Consumer Data Right rules amendments (version 3)

Enabling financial empowerment

Governments and the global policy community are focused on expanding financial empowerment as part of economic policy. Around the world, we see consumers expect more control over their lives, including how they manage their finances.

G20, World Bank, IMF, OECD all advocate for digital financial tools to provide financial access, especially to the underserved. These tools, or more specifically, Digital Financial Services (or DFS), are defined as "financial services accessed and delivered through digital channels", often "powered by FinTech's."

The main focus of financial empowerment is to build the skills consumers need to manage money and learn to choose the financial products and services that work for them. These new financial channels are helping democratise digital tools for consumers and small and medium enterprises (SMEs), putting the knowledge, confidence, and tools that enable small businesses to grow via insights previously only available to large entities.

Digital Financial Service platforms such as Intuit QuickBooks enable small businesses to be compliant and organised better understanding and managing their finances with insights, tools, and opportunities. They help entrepreneurs get paid, gain access to capital, better understand their books, find new customers, and reduce costs.

Small and medium-sized businesses have shown they can be agile and innovative and connect all aspects of a business through digital, from cash flow to payments, payroll, capital, and money management. They can boost productivity and unlock new revenue opportunities.

Australia's Consumer Data Right must leverage the accelerated shift of financial empowerment and control to help bring prosperity to all Australian consumers, including those operating and advising small businesses.

Increasing pathways to participation

Intuit supports the efforts of the Treasury to remove barriers to participation and to fostering competition and innovation by increasing pathways to participation.

As the original report into establishing a Consumer Data Right noted, open banking should create opportunities. It should provide a framework on which new ideas and businesses can emerge and grow, establishing a vibrant and creative data industry.

Treasury's consultation paper rightly acknowledges that the consumer benefits of the CDR are intrinsically linked to establishing a vibrant ecosystem of accredited data recipients (ADRs) and other participants.

By providing alternative and more economical pathways to participation within the CDR regime, we expect that more digital financial service businesses will participate and innovate and that new products and services will be developed and offered to Australian consumers and small businesses.

Intuit supports the proposed draft rules giving sponsors a new obligation under Schedule 2 to the CDR Rules to implement a third-party management framework requiring affiliates to be managed by the sponsor in line with a defined third-party management framework.

It is worth noting the robust third-party management frameworks that already exist at Intuit and other Digital Service Providers (DSPs) organisations.

The ATO collaborated with DSP) 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 cybersecurity controls designed to reduce the risk of a malicious cybersecurity incident or an accidental data breach.

Trusted Advisers

Intuit has long supported the inclusion of the advisers of small businesses (including accountants, bookkeepers, tax agents etc.) as trusted recipients of a consumer's small business data to provide advice or services - particularly those that offer business, taxation or regulatory compliance advice and services.

We support in principle the amendments to Schedule 3 of the CDR Rules to allow a consumer to consent to an accredited person disclosing a consumer's CDR data to a person within a specified class (referred to as 'trusted advisers') however;, we have three major concerns:

1. it does not reflect the current real-world use of non-professional advisers by small businesses and would introduce significant friction to the consumer's existing experience;
2. it places onerous audit responsibilities on Digital Service Provider ADRs; and
3. the prescriptive nature of the designated professional classes constricts the CDR regime's ability to foster innovation as new use-cases emerge.

Non-professional advisors

Treasury's intention for the rules to facilitate current consumer practices of the permissioned sharing of their data with trusted third parties to receive advice or service and increase convenience and control for consumers is a good one and deserves support. However, it doesn't encompass the agency small businesses in Australia currently enjoy and depend upon to run their businesses.

Rule 1.10C provides that an accredited person can invite a CDR consumer to nominate one or more trusted advisers. The trusted adviser must be a member of one of the following classes:

- qualified accountants;
- persons who are admitted to the legal profession;
- registered tax agents, BAS agents and tax (financial) advisers;
- financial counselling agencies;
- financial advisers or financial planners;
- mortgage brokers.

While the six trusted advisor classes proposed by Rule 1.10C may be appropriate for most individual Australian consumers, it is insufficient to adequately serve the current needs of Australian small businesses.

The reality is that while most small businesses will make use of one or more of these professional classes on a regular basis, it is quite common for an SME to have some of its

backend functions (such as bookkeeping) performed by non-professional employees, family members or other trusted associates.

