CDR Rules Consultation: CDR rules expansion amendments

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 the CDR rules expansion amendments.

We believe that data is the lifeblood of consumer and small business finance. With the appropriate consumer consent and a robust privacy and security framework, individuals and small business owners should be able to access their financial data in whatever format they wish or with whatever app they would like to use to better their financial life.

We are strongly supportive of the ACCC's efforts to accommodate tiered accreditation and more applicable consent mechanisms into the Consumer Data Right (CDR) rules framework.

We look forward to continued collaboration with the ACCC to implement the CDR giving Australian consumers greater access to, and control over, their data.

1. Comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

Intuit supports in principle the proposed timelines; however, we note that changes to rules and compliance timelines have a significant impact on the cost and ability to build compliant CDR products, particularly where binding CDR data standards are needed to be updated to enable rules compliance.

Short consultation timeframes for CDR rules and data standards have the potential to create negative flow on effects to Authorised Data Recipients (ADRs) and a delay in the CDR roll-out to consumers.

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.

Intuit welcomes the introduction of tiered risk-based accreditation model as was recommended in Scott Farrell's Review into Open Banking (the 'Farrell Review'). Having tiered accreditation would encourage more participation in the CDR regime and discourage practices that fall outside the regime.

We believe it is appropriate to have lower risk-based compliance obligations to encourage the competition and innovation objectives of the regime, and for the CDR to support Australia's digital economy.

While we welcome the concept of tiered accreditation has brought with it additional and in our view unnecessary complication. Tiers should be based on the activities restricted CDR participants do and should not be contingent on their relationship with an unrestricted accredited party. This allows for flexibility and fluidity as these relationships may change regularly.

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.

As was recommended in the Farrell Review, we believe that accreditation models should have regard to existing licencing and regulatory regimes.

Intuit recommends that the ACCC consider the use of existing financial data accreditation frameworks, specifically the Australian Taxation Office's (ATO) DSP Operational Framework ('Ops Framework') and the Security Standard for Add-on Marketplaces (SSAM) to manage accounting software intermediaries and their platform ecosystems..

Following consultation with digital service affiliates (DSPs) and the Australian Small Business Software Industry Association (ABSIA), the ATO & ABISA produced an assurance framework that defined cyber-security controls for Software Standard for Add-on Marketplaces (SSAM).

Both the Ops Framework and SSAM frameworks address technical cyber security controls designed to reduce the risk of a malicious cyber security incident or an accidental data breach. There is a substantial degree of commonality and alignment between the technical controls and other requirements outlined in the CDR Rules and the existing ATO Operational Framework.

Given the alignment, Intuit believes the potential exists for the ATO and ACCC to collaborate to recognise accreditation partially or fully under either scheme as a form of mutual recognition under the CDR framework. This may provide cost benefits and efficiencies for scheme administrators and DSPs.

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?

We do not support the definition of CAP arrangements particularly that certain actions are done 'on behalf' of a principal (being an unrestricted accredited party). This raises the prospect of the principal being liable for the actions of the provider using the CDR data, which is not how commercially the parties wish to structure their business relationship.

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.

While we welcome the concept of affiliate accreditation, given the proposed requirement for affiliates to meet all provisions of Part 1 and almost all of Part 2 of Schedule 2, we do not believe that the affiliate restriction - as proposed - would increase participation in the CDR. In fact, we believe that the requirements for affiliate accreditation creates an unnecessarily costly and demanding barrier to participation.

Consumers who choose to acquire the services of a third party affiliate through the platform operated by a sponsor do so on the affiliate's terms and conditions and services. In light of the fact that there is no form of agency between the sponsor and affiliate, we believe that the proposed obligations on sponsors are necessarily onerous.

We support the Australian Business Software Industry Association's view that sponsor obligations should be limited to receiving their affiliate's annual self assessments along with any underlying evidence to support their assessment and sharing this information with the

ACCC via the Digital Partnership Office at the ATO.

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

No. Again, we recommend that the ACCC heed the Farrell Report's recommendation to have regard to existing licencing and regulatory regimes. With this in mind, we recommend the ACCC recognise the SSAM as sufficient and appropriate for sponsors to manage their affiliates.

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?

No. Given there are many different types of use cases for affiliates, the CDR Rules need to allow for a flexible approach to allow affiliates and sponsors to contractually determine the obligations and liabilities each of them should bear according to the arrangement.

We caution that overly prescriptive CAP liability arrangements would act as an inhibiting factor for innovation and startups offering new services as it is unlikely that they will have the resources and capacity to establish and maintain the necessary levels of due diligence.

