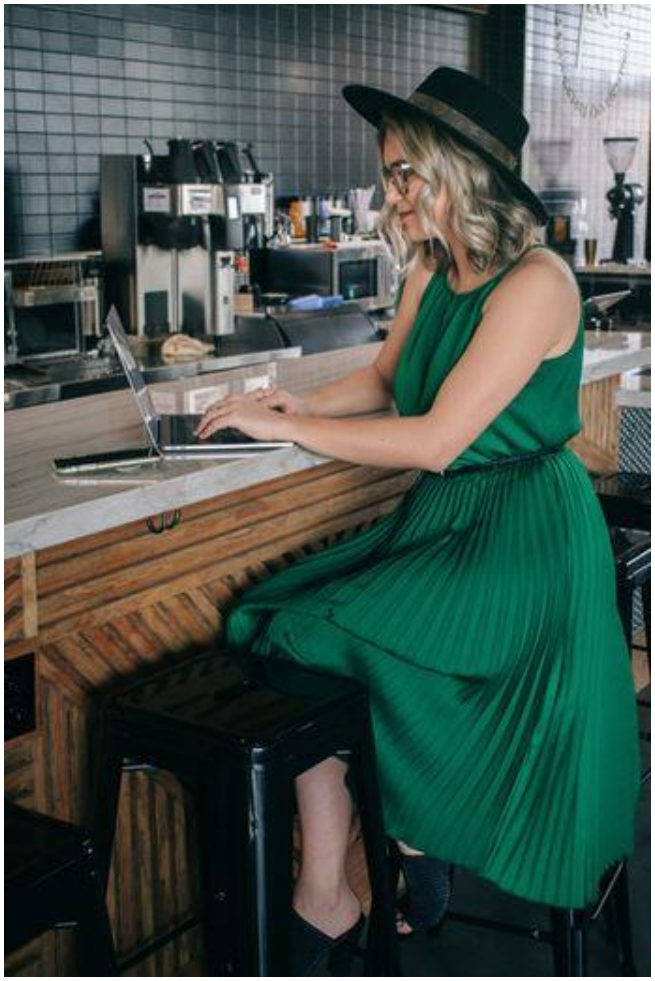
Financial Data and Technology Association



SUBMISSION PAPER:

Submission to the Treasury – Consumer Data Right rules amendments (version 3)

FDATA ANZ and our members are pleased to offer this submission in response to the request for feedback on the proposed amendments.

TABLE OF CONTENTS

1. Foreword

Open Banking, a precursor to the Consumer Data Right, began as a grassroots movement, campaigning for the legal rights of consumers and businesses to have control of their financial data and share this data with businesses of their choice digitally. It is part of a broader suite of Open Data initiatives to empower consumers and small businesses to access, change and benefit from the data held about them by governments and institutions.

The initiative has gathered considerable momentum; various markets worldwide assess, adopt, or implement laws and regulations to support it. In the EU, Canada, USA, Mexico, Brazil, India, Japan, Australia, Russia, New Zealand, South Korea, Singapore, and many other significant markets are already at varying stages of review, policy development or implementation.

Despite these positive market developments, there is still much to understand about the versatility of Open Data and Data Portability to unlock economic potential and improve customers' financial well-being. In addition to exploring these opportunities, there are also risks and ethical considerations which will be critical factors for governments and regulators in developing policies moving forward.

Research is needed to understand, measure, and forecast the considerable impact of Data Portability on society and shape public policy to ensure a Consumer Data Right creates positive disruption and the appropriate flows of capital allocation in markets and assess regulation techniques.

FDATA wishes to commend the Australian government and the Treasury Department in engaging in a formal consultation on the format that a Consumer Data Right may take and how this regime will positively affect and benefit the nation. Various groups have supported these works intending to design and develop a fit-for-purpose solution.

FDATA will continue the CDR conversation and assist in the exploratory process with Industry, Consumer Groups, and the Government alike. The importance of a planned and fore-thinking approach that involves various stakeholder groups will benefit the ecosystem and benefit the nation.

To arrive at the most suitable solution for Australia, working with such groups of expertise and enthusiasm and a comprehensive suite of participants is essential. In Australia, FDATA has provided comprehensive research and advisory to Federal Regulators and Government alike.

2. About FDATA

The Financial Data and Technology Association is the not-for-profit trade association leading the campaign for Open Finance across many markets. It is also a focal point of that industry knowledge in the financial community. FDATA was initiated in the UK when the government considered adding account data access to the Second Payments Services Directive in 2013 and was formalised in 2014.

In addition to working with EU policy makers, FDATA was heavily involved in the UK Open Banking Working Group in 2015. In 2016 the working group's output was published by HM Treasury as the Open Banking Standard.

Having helped UK regulators to shape the agenda that led to the formation of the UK Open Banking Implementation Entity (OBIE), FDATA has been represented on the Open Banking Steering Group. We have also played a significant role in helping OBIE drive high-quality standards and ensure that regulators and policy makers have been kept fully involved in the challenging areas.

The effort of coordination to common standards was recognised when FDATA was invited to develop a programme of engagement amongst policy makers in many different markets. Having already launched new chapters in North America in 2017 and Australasia in 2019, the FinTech community requested to continue developing across other markets. FDATA Global now has active chapters in Asia and South America from 2019, and the mandate is to expand in Asia and establish an African chapter in 2021.

Adding to the broad scope of its international representation, FDATA has also been heavily involved in the UK in developing input to assist the Pensions Dashboard programme. This assistance is in addition to representation in the Steering Group of the Open Savings and Investment programme run by TISA, in the FCA Open Finance Advisory Group and several initiatives in the domain of digital identity.

This work is intended to be an organic, iterative document and updated as the story unfolds in subsequent versions. It is specifically designed as a high level and convenient reference guide in this edition. It will continue to expand to provide more depth in technical and regulatory matters in subsequent editions.

The Australasian Chapter of FDATA continues to work closely with Federal Ministries such as the Treasury Department and Department of Finance, Federal Regulators including the ACCC and OAID, and all echelon of industry in the pursuit of the most effective Consumer Data Right environment and the highest level of Open Finance available to consumers across the region.