By specifying the professional classes with whom an Australian business participant in the CDR may share their data creates a real risk that millions of small businesses will no longer be able to rely on the non-professional but trusted services that are essential to their productivity and growth.

While trusted advisers such as accountants and bookkeepers are well known for helping small business operators make excellent decisions when it comes to their business and financial success, we believe that with appropriate consent controls, business CDR consumers should not be restricted to sharing their data with a limited class of certified professionals.

We recommend that the CDR Rules explicitly incorporate a Trusted Adviser disclosure consent model for business. Consent controls for business trusted advisers might include broad purpose identification, including but not limited to business compliance, business record keeping, business strategy and business marketing advice. We submit that such CX standards made by the Data Standards Body must ensure informed decision making while remaining understandable, intuitive and effective.

Business CDR consumers should be trusted to obtain the advice and services they need with the freedom to share their data if they desire. It should not be the responsibility of the Rules to dictate to business CDR consumers with whom they may legally conduct business.

If the Government has concerns about how a consumer's data is managed after the directed and permissioned sharing by an ADR, we suggest that with reform, the Privacy Act is the appropriate legislation to regulate how that information is handled.

Reasonable steps

The most significant barrier to business CDR consumers participation in the open banking regime is the requirement that an ADR cannot disclose CDR data to a trusted adviser unless it has taken reasonable steps to confirm the person to whom the data is to be disclosed is a member of a class of trusted advisers set out in the CDR Rules (rule 7.5A(3)).

The Exposure Draft Explanatory Materials (the EM) to the Rules make it clear that 'reasonable steps' has yet to be defined. It is envisaged that what constitutes reasonable steps will be detailed in guidance material. Until it is known what those reasonable steps may entail, we are unable to support this proposed amendment.

The EM suggests that reasonable steps might include the ADR checking a register for the relevant class of trusted advisers. Given there is no existing online register whereby an ADR may confirm that a trusted adviser is a member of a class of trusted advisers mentioned in subrule 1.10C(2), the creation of such a register would require the development of an entirely new CDR regulatory layer on top of the existing ACCC Register involving all

relevant industry groups; ADRs and the ACCC. This seems more complex and costly with inevitable delays than necessary.

Consistent with previous submissions, we believe that the CDR rules framework should not attempt to regulate or limit human interaction, instead of focusing on the regulation of and data standards of the machine to machine processes of the CDR.

We recommend that business CDR consumers are presented with an informed consent experience to ensure they know their obligations. Following informed consent from business CDR consumers, data should flow.

We recommend ongoing consultation with accounting, bookkeeping and small business organisations to fully appreciate the extent to which small businesses make informed consent decisions every day to share individual revenue, liability and asset records with trusted advisors on whom they rely.

Limiting innovation

While we understand that the Consumer Data Right rules are intended to be 'iterative' and evolve with community expectations, unless either the classes of 'trusted advisor' or definition of 'insight disclosure' is expanded, the Rules run the risk of preventing new use cases from similarly evolving due to the exclusive prescription of certain classes of professions as Trusted Advisors.

New and emerging use cases, including ag-tech, MedTech and regtech, will not develop sparked by CDR-enabled innovation due to those sector's advisors not fitting the prescribed class. For example, approximately 2.2 million workers are directly paid under Australia's modern award system. With over 120 awards with complex and often confusing rates of pay, allowances and role classifications, there is a lot that businesses must navigate to pay their employees correctly, leaving staff underpaid and businesses facing back payments and fines. RegTech and FinTech can help millions of small businesses reduce the effort and cost of complying with awards.

Unless Australian small businesses are empowered under the CDR with the same rights to securely share their permissioned data with emerging technologies as they have today, the innovation that removes further friction from business processes and improves productivity will not be enabled under the CDR.

Again, we submit that business CDR consumers presented with an informed consent experience should be trusted to obtain the advice and services they need with the freedom to share their data if they desire securely.

CDR insights

Intuit welcomes Treasury's efforts to provide the disclosure of CDR insights as enabling a more secure and auditable way for business CDR consumers to share insights from their CDR data. This is particularly important for the millions of Australian small businesses that rely on sharing their revenue, liabilities, and asset data for taxation or regulatory compliance, advice, and services.

