10</p>	<p>Intuit's response</p>
<p>What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?</p>	<p>We believe the existing privacy laws and Australian Privacy Principles as well as the consumer protections under the SPAM Act and other applicable legislation would protect consumers as they are protected today without the CDR regime.</p>

Question 11	Intuit's response
What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?	We believe that a link to the accredited person's CDR policy and a statement that the consumer can obtain further information about such disclosures from the policy if desired included in the information presented to consumers when asking for consent will be sufficient to allow the consumer to properly understand what he or she is consenting to.

Intuit would be more than happy to discuss any part of this submission in more detail. Please contact Simeon Duncan at [REDACTED] or Steve Kemp at [REDACTED] for further information.