Our membership has grown significantly over the past twelve months to now include Digital Banks, Regional Banks, Intermediaries, Technology Providers, Platform Providers, Privacy Platforms, Deep Data Houses, Insights Brands, FinTechs and Out of the Box Providers. Our membership now includes several International Brands that have entered this market after dominating the United Kingdom, the United States or Europe. Right now, it is truly an exciting time to be involved in Open Data in Australia.

3. Executive Summary

FDATA commends the Treasury Department and the Data Standards Body in their review and reconsideration of the Competition, and Consumer (Consumer Data Right) Rules 2020.

FDATA and our members have been actively involved in exploring and reviewing the proposed rules, both as a community and within our ecosystems. This submission reflects those views and our considerations on building a robust and flourishing CDR environment.

FDATA ANZ is pleased to offer this submission in response to the request for feedback on the proposed amendments. Please accept this shortened submission in light of the call for succinct (short-form) and direct feedback to proposed amendments. If a longer-form expanded report is deemed to be advantageous, please do not hesitate to reach out.

We have chosen to provide a series of responses and recommendations to seven categories:

1. Amendments relating to sponsored accreditation
2. Amendments relating to CDR Representatives
3. Amendments relating to Outsourced Service Providers
4. Amendments relating to Trusted Advisers
5. Amendments relating to Insights
6. Amendments relating to joint accounts
7. Amendments relating to staged implementation

And based on the following priorities:

Introduction of new accreditation levels: creating new pathways for service providers to become accredited data recipients. Proposals for new levels ('tiers') of accreditation promise lower barriers to entry and reduce compliance costs for service providers that do not require unrestricted access to CDR data. They also recognise that supply chains for data services regularly involve multiple service providers and that CDR participants can appropriately manage risk and liability through commercial arrangements.

Provide greater choices for consumers about whom they share their data with: permitting accredited data recipients to disclose CDR data with a consumer's consent to third parties, including to their trusted professional advisors (such as accountants, tax agents and lawyers), and any third party on a limited 'insights' basis.

I**ncrease the consumer benefit:** allowing business and corporate consumers to access their CDR data and adding flexibility and functionality to improve the consumer experience regarding the management of consumer consents to collect and use CDR data, joint bank accounts, and accounts have additional cardholders.

As shared in previous feedback and formal submissions, FDATA supports the principle of aligning privacy consideration with well-formed technology, supported by robust and understandable consent frameworks.

We have chosen to provide a series of responses and recommendations considering the:

FDATA Member's Views: As a membership-based organisation, FDATA collects, collates and shares the views and opinions of our members who are active participants within the banking and fintech community.
Global Participants: As a global trade association, our experience and participation within the United Kingdom, European, North American, South American and Australasian markets influence our advice and feedback on the creation, introduction and evolution of the Open Banking and Consumer Data Right in Australia.
Industry Experience: The regional representatives and associated staff of FDATA have worked within the banking and financial sectors within their respective geographies. This experience is employed within the collective contribution and community discussions as facilitated with FDATA's membership.

FDATA understands the appeal in developing one set of rules that can be employed across all sectors but advises the need to separate the complexities of data sharing via read-access and action initiation. For some of the proposed amendments, the complexities and risk parameters will not significantly increase when applied solely to data sharing, "Read Access".

When combined with the ability to initiate payments, "Action Initiation", however, the supply of insights combined with moving money may increase the potential risk for the consumer.

4. Amendments relating to sponsored accreditation

Amended Rules

Part 1—Preliminary

1.10D Meaning of *Sponsorship Arrangement, Sponsor and Affiliate*

Part 5—Rules relating to accreditation

Division 5.1—Preliminary

5.1 Simplified outline of this part

Division 5.2—Rules relating to the accreditation process

Subdivision 5.2.1A—Levels of accreditation 80

5.1A Levels of accreditation

5.1B Sponsored accreditation

Schedule 1—Default conditions on the accreditation

Part 2 —Default conditions on accreditations

2.2 Conditions on sponsors and potential sponsors

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

Part 1—Steps for privacy safeguard 12

Part 2 —Minimum information security controls

FDATA Response

FDATA's membership has reviewed the proposed rules in line with consideration to:
Privacy Impact, Commercial Models, Technology and Infosec Requirements, Liability Frameworks and the Requirements for both the Sponsors and the Affiliates to operate as part of a Sponsored Arrangement. It is for this reason that two different trains of thought have appeared. We have separated these into Options; Option 1 and Option 2.

In principle, FDATA supports the attempt of the ACCC to remove barriers for participation and remain focused on the CDR intent of promoting innovation and Competition amongst Industry.

In prior submissions, we have advocated for a balance between introducing a simplistic regime and removing potential entry barriers. We acknowledge that barriers may exist due to the size and maturity of the participants, confusion over classifications and obligations of participants, or through multi-faceted business models that are difficult to categorise within simple accreditation levels.

As with the other proposed models of Outsourced Service Provider and CDR Representative, the membership of FDATA supports the continued inclusion of the Sponsor/Affiliate model within the Consumer Data Right.

Option 1:

Option 1 is the most closely aligned to the proposed rules of Sponsor/Affiliate.

In principle, many of our members support the intended liability model, accreditation requirements, collection and sharing of data parameters, and the Sponsor's requirement to provide 'assurance' for the Affiliate.

There are, however, several points that require clarification or consideration.

Affiliate Registration:

The ability for an affiliate to operate without a sponsor creates a risk of non-compliance and a changed liability framework for the period that this occurs. It is essential to acknowledge that the commercial arrangement between an Affiliate and a Sponsor may expire for many reasons and may not be at the Affiliate's fault. One thought is to freeze the accreditation through the period that the Affiliate lacks direct Sponsorship. As per the proposed rules, the Affiliate is not allowed to request Data without Sponsorship. This would remove the ability for the Affiliate to 'operate'. It is not articulated in the proposed rules what the Affiliate may continue to do during this period. Still, it is assumed that they may maintain their software, continue to have visibility over users and develop their offering. Without access to data, they would not be able to process any user requests.

This inability to operate a business, essentially frozen without Sponsorship, may impact the attractiveness of this model to market entrants and other participants considering seeking Sponsored Accreditation. That being said, the time that an Affiliate can operate without Sponsorship should be less than the current proposed period of time (4 months), considering that the party would essentially be operating without any discernible liability framework should a breach occur.

