CDR Rules Consultation: Draft rules that allow for accredited collecting third parties ('intermediaries')

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.

The Combined accredited person (CAP) arrangement

Intuit supports the need for appropriate accreditation for all participants in the CDR however, it is our view that the proposed draft rules to require 'Providers' to be accredited to the "unrestricted" level creates an unintentional barrier to a consumer's rights over their data and an unnecessarily onerous burden to CDR participation that will inhibit product innovation and stifle the growth of new service offerings.

Who is a 'Principal'

Intuit is satisfied with the definition of 'Principal'.

Matters relating to a 'Provider'

As alluded to above, Intuit's view is that there should be an appropriate accreditation model with tiered levels of accreditation for both Principals and Providers.

Having tiered accreditation for Providers would encourage more participation in the CDR regime and discourage practices that fall outside the regime. We believe it is appropriate to have lower compliance obligations for Providers, such as those Providers who may not actually need to obtain raw CDR data, but data that is derived CDR data, combined with other data, from an intermediary.

The explanatory notes to the draft rules state that "the principal and its branded goods and services will always be the consumer-facing entity with whom the CDR consumer has a contractual relationship. A Provider can only provide services to the CDR consumer on behalf of the Principal." It is unclear how the ACCC came to this position or why it must be

so. Intuit believes that the CDR ought to facilitate a financial services ecosystem where there are multiple options available to both Principals and Providers. This is particularly pertinent for Providers of data-driven platforms, like Intuit's via its flagship product in Australia, QuickBooks Online. Intuit does not have, nor seek to have, the ability to provide every ancillary specialist service that may be of value to a small business customer. However, the QuickBooks Online marketplace facilitates secure API connections to the cloud-based apps of our many third party service Providers. These connections help our small business customers to safely pass their data and receive incoming data to and from various service Providers, enabling them to receive invaluable services for running their businesses. These services include invoice management, ATO tax lodgements, Single Touch Payroll and also using accounting data to access credit.

To achieve publication on the QuickBooks app store, third party service provider apps must not only meet stringent security and technical requirements at the time of publication, but continuously after publishing. In addition, third party apps not published on the app store must meet these requirements if they exceed 500 connections. Intuit checks all apps annually to ensure that they still meet the technical and security standards required.

Those of Intuit's small business customers who choose to acquire the more specialist services of third party Providers using the Intuit platform, do so on the Provider's terms and conditions of service. Our partners provide their services for payment and of course bear responsibility for the quality of those services directly to the customer. Of course our customers may access these services outside of their QuickBooks Online account. If they did so, there would be no doubt that they were contracting directly with the third party Provider. However, Intuit's secure data sharing APIs offer a highly convenient and safe way to share data. For example, having to first download accounting data and then attach it to an email to send to a service Provider, is a thing of the past for many of our customers.

Existing frameworks

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

The ATO collaborated with Digital Service Providers (DSPs) throughout 2017 to develop the initial version of the DSP Operational Framework (Ops Framework). The Ops Framework segments the DSP Marketplace into SaaS and Customer-hosted solutions and defines a suite of baseline cyber-security controls that must be met before a DSP is permitted to use the ATO's Digital Services within a designated risk category.

The ATO's DSP Operational Framework requirements and technical controls are closely aligned with the CDR Information security guidelines.

In 2019, the ATO further collaborated with DSPs and the Australian Small Business Software Industry Association (ABSIA) to produce a subsequent assurance framework that defined cyber-security controls for Software Standard for Add-on Marketplaces (SSAM). This framework was based on Intuit's existing QuickBooks Online App Store review processes.

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. Parties need to become accredited under these schemes. 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. This alignment has been described in Table 1.

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.

Consent transparency

If Providers are not required to have "unrestricted" CDR accreditation and do not obtain CDR data directly from data holders themselves, then it is our view that it is appropriate for principals to facilitate obtaining the consumer's consent to share the CDR data with Providers, before the CDR data is shared. Intuit adopts this approach currently with its customers who may use the Intuit platform to acquire services from third party Providers.

Record keeping

Intuit does not object to the proposed requirements to keep and maintain records that record and explain their CAP arrangements, including a copy of all relevant CAP arrangements, for a period of 6 years.

However, we do have concerns about conflicting data retention and segregation requirements. As an accounting software Provider we store accounting records on behalf of customers to enable them to meet their various legislative requirements e.g: Income Tax Assessment Act 1936 (Cth).

Without a limit on when CDR data ceases to be classified as 'derived data', there arises the potential for a conflict for accounting software businesses between record keeping to enable their small business customers to meet their legal obligations and CDR data and derived CDR data deletion requirements.

For example, when Intuit collects CDR data on behalf of a customer, it becomes derived CDR data as it is incorporated into our customer's QuickBooks accounting records. From that point, the derived CDR data is not tracked according to its source and has become

inextricably embodied into our customer's accounting records. This means Intuit would be unable to identify and delete derived CDR data collected from any one particular source. Being able to do this would be of no use to our customers in any case, because it would result in their accounting records being inaccurate and unbalanced, effectively rendering them useless.