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?

We recommend that the ACCC align CDR accreditation requirements and processes with the ATO's existing Operational Framework and SSAM licencing and regulatory regimes to avoid duplication or disparity of risk-based standards and reporting requirements for accounting software providers.

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?

No. The initial consent to collect is provided to the ADR. To ensure consent is voluntary and

informed, consumers ought provide additional consent for disclosure to additional ADRs separately.

It is important to the integrity of the CDR regime that consumers are aware of who they have granted access to their data and how that data will be used by ADRs to provide a good, service or benefit to the customer.

Given the private sector application relies on the freedom to contract to terms, we do not believe that commercial arrangements between ADRs must be disclosed to consumers.

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?

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 and direct the ADR to pass on 'derived data' in a manner that the customer chooses.

While we welcome the professional classes that the ACCC has proposed as non-accredited data service providers, we believe that the CDR rules framework should not attempt to regulate or limit human interaction, instead focusing on the regulation of and data standards of the machine to machine processes of the CDR.

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?

No further measures or stipulations are necessary. Sharing data needs to be limited to instances where a good, service or benefit is being acquired.

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)?

As an accounting software provider, Intuit would not be sharing 'raw' CDR data with third parties; however, we recognise that the current definition of 'derived' data is broad and can include data and data insights that were not intended to be captured in the CDR regime.

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?

Given any CDR derived data can be considered as insights then consumers must go through a consent process similar to the CDR consent process, though should not need to be identical. For example, existing internationally adopted OAuth 2, OIDC standards can be adopted for the consent process.

Consenting to share insights should not be a blanket consent during the initial consent process but rather on a case-by-case basis where an ADR may alert the consumer that another service offered by a non-accredited person may be of benefit to the consumers. Opting into that service and through explicit consent by the consumer means derived CDR data may be shared.

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

Offering consumers the ability to make amendments in the consumer dashboard should be optional features offered by ADR as each ADR's use-case is different.

Any such amendments should only be made from the ADR side as only the ADR understands the rationale for an amendment. ADHs should not be allowed to offer amendments to customers as DHs have no context on how the data is used on the ADR side.

Amending accounts and data cluster consents are significant changes on the ADR side. These typically have a much bigger impact on the ADR services being offered. Such changes are better facilitated via a revocation of existing consent and authorisation of a new consent.

Amending sharing consent via consumer dashboard ought be a simple authorisation mechanism to extend sharing duration without changing other parameters with the existing consent.

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

Yes; however, this should be made in the design of the technical specification of the data standards as well as the CX guidelines rather than being incorporated into the CDR Rules.

It is important for the ADRs to request explicit items of change, e.g. change of account selection, change of sharing duration, change of data clusters, or a combination of them. The ADHs need to present information relevant to the requested change and nothing more. Only ADRs understand what changes will be of benefit to their customers.

As an example, if an ADR only requested a change of sharing duration, but DHs allow accounts to be also changed then this may have a damaging effect at the ADR end where existing services may no longer operate correctly.

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).

Given the legislative obligations that most customers of accounting software providers have to keep their financial records for a certain number of years under the Income Tax Assessment Act 1936 (Cth) and keeping their records in the cloud and electronically is permitted to satisfy their requirements, we support the need to separate the consent to collect sharing duration for consent to collect and consent to use.

We recommended that consent to use to be perpetual until consumer explicitly revokes consent to use or cancel service with ADR. This avoids "re-consent fatigue" for consumers for continued data use and is a common practice today in a lot of consent flows where consumers are notified the consent will be in-place until cancelled explicitly by consumers.

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)?

Yes. Accredited persons should be able to offer disclosure consents contemporaneously with offering collect and use consents or at any time thereafter.

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.

We agree that this is required; however, how is the consumer's authorisation withdrawal manifested? If initiated from DH side, how do ADRs know it is a 'point-in-time' revoke of collect and can continue to use the data?

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

We believe the current receipt mechanism notifying customers of consent expiry is sufficient.

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

We are of the view that the proposed rules to improve consumer experience more properly belongs in the Consumer Data Standards and registry specifications. In the event that the CDR rules specify consumer experience, this ought to be a new property attached to the ADR's metadata in the Registry.

Intuit appreciates the opportunity the ACCC has provided to participate in this consultation and provide recommendations on the evolution of the Rules. We look forward to contributing to the ongoing discussion on how best to deliver a best-in-class and globally consistent Consumer Data Right for the benefit of all Australian consumers, giving them more control over the financial data they choose to share.

Please contact Steve Kemp at [redacted] or Simeon Duncan at [redacted] for further information.