Rule 1.10A(3) defines an insight disclosure consent as a consent given by a CDR consumer for an accredited data recipient to disclose particular CDR data (the CDR insight: see rule 1.7(1)) to a specified person for a specified purpose, which are:

- to identify the consumer
- to verify the consumer's account balance
- to verify the consumer's income, or
- to verify the consumer's expense.

We recommend two amendments that need to be made to Rule 1.10A(3) to ensure that business CDR consumers can disclose business-relevant CDR data. Specifically, it is unclear if references to verify[ing] the consumer's "income" and "expenses" sufficiently incorporate a business CDR consumer's accounting needs.

Secondly, the purposes of 'verify' as explained in the EM accompanying the Rules seem to contemplate a binary 'Yes/No' response. While this information may be helpful in many consumer-facing use cases, it is not sufficient in most business-use instances in which a business CDR consumer will need to share discrete point-in-time insights.

For example, a small business may elect to provide and confirm relevant factual information about their business revenue, liabilities and assets with a third party to create financial statements, analyse and validate them, then report to the Australian Tax Office. Such insights need to include historical insights to properly account for business activities and enable small businesses to comply with their tax and recordkeeping obligations properly.

To ensure that business CDR consumers can safely disclose relevant CDR insights, we recommend including the following specified purpose be included in Rule 1.10A(3):

- *to verify the consumer's individual business revenue, liabilities and/or assets*

We submit that clarification on the purposes of 'verify' in the EM accompanying the Rules to clarify that discrete insights are also in view is necessary for the avoidance of confusion.

Derived Data

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-management 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. However, for transactions to be entered into a business ledger, the small business operator, employee, or trusted advisor reconciles/verifies pending transactions and may assign those transactions categories, append notes or correct details. Under the current proposed CDR rules amendments, despite the reconciliation and addition of new information to the 'raw' CDR data, because the ledger data now contains CDR data, it is subject to and must be dealt with in accordance with the CDR regime. This can easily lead to a scenario where all a business CDR consumer's accounting information is treated as CDR data. Given that such accounting data must sometimes be kept and shared with a wide range of business and regulatory stakeholders (e.g., directors, shareholders, ATO, ASIC, and ASX, to name a few), we do not believe that the reconciled ledger entries of a business CDR consumer should be considered CDR derived data.

Because ledger entries are not raw data from an accredited data holder but user-entered, reconciled transactions, one acceptable limit to 'derived data' is to treat ledger data as a CDR insight. This would enable a safer and more efficient way for consumers to share insights obtained from their CDR data to receive goods and services and comply with their taxation or regulatory obligations.

Extending ill-defined terms such as 'derived data' onto financial management software platforms, already providing essential productivity and compliance-related services to small businesses through consumer control of data, will have significant detrimental effects when the focus needs to be on enhancing consumer control and business productivity.

Conclusion

As a long-time global leader in financial technology innovation, Intuit has been working for years to make digital financial life better for consumers, small businesses, and the self-employed. Underlying this innovation is the core tenet that consumers 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.

Over the last 18 months, we've been inspired by the resilience and tenacity of Australian small businesses. Small business owners and operators have had to reimagine virtually every aspect of their business during COVID. They've gone to great lengths to keep their doors open, keep their employees and customers safe, and navigate the uncertainty that comes with a global pandemic.

Without sensible amendments to provide for the permissioned sharing of data with a business CDR consumer's chosen trusted adviser and a limit to the extent that CDR data is classified as 'derived data', small businesses will be prevented from accessing the advice

and services they need to be productive and meet their taxation and regulatory obligations.

We believe that one way of enabling SMEs to have full access to the benefits of the CDR is to ensure Australian small businesses have the same agency to share their data with trusted advisors and third parties as they currently do outside the CDR.

We are greatly encouraged by the engagement that we have had with Treasury. We appreciate that Treasury is actively seeking to understand the needs of small businesses and listening to the feedback from the financial management software industry. We are hopeful that current impediments to CDR participation by business consumers and trusted advisers will be addressed and remedied in a timely manner.

Please contact Steve Kemp at steve_kemp@intuit.com or Simeon Duncan at simeon_duncan@intuit.com for further information.