For the sake of CDR consumers, there needs to be clarification on when their accourning data stops being CDR data so that they are able to meet their legislative obligations.

Liability structures

The draft rules say that a "principal who is providing the services and goods to the CDR consumer remains liable at all times. The principal also remains liable for the acts and omissions of the Provider whether or not the Provider is acting within or outside of the scope of the CAP arrangement." Similarly, if a Provider obtains accreditation in its own right, it seems at odds to hold the Principal liable for any breach in respect of CDR data committed by a Provider (as per draft Rule 1.10A(4)(b)(ii) where a breach by the Provider will be taken to be a breach of the Principal).

Given there are many different types of use cases for Providers, the CDR Rules need to allow for a flexible approach to allow Providers and Principals to contractually determine the obligations and liabilities each of them should bear according to the arrangement. For example, if the Provider collects the CDR data on behalf of the principal, different considerations will apply to the situation where the principal is sharing CDR data at the request of the consumer to a Provider.

We believe it is still appropriate for Principals to hold "unrestricted" accreditation and comply with all obligations under the CDR Rules given it will obtain CDR data from Data Holders and will store and use it for its customers. The fact that customers may choose to share the CDR data that Intuit has obtained with a third party Provider should not relieve Intuit of any obligation or liability in respect of the CDR Data. Intuit is merely providing a platform for the customer and third party Provider to connect and facilitate the secure sharing of CDR data at the request of the customer, to enable the customer to acquire the goods or services from the Provider.

Consumers who choose to acquire the services of third party Providers through the platform operated by a Principal do so on the 'Provider's' terms and conditions and services. There is no form of agency between the principal and Provider - in other words, Providers will bear exclusive responsibility for the services they provide to consumers and consumers will be able to enforce their rights against Providers.

For example, consider QuickBooks Online customers inviting their accountants and bookkeepers into their QuickBooks Online accounts. Customers are able to choose who their accountants/bookkeeper's are and Intuit as principal would not bear any liability for

the quality of the services provided by that accountant or bookkeeper to the QuickBooks Online customer.

We believe the proposed inflexibility of CAP liability arrangements would also 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.

Furthermore, we believe that without significant changes in the proposed CAP arrangements to provide for tiered accreditation, the retention of relevant CDR data to satisfy legislative obligations, a limit to the extent that CDR data is classified as 'derived data', and contractually determining liability arrangements, accountants and bookkeepers will be unintentionally hampered in their ability to provide their services to Australian consumers.

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.

Please contact [redacted] or [redacted] for further information.

Table 1. Alignment between CDR Requirements, ATO DSP Operational Framework and SSAM

CDR Requirement Source	CDR Requirement Category	DSP Ops Framework (Low volume)	DSP Ops Framework (10K records)	SSAM (1000+ connections)
CDR – Supplementary accreditation guidelines Information security	Assurance Report & comparable standards	· ISO27001 / IRAP / OWASP ASVS 3.0 / SOC 2 Self-Assessment	· ISO27001 / IRAP	· Self-assessment against SSAM controls
	Ongoing Information Security Reporting obligations	· Annual review and bi-annual self-certification · Notification of material change of circumstances	· Annual review & re-certification as required by the applicable standard · Notification of material change of circumstances	· Annual self-assessment submitted to DSP
	Privacy Safeguard 12	· Mandatory security monitoring and notification practices – including reporting to the ATO and as per the Notifiable Data Breach scheme, APPs, and Privacy Act.		
	Information Security Controls	· See below - CDR – Accreditation Controls guidance		
	Guidance on outsources service Providers	· Supply chain visibility – Entity, ABN, Service Provider role. · Add-ons > 1K connections report · Additional offshore data hosting requirements – APRA CPG 235 / SPG 231		
CDR – Supplementary accreditation guidelines Insurance	This requires an accredited person to have adequate insurance, or a comparable guarantee, in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of any of the following to the extent that they are relevant to the management of CDR data: obligations under the Act, any regulation made for the purposes of the Act, and the CDR Rules.	· No equivalent	· No equivalent	· No equivalent

CDR – Accreditation Controls guidance	1. An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	· Required – DSP to self-assess compliance with ISO27001	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· Partial mapping – Add-on to self-assess
	2. An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	· Required – DSP to self-assess compliance with ISO27001	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· Partial mapping – Add-on to self-assess
	3. An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle.	· Required – DSP to self-assess compliance with ISO27001	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· Partial mapping – Add-on to self-assess
	4. An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	· Required – DSP to self-assess compliance with ISO27001	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· Partial mapping – Add-on to self-assess
	5. An accredited data recipient must take steps to limit prevent, detect, and remove malware in regard to their CDR data environment.	· Required – DSP to self-assess compliance with ISO27001	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· Partial mapping – Add-on to self-assess
	6. An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data.	· Required with some allowances for micro-DSPs	· Mandatory – DSP is independently certified against ISO27001 or ISM.	· No equivalent