We encourage the requirement of a valid Sponsorship Arrangement to be demonstrated before the Affiliate can apply for Sponsored Accreditation. The arrangement is the deciding factor in the ability of the Affiliate to operate, so it would be logical that this must exist before the accreditation application reaches the DRA. In addition, we advocate for the Affiliate giving assurances to the DRA of them complying with rule 1.9 Fit and proper person criteria before being eligible for accreditation.

Sponsorship Compliance:

Under this option, we support the concept of Sponsors creating and maintaining stringent compliance, training and risk assessment programs, not just via the initial assessment and registration of the Sponsorship or during the annual review, but on an ongoing basis. For those Sponsors willing to assume the role of Primary in this option, their existing compliance and third-party management systems may be adapted to meet the requirements of the CDR.

This would have two primary benefits to the relationship.

- Firstly, the Sponsor will pass on controls and checks via a robust third-party management framework that will benefit the Affiliate through the repeated process/system. If the Affiliate is a market entrant, depending on the size and maturity of the organisation, it may not possess standalone resources to focus on these elements. The ability of the Sponsor to pass on these tools and processes will benefit the Affiliate's development.

- The second positive outcome of stringent Sponsorship Compliance and a robust third-party management framework will be through the regular and ongoing re-assessment of the Affiliates compliance with the Infosec parameters outlined in

Schedule 2 risk-assessments, training and access to the Sponsors risk/compliance team. The more rigorous compliance framework within a Sponsor's organisation may increase the attractiveness of an arrangement with potential Affiliates and increase the commercial opportunities of a proposed Sponsorship arrangement.

Option 2:

In Option 2, the entire relationship between the Sponsor and the Affiliate is fundamentally altered. In this option, the role of the Sponsor is to provide a product or service to enable the Affiliate to operate within the CDR environment. This offering is often referred to as 'Open Banking in a Box'. The Sponsor would be primarily responsible for ensuring the Affiliate meets their technical and CX requirements and may or may not include providing additional services such as Data Storage or the provision to operate within a Data Enclave environment.

The Affiliate in this arrangement would carry the burden of the remainder of CDR Accreditation, Liability and Compliance Requirements.

Placing the accreditation responsibilities onto the Affiliate is thoughts to bring several benefits to them:

- The accreditation preparation process requires an organisation to address critical elements such as creating crucial documentation, operational systems and processes, creating Organisational Charts, meeting the minimal Infosec Requirements, Insurances, Identifying Key Personnel, Risk Frameworks, and such. By placing the burden of compliance and attestation on the Sponsor, the Affiliate misses essential business development elements that will ultimately benefit their longevity in the market.
- The ability for the Affiliate to apply for accreditation will reduce the risk of a Sponsor-less Affiliate operating in an unprotected manner without access to an adequate Liability Framework.
- Will reduce the potential for confusion should a Breach Event be triggered within an Affiliate operating under multiple Sponsorship Arrangements.

- Align more closely with international models of Sponsors providing a Technology Environment or a Suite of Services to an Affiliate; with the Affiliate ultimately responsible to the client from an operational perspective.

In this option, the Sponsor would be entitled to enter into a Commercial Arrangement with an Affiliate for the Product/Platform/Services provision and would be liable under contract law for these elements. The Affiliate, in attaining accreditation, would assume the liability for the operations of their entity and for any potential Data Breaches that may occur through their operations.

The Sponsor's provision of a verified Product/Service would reduce the risk of non-compliance by the Affiliate and would therefore allow for an "Accreditation Light" model to exist.

5. Amendments relating to CDR Representatives

Amended Rules

Part 1—Preliminary

1.10AA Meaning of *CDR representative* and related terms

Division 1.4—General provisions relating to data holders and to accredited persons

Subdivision 1.4.4 – Other obligations of accredited persons

1.16A Obligations relating to CDR representative arrangements

Part 4—Consumer data requests made by accredited persons

Subdivision 4.2.2—Requests to seek to collect CDR data from CDR participants

4.3A request for accredited person to seek to collect CDR data, made to CDR representative

4.3B Modifications of Division 4.3 in relation to CDR representative

Part 7—Rules relating to privacy safeguards

Division 7.2— Rules relating to privacy safeguards

Subdivision 7.2.1—Rules relating to consideration of CDR data privacy

7.3A Rule relating to privacy safeguard 4—destruction of unsolicited data—CDR representative

Subdivision 7.2.4— Rules relating to integrity and security of CDR data

7.10A Rule relating to privacy safeguard 11—quality of data—CDR representative

Subdivision 7.2.5— Rules relating to correction of CDR data

7.10A Rule relating to privacy safeguard 11—quality of data—CDR representative

Schedule 1—Default conditions on accreditation

Part 2 —Default conditions on accreditations

2.3 Conditions in relation to CDR representatives

FDATA Response

In principle, FDATA membership supports the proposed CDR Representative Model rules. This model appears to be the closest example of the successful agency model in the United Kingdom's Open Banking framework.

To summarise, our members support the following inclusions in V3 of the rules:

- The request for accredited person to seek to collect CDR data, made to the CDR representative.
- A CDR consumer requests a CDR representative to provide goods or services to the CDR consumer or another person; and,
- The CDR representative needs to request its CDR principal to collect the CDR consumer's CDR data from a CDR participant under these rules to use it to provide those specified goods or services.
- The CDR representative may, per Division 4.3 of the rules, ask the consumer to give collective consent for the Principal to collect their CDR data from the participant; and
- To use that consent to disclose that data to the CDR representative, and for the CDR representative to use that specific CDR data to provide those requested goods or services.
- That the amended rules give valid consent to the CDR principal to seek to collect the requested CDR Data from the CDR participant

Data Flow through CDR Representative Model:

Concerning the consent flow of service data, we support the insertion that:

From the point of view of a CDR consumer who is the customer of a CDR representative, the consumer deals only with the CDR representative, as if it were an accredited person. The consumer requests the goods or services from the CDR representative; the CDR representative identifies the CDR data that it needs to provide the goods and services; the consumer gives their consent to the representative to collect and use the CDR data. The consumer is informed that the CDR principal will do the actual collecting but as background detail.

This alignment between the expected CX experience commensurate to dealing with the B2C application/brand will avoid unnecessary confusion over the single brand of the Principal or subsequent providers within the data chain. Additional clarity around the treatment of subsequent providers, such as aggregators that may supply goods or services to the Principal, is needed to assess the consumer's overall CX experience.

Proposed Liability Model of CDR Representative Model:

Our members support the proposed liability framework and the data collection, data obligations and safeguard provisions that this model provides. Regarding amendments under

1.16A, our member's support the needs for the Principal in this CDR Representatives arrangement being an accredited person/party. Given that this model defaults liability to the Principal, ensuring that the Principal holds the appropriate processes, systems and insurances would be mandated by the accreditation process within the CDR framework. The insertion of rule 4.20A to Subdivision 4.3.5 is supported.

CDR Representative Registration:

Under rule 2.3 of Part 2 of Schedule 1, our members support the notification of appointing a CDR Representative within 30 days. This timeframe is in keeping with corporate reporting requirements.

6. Amendments relating to Outsourced Service Providers

Amended Rules

Part 1—Preliminary

1.10 Meaning of *outsourced service provider* and related terms

Schedule 2—Steps for privacy safeguard 12—security of CDR data held by accredited data recipients

Part 1—Steps for privacy safeguard 12

Part 2 —Minimum information security controls

FDATA Response

In principle, FDATA and our membership support the Outsourced Service Provider (OSP) model's continued inclusion within the Rules. As per the model's entry in the first *Competition and Consumer (Consumer Data Right) Rules 2019,* FDATA believes that this commonly used and long-standing commercial example exists across any number of sectors and will bring closer alignment between existing practices and acceptable participants in the data-sharing arena.

CIO Australia magazine defines Outsource Service Provider as; *"Outsourcing is a business practise in which services or job functions are farmed out to a third party. In information technology, an outsourcing initiative with a technology provider can involve a range of operations, from the entirety of the IT function to discrete, easily defined components, such as disaster recovery, network services, software development or QA testing."*

Proposed Amendments and Inclusions of the Outsourced Service Provider Model:

To summarise, our members support the following inclusions in V3 of the rules:

(1) Where two persons are the Principal and the provider in a CDR outsourcing arrangement, the provider is an ***outsourced service provider*** of the Principal.

(2) The ***CDR outsourcing arrangement*** is a written contract between a person (the ***Principal***) and another person (the ***provider***) under which the OSP may:
   a. Collect CDR data from a CDR participant on behalf of the Principal and/or
   b. Provide goods or services to the Principal using CDR data that it has collected on behalf of the Principal or from the Principal; and
   c. If the OSP is an accredited party, they may collect CDR data from a CDR participant on behalf of the Principal and/or
   d. Provide goods or services to the Principal using the data disclosed to the OSP by the Principal.

(3) The OSP must comply with the steps in Schedule 2 and must not use or disclose the service data other than per the outsourcing agreement with the Principal, and if directed by the Principal must:
   a. Provide the Principal with access to any service data that it holds;
   b. Return to the Principal the data that the Principal disclosed to it;
   c. Delete any service data that it holds per the CDR data deletion process;
   d. Provide, to the Principal, records of any deletion or direct any other person to which they have disclosed CDR data to take corresponding steps.

(4) The OSP will only disclose CDR data to parties for which they have entered into a CDR outsourcing arrangement.

Lowering Barriers to Entry:

Regarding the inclusion of OSPs to the accreditation models to lower the barriers to entry, this is a double-edged sword and may not achieve the desired effect.

Suppose the OSP enters into an arrangement with an ADI. In that case, there is no additional requirement for auditing of Infosec, assurance or attestation to establish or maintain a contractual relationship due to the existing governance of ADIs by prudential standards such as CPS 234. The ADI is obliged to provide a biennial assurance report and attestation – deferred for the 1st year as per the current rules. It is considered that the ADI will assume liability for the OSP and has more than the necessary systems, processes and safeguards to ensure the safe practices of the OSP. The ADI will also assume the liability of the OSP, and should any claims arise, will enforce the commercial contract between the two organisations. It would be in the ADI's interests to ensure that appropriate contractual arrangements are established and maintained within the commercial contract.

If the OSP enters into an arrangement with an ADR, then there is a requirement for the ADR to be audited and, by association, the OSP at the cost of the ADR. The audit will either be triggered by the registration of the ADR if registering the use of an OSP as part of the initial accreditation or by the notification of a material change to the use-case/operation of the ADR. This increased cost and audit requirement makes this model potentially less attractive and will not reduce the barrier to entry for the ADR.

7. Amendments relating to Trusted Advisers

Amended Rules

Part 1—Preliminary

1.10A Types of consents

1.10C Trusted advisers

FDATA Response

In our October 2020 submission, FDATA's members supported the concept of the inclusion of a category for Trusted Advisers;

At the heart of these questions is the concept that the consumer is requesting or directing their data to be shared with any individual or entity outside of a traditionally accredited participant.

Existing Use-Cases for Engaging a Trusted Advisor:

Long established existing practices currently stand. Examples of these consumer directives may be, but are not exhaustive:

- The sharing of (considered CDR applicable) data to prepare a financial statement.
- The sharing of (considered CDR applicable) CDR data to apply for a product or service.
- The sharing of (considered CDR applicable) CDR data in regards to a taxation requirement.
- The sharing of (considered CDR applicable) CDR data in the purchase of assets or property.

In each of these cases, the classification of a specific occupation and data requirement may be identifiable, i.e., Accountant, Financial Planner, Real Estate Agent, and so forth. For this reason, the category of Trusted Advisory may be appropriately assigned to provide greater protection to the consumer and to create a monitored environment.

When a consumer requests sharing their data with an unlisted class of professionals, a business, or a rare use case, the issue remains. Currently permitted through established practices, the introduction of CDR will require that current practices cease or materially change. This will invariably lead to consumers being forced to exit or circumvent CDR to access a service, or in some cases, just run their daily operations.

Under the current rules, a consumer can direct that a data holder transfer data directly to the consumer, who can then choose to share it with whomever they want, including a professional or a trusted advisor. Or that the business may send the requested data on behalf of the consumer directly from their files.

The Farrell Review noted that 'For consumers to have confidence in Open Banking they will need assurance that other participants – data holders and recipients – are accredited entities…'. This notion echoes the United Kingdom in their prohibiting the sharing of data with non-accredited entities. But this practice mainly covers the raw data, not Materially Enhanced or Derived Data as Financial Statements or Accountant Documents.

The juxtapose position of current practices, and the intended CDR processes may lead to individuals circumventing the framework and inadvertently increasing the risk to the consumer through reduced cyber protections and the assurances that accreditation may afford. This, in turn, will undermine the trust that consumers have in the system and will event in reduced participation from consumers.

FDATA supports the concept of an alternative approach of establishing an accreditation category for professionals and trusted advisors.

This would:

- Mean that data was not shared by a data holder or an accredited data recipient with a non-accredited data recipient.
- Mean that the ACCC did not need to try and determine and maintain a regulatory description of a professional or trusted advisor.
- Allow any party to be considered an accredited data recipient for this tier.

In adopting this approach, consideration should be made when accrediting professionals and trusted advisors to leveraging existing professional requirements for privacy and information security that professionals and trusted advisors are already required to meet.

Trusted Advisors Rule Inclusions:

There are several proposed rules that our members do not principally object to;

- Our members support the ability for consumers to nominate one or more persons as their Trusted Advisor.
- They support the inclusion of these six classes of Trusted Advisers. They do not dispute the classifications that have been proposed nor their definitions of the six classes. However, FDATA's members have raised concerns that the prescriptive nature of classes may limit the potential use-cases or constrict the regime's evolution as new use-cases and consumer directions come onboard. For this reason, these six classes do represent an exhaustive list.

Requirement for expanding the classes of Trusted Advisers under CDR:

If specific classes of Trusted Advisors are to be specified and defined, there will be a need to expand or evolve the list of acceptable occupations/positions.

Two additional classes of advisers currently receiving consumer data daily are Bookkeepers and Stock Brokers/Investment Advisers. Every day, Australian consumers and businesses share their confidential data, bank records, access to their bank feeds, copies of taxation records, and any number of private and confidential financial datasets to receive services from these professionals.

The Consumer Data Right is intended to raise consumer protections and to rely on well-formed APIs and privacy by design frameworks to share data upon consumer consent. By not broadening the classification of Trusted Advisers or prescribing which professionals are in and omitting standard classes of adviser, consumers will be forced to engage in potentially unsafe or dangerous data-sharing arrangements. They will not receive the enhanced consumer protections of the CDR.

The requirement to confirm the membership of an Adviser:

In addition, and potentially the most significant hurdle to implementing this model, rule 7.5A refers to the need for the accredited party to take reasonable steps to confirm that the trusted adviser is currently a member of a class of trusted advisers mentioned in subrule 1.10C(2).

At present that is no online directory of such advisers. There is no industry body that the accredited party can contact to confirm current registration in an appropriate timeframe. There is no ability for an API call to be initiated upon receipt of a consumer disclosure consent. This requirement is not practical, and the implementation of this rule without further consideration for the obligation of the accredited party will make disclosing data to these classes a risky and potentially liable option. This will render the ability for the consumer to request the data to be shared with Trusted Advisers a point of contention between the accredited parties and their obligations to conform with the rules.

One potential method of overcoming this requirement is for the government to amass and maintain a digital database of currently accredited advisors. However, this is not practical and will pose similar constraints to the government as it will to the market. FDATA's members appreciate the intention but are unable to reconcile the practical implementation of this requirement.

The presentation of an informed and complying consumer consent should be considered sufficient to allow data movement. However, if the introduction of a Trusted Advisor provision were to be adopted, this would require that that ACCC develop and maintain a detailed description in the Rules of each acceptable professional or trusted advisor. To increase consumer trust in the environment, consideration should be given to maintaining a register of accredited parties/professionals.

Trusted Advisors for Business Purposes

Further consideration must be given to the differences between how consumers engage Trusted Advisors and the nature of the service provision of Trusted Advisors to businesses. When an individual engages a Trusted Advisor, this may be for a single purpose or transaction such as a mortgage broker assisting with an application or on a more infrequent basis such as once a year to prepare their tax return. In contrast, businesses often use various advisors

and may have an ongoing relationship with them. This engagement may also involve both professional and informal advisors depending on the nature of and the complexity of the business.

FDATA believes that in the pursuit of operating a small business, they should be able to share their data with the advisers that perform a variety of complex or speciality functions. This may be more than the six classes listed in the proposed rules. To protect businesses, we also recommend that this business trusted advisor model is for physical persons only, not apps. They would only be able to access the data needed to perform their service in line with informed and expressed consent flow.

The proposed model moves away from Consumer Choice:

The decision to incorporate standard everyday practices of consumers and SMEs in Australia and their requirements to share financial data with third parties will disrupt or violate long-standing dependencies. Our members commend the attempts of the Treasury to evoke consumer protections; however, in doing this, there is a genuine risk that everyday businesses, and consumers at large, will no longer be able to rely on professional services that are critical to their businesses/lives.

- A small business can engage a neighbour or a friend to 'do their books'.
- A tradie to utilise a local bookkeeper in invoicing customers and preparing his GST reports.
- A manager/owner of a family business to grant access to his accounts to his stockbroker to manage the firm's investments.

These are all examples of everyday transactions that will be affected by this proposed model.

Scott Farrell's vision for Open Banking was, "***Consumers can now share the data they have, with the businesses they select, for use as they choose.***"

It was not, ***"Australians can now share some of their data, with selected businesses, for purposes that the Government have deemed acceptable."***

8. Amendments relating to Insights

Amended Rules

Part 1—Preliminary

1.10A Types of consents

FDATA Response

FDATA and our members support the entry of the term of Insights within the proposed rules. This particular class of data has been of great interest to the market. Given the evolution of data science empowered by the digitalisation of industry, the potential for the regulated use of Insights within the Consumer Data Right is immense.

As previously stated, our members are concerned about the limitations that the current prescription of the designated insight categories may bring for several reasons, in addition to the limitations of the use of insights more generally.

Potential Misalignment between Legislation, DDF and the interpretation of the Proposed Rules:

There is a significant misalignment between the CDR Legislation, the Data61 Deidentification Framework and the Proposed Rules.

Under the Legislation, the treatment of Insights and the de-identification of CDR data is:

Subdivision 1.4.5—Deletion and de-identification of CDR data

1.17 CDR data de-identification process

(1) This rule sets out the ***CDR data de-identification process*** for particular CDR data (the ***relevant data***).

Note: This process is applied by an accredited data recipient when de-identifying CDR data per consent from a CDR consumer (see Subdivision 4.3.3) and de-identifying redundant data for privacy safeguard 12 (see rule 7.12).

(2) First, the accredited data recipient must consider whether having regard to the following:

(a) the DDF;

(b) the techniques that are available for de-identification of data;

(c) the extent to which it would be technically possible for any person to be once more identifiable, or reasonably identifiable, after de-identification in accordance with such techniques;

(d) the likelihood (if any) of any person once more becoming so identifiable, or reasonably identifiable from the data after de-identification;

it would be possible to de-identify the relevant data to the extent (the ***required extent***) that no person would any longer be identifiable, or reasonably identifiable, from:

(e) the relevant data after the proposed de-identification; and

(f) other information that would be held, following the completion of the de-identification process, by any person.

(3) If this is possible, the accredited data recipient must:

(a) determine the technique that is appropriate in the circumstances to de-identify the relevant data to the required extent; and

(b) apply that technique to de-identify the relevant data to the required extent; and

(c) delete, per the CDR data deletion process, any CDR data that must be deleted to ensure that no person is any longer identifiable, or reasonably identifiable, from the information referred to in paragraphs (2)(e) and (f); and

(d) as soon as practicable, make a record to evidence the following:

(i) its assessment that it is possible to de-identify the relevant data to the required extent;

(ii) that the relevant data was de-identified to that extent;

(iii) how the relevant data was de-identified, including records of the technique that was used;

(iv) any persons to whom the de-identified data is disclosed.

(4) If this is not possible, the accredited data recipient must delete the relevant data and any CDR data directly or indirectly derived from it in accordance with the CDR data deletion process.

Note: For the CDR data deletion process, see rule 1.18.

(5) For this rule, the ***DDF*** is *The De-Identification Decision-Making Framework* published by the Office of the Information Commissioner and Data61, as in force from time to time.

Note: The *De-Identification Decision-Making Framework* could in 2020 be downloaded from Data61's website (https://www.data61.csiro.au/).

In addition, the Legislation states:

4.12 Restrictions on seeking consent

(1) An accredited person must not specify a period of time for the purposes of paragraph 4.11(1)(b) that is more than 12 months.

(2) An accredited person must not ask the CDR consumer to consent to collect or use their CDR data unless the accredited data recipient would comply with the data minimisation principle regarding that collection or those uses.

Note: See rule 1.8 for the definition of "data minimisation principle".

(3) An accredited person must not ask a CDR consumer to give consent to use or disclose their CDR data for any of the following uses or disclosures:

(a) selling the CDR data (unless de-identified following the CDR data de-identification process);

(b) subject to subrule (4), using the CDR data, including by aggregating the data, for the purpose of:

(i) identifying; or

(ii) compiling insights in relation to; or

(iii) building a profile in relation to;

any identifiable person who is not the CDR consumer who made the consumer data request.

(4) Paragraph (3)(b) does not apply to a person whose identity is readily apparent from the CDR data if the accredited person is seeking consent to:

(a) derive, from that CDR data, CDR data about that person's interactions with the CDR consumer; and

(b) use that derived CDR data to provide the requested goods or services.

Under the Data 61 Deidentification Framework (DDF)

Functional de-identification considers the whole data situation, i.e., both the data and the data environment. When we protect privacy and confidentiality, we are, in essence, hoping to ensure that de-identified data remains de-identified once it is shared or released within or into a new data environment, and therefore, functional de-identification has to consider all relevant aspects of this situation.

Yet under the proposed rules, and the interpretation provided by the Treasury Rules Team, whilst upholding the legislative de-identification parameter, as per Subdivision 1.4.5— Deletion and de-identification of CDR data, 1.17 CDR data de-identification process, the messaging from the Treasury around the treatment of entities creating insights and sharing

with unaccredited parties differs significantly from the treatment of parties creating insights for their own in-house use.

Consent aside, and assuming compliance with the data minimisation principle, the ability for an entity to create an insight within one part of their business renders their entire corporate environment according to the CDR obligations without increasing the risk of handling this data or any increased risk to the consumer. Suppose an insight is considered of low potential risk, allowing it to be shared with literally anyone. How can the retention of these insights be deemed significant enough to render the change in an organisations structure to utilise or store these insights internally? Mixing insights, or what has been labelled as "derived data", with non-CDR data does not materially increase the risk to the consumer if the accredited party has followed the Data Minimisation Principle and is not intending to abuse the rights and privacy of the consumer. If this was the case, why are the proposed rules deeming the risk parameter around sharing insights low to negligible, without any other prescription around its use or maintenance?

This treatment is further muddied by the interpretation of;
Subdivision 4.3.4—Election to delete redundant data
4.16 Election to delete redundant data
(4) This rule does not require the deletion of derived CDR data that were de-identified per the CDR data de-identification process before the collected data from which it was derived became redundant.

The proposed format of "Designated Insights":
Another issue is requiring insights to be formatted by the expressed response, 'this insight is equal to (set amount)', and most responses will be omitted. In simple terms, the chances of my bank balance being equal to the exact amount checked may be slim. There is a significantly greater probability that my balance may be equal to or greater than or equal or less than the figure requested to receive confirmation.

A typical treatment of calculating and sharing data insights is the Boolean data type. This data type has one of two possible values (usually denoted true and false) intended to represent the two truth values of logic. The Boolean data type is primarily associated

with conditional statements, which allow different actions by changing control flow depending on whether a programmer-specified Boolean *condition* evaluates true or false. For this example, one would include the parameters to check if specified data is Greater Than or Equal to a specified value. Alternatively, depending on the use case, Less Than or Equal to a specified value.

An example of a CDR Insight in practice:
If prospect.balance ≥ $1,000
Then return. positive. insight

Expansion and Review of Designated Insights:
Our members understand the proposed rules will allow for the four designated insights to be shared with unaccredited parties. Acknowledging the reduced risk of transmitting the limited data from the CDR bubble to outside the bubble, the reward is considered more significant than the potential risk.

With that being said, our members would like to understand the practice of reviewing the designated insights.

- Who is primarily responsible for reviewing the insights within this list?
- What are the processes proposed for such review?
- On what basis would a new insight be considered?
- Can the market recommend additional insights?

Additional Designated Insights:
We then created an equally long list of conditions around using these insights: our members believe that the current list is limited and not as valuable as it could be, particularly given the complexities around gaining access to the data and the prescribed use-cases under which it can be leveraged. If we continue to mandate designated insights, we risk creating a long laundry list of options for included insights.

- How do consumers provide consent for each one that they wish to use?
- How do we combine multiple insights?

- Can they be bundled?
- Will this be similar to the example of the data-sharing cluster when each must be selected individually?

Consent Parameters for Sharing of Designated Insights:

Our members have also raised concerns around the consent frameworks surrounding the designated insights. Further clarification is needed on consent to frame reasonable use of the insights and reasonable timeframes for the retention and addition uses of the insight. Our members have also raised concerns over the ability for insight disclosure consents to be bundled with other consent requests. An example of this may be for a Car Finance user-journey; Finance Provider A (as a Data Recipient) used a Consumer's consent to access CDR data and used the data to create an instant drive-away car finance product. Adding Action Initiations means Finance Provider A could also instruct the ABC Insurance Company to insure the car (using the same CDR data for the application) and pay the premium from the Consumer's bank account, all from a single consent.

The Implications of Consent Bundling are that:

- Accredited Parties with solid brands and value propositions will benefit most from the CDR because:
- Consumers will Consent to share more Action Initiations across a broader range of industries. The more Action and Payment Initiations can be bundled into a single consent, the more value for the customer and strategic growth for the recipient.

Initially, this may not represent a significant risk to the consumer, but the potential for abuse when Action Initiation and Payment Initiation is launched may be significant.

Sharing of Insights with Accredited Parties:

Further clarification may also benefit the market around the sharing of non-designated insights between accredited parties. The classification of insights is one of the most attractive to the market in providing products and services. Greater clarification around the inclusions/exclusions, transparency within consents, and the treatment of insights once processed are all items that need additional material published. Without clarification, there is

a significant risk to consumers and the market at large that interpretations may lead to practices outside of the rules, not through deliberate acts but rather through assumptions and misunderstandings.

The United Kingdom Experience:

Despite recognition over the sharing of global best-practice data standards and technical frameworks, there is a misalignment between the Australian version of the rules and the approach taken by the United Kingdom. The issue of Derived Data, including insights, including materially enhanced and value-added data, are no longer treated as Open Banking data once shared. This satisfies the prohibition of Open Banking participants sharing Open Banking Data with non-accredited parties. In this example, the classification of Open Banking Data has changed when the raw data has changed. There is a view that once data that a service provider has altered at the **consumer's request** or containing the IP of the accredited participant, the consumer can direct it to be shared under the protective provisions of GDPR. The GDPR enforces consumer protections and regulates privacy concerns for individuals and entities.

9. Amendments relating to joint accounts

Amended Rules

Part 4—Consumer data requests made by accredited persons

Part 4A Joint accounts

Division 4A.2A—Disclosure options

4A.4 Disclosure options for joint accounts

Division 4A.3— Consumer data requests that relate to joint accounts

Subdivision 4A.3.2 How consumer data requests to data holders under Part 4 that relate to joint accounts are handled

4A.12 Asking relevant account holders for approval to disclose joint account data

4A.14 Joint account data the data holder is authorised to disclose

4A.15 Consumer dashboard for joint account holders

4A.16 Notification requirements for consumer data requests on joint accounts

FDATA Response

FDATA reiterates its position at its fundamental base, as per our submission made on Joint Accounts May 2021. The inclusion of Joint Accounts within Open Banking is integral to the adoption by various consumers/businesses and the ability for solutions to expand to accommodate use-cases focused directly on complex scenarios and transaction types.

The Proposed "Opt-Out" Model:

FDATA supports the premise that *"The default is the pre-approval option. If this option applies, CDR data relating to the joint account can be disclosed in response to the request without the approval of the other account holders. Still, the other account holders can revoke the pre-approval about a particular consumer data request at any time."*

In its simplest form, the alternate solution, the 'opt-in' process, is considered confusing, difficult to implement and introduced friction that could potentially render some forms of data sharing virtual impossible by participants. Any breakdown could lead to a loss of trust in Open Banking and brand damage for both the ADRs and DHs involved in the request for data sharing.

Irrespective of the differing treatments of cash and data in the scenario of Joint Accounts, if the implementation echoed the existing operation principles that apply to joint bank accounts, introducing similar principles in Open Banking will provide further clarity to consumers/SME's and will increase consumer confidence in the regime.

Messaging and Communications:

FDATA supports the minimisation of messaging and communications to consumers. The language of communications should adopt standard sectoral messaging from their existing brands and should not be so frequent that customers ignore or delete messages before reading/comprehending/action them. Research has shown that there is a risk in consumers switching off when bombarded by requests and communications. Excessive notifications will re-introduce friction and reduce instances of use, thus further eroding adoption, usability and trust over the system.

FDATA supports the concept of Enhanced CDR Participation Communication. The ability for ADRs to obtain real-time communication on any status relating to the supply of data that affects their ability to provide a product or service to the consumer is beneficial. The failure of UK-based ADR-equivalents to receive data from the banks resulted in brand/reputational damage to the ADR primarily, with FinTechs and applications often labelled faulty or useless. This failure could vary from API call failures to banks refusing to share data. However, the consumer-facing portion of the process is the ADR terminal or screen. Suppose an ADR receives enhanced communications, such as status notifications. In that case, they will then manage the consumer expectation, thus avoiding the blame for a failure to provide a product/service. Enhanced communications create opportunities for consumer experience.

Switching between approval models:

The consumer retains the ability to switch to co-approval should they have a personal preference over access/control rights. To extend on this concept, FDATA supports a failsafe 'brake' on data sharing that would mirror the ability to place a freeze on a credit card should it be compromised. The brake is over and above the consent framework of account holders as discussed in the three Options, but would reflect the potential risk should an account

holder have doubts about data sharing with a particular ADR, or for a specific purpose, or in the case of a potential data breach or bad actor.

The CX Experience:

The impact on the consumer experience is paramount to the success of adoption for the Consumer Data Right. Removing friction and increasing convenience while enforcing the sector's commonly employed processes and practices will enhance the customer experience. Simple messaging, clarity in terms and conditions upon opening an account and educational activities will enforce the control element of Open Data Sharing and the Consumer Data Right. Our members believe the operational authority that this model most closely resembles the practices of traditional account authorisations. This model is also the standard, acceptable practice to ADIs and the existing practice for consumers. Direct Feeds from banks have operated in this manner for more than ten years now. Our members have indicated that approximately 70% of direct feeds from banks are currently joint accounts/complex accounts. If the 30-day re-authentication/re-consent framework is introduced, other account holder notification is not necessary.

Regarding the CX experience, we concur with our members' view that the design of the consumer accounts screen should list all consumer accounts during the authorisation process. However, if there are accounts that they cannot share, these accounts should not be selectable. This feature will avoid a consumer consenting to share data of which they are not eligible to share. There is a potential for those ineligible accounts to present information advising them 'these are not shareable at this time, and should they wish to share the data from these accounts, you should speak with your ADI'.

It may be helpful for ADRs to know if joint accounts have been selected for sharing within the consumer consent process. That fact can strongly influence the required CX on the ADR side and the associated messaging – i.e., "Make sure you've told all other JAHs about this" or "Does JAH2 have any other accounts that are relevant to this application?"

Differing Account Types:

FDATA acknowledges the differences between consumer accounts and business accounts. There is a risk in compromising existing authorities and security parameters in business

accounts or complex joint accounts. Signing authorities on business accounts are either any to sign (most common), all to sign, or any number of parties to sign, where the account owner selects this number at setup. The parallel nature of this model avoids the need to introduce new patterns, processes or authorities for account holders. The complexity of some joint accounts may increase the friction to ADR's in obtaining access to data; however, this is offset in reducing friction to the consumer and the Data Holders by negating the need to understand new processes or practices in authorisation and consent over traditional arrangements.

Additional Sectors:

Under the Rules Considerations, 6.2. reference to sector-wide joint account provisions is referenced. We applaud the attempt to create sector-wide joint account provisions but believe that any further delay in future planning the CDR will adversely affect the initial sector, banking. FDATA supports the need to finalise joint account rules and represents our members' views on finding a logical, common-sense approach for this sector.

Vulnerable Consumers:

Our membership acknowledges that concerns exist over the potential risk of the proposed model impacting and disadvantaging vulnerable consumers. The existing practices of Australian Banks in identifying such accounts and 'flagging' these accounts will assist in establishing an exemption framework. Should a request to share data from a flagged account be received by the bank, the entire account must be treated as 'opt-in' by default. Unless both parties elect to participate, the ability of technology to assist in protecting vulnerable or at-risk consumers will assist in limiting the risk of data-sharing. Once the bank has received a request, sending an exception code to the recipient should be a sufficient explanation for data denial, but not so specific as identifying a sensitive classification or breach of the consumer's right to privacy.

10. Amendments relating to staged implementation

Amended Rules

1.10AA Meaning of *CDR Representative* and related terms

FDATA Response

Wide-spread reform and adoption of a regime of this complexity will take time. Officially, one year in, the progress has been substantial, but we have a long way to go as a nation.

FDATA and our members appreciate the need for a phased introduction. However, the ability for Open Banking in Australia to gain traction and momentum requires not only these rules to be finalised and ratified, but each of the categories mentioned above of elements to be implemented. It is only when true clarity is presented that we will see significant participation realised.

As per our October 2020 submission, our members still believe:

FDATA considered a phased approach of compliance, implementation, development and application appropriate and necessary in principle. In regards to the specific timeline for these elements' consideration may need to be given to;

- The effects that the application process and associated compliance requirements may have on accredited participants.
- The customer experience of early adopters if the comprehensive offering is not finalised before consumer use (As seen in the UK).
- The technology demands, both in build and funding obligations of participants, may cause stress to individuals and businesses. Build times of API readiness, including the necessary Data Governance exercises, construction of dashboards, consent frameworks, and so forth, may take several months from when participants commit to their path forward. Finalisation of the rules and Legislation will remove prolonged planning and enable operational readiness of participants.

- The timeline for canvasing industry/customer feedback and finessing the roadmap should be enhanced by detailed research and international learnings. The timing of some consultation rounds, when overlayed with other pressures such as Senate Inquiry releases or Scott Farrells reports, in addition to the finalisation of legislative reform, does not allow sufficient time for responsible parties to consider the sheer volume of feedback offered by participants, industry and consumers alike.
- CDR participants are experiencing heavy demands and feedback requests on regulatory reform with current/recent requests from changes to Data Sharing and Release, CDR, Senate Inquiries, additional Sector inclusions and Digital Framework. Some FDATA's members have indicated they will not be providing individual feedback at this time due to competing obligations and a need to focus on brand readiness for entry.
- Covid is still having a substantial effect on the market. While some brands are reporting delays due to remote workforces and delaying capital raising, others are reporting that COVID has created more digital use cases that CDR will power. These changes may result in their prioritisation of core operational functionality away from the previous CDR focus. Any delay, in turn, may slow CDR participation or readiness for market participation.

The Prior Timeline for Implementation:

~~Data holder~~	~~Data sharing obligations~~	~~Start date to 31 Jan 2021~~	~~1 Feb 2021 to 28 Feb 2021~~	~~1 Mar 2021 to 30 Jun 2021~~	~~1 Jul 2021 to 31 Oct 2021~~	~~1 Nov 2021 to 31 Jan 2022~~	~~1 Feb 2022 onward~~
~~Initial data holders (NAB, CBA, ANZ, Westpac~~	~~Part 2~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~
	~~Part 3~~	~~-~~	~~-~~	~~-~~	~~-~~	~~All product phases~~	~~All product phases~~

~~branded products)~~	~~Part 4~~	~~Phase 1 Phase 2~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~
~~Any other relevant ADI and initial data holders for non-primary brands~~	~~Part 2~~	~~Phase 1~~	~~Phase 1 Phase 2~~	~~Phase 1 Phase 2~~	~~All product phases~~	~~All product phases~~	~~All product phases~~
	~~Part 3~~	~~-~~	~~-~~	~~-~~	~~-~~	~~All product phases~~	~~All product phases~~
	~~Part 4~~	~~-~~	~~-~~	~~-~~	~~Phase 1 (see sc 6.4(3))~~	~~Phase 1 Phase 2~~	~~All product phases~~
~~Accredited ADI and accredited non-ADI (reciprocal data holder)~~	~~Part 2~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~	~~All product phases~~
	~~Part 3~~	~~-~~	~~-~~	~~-~~	~~-~~	~~All product phases~~	~~All product phases~~
	~~Part 4~~	~~-~~	~~-~~	~~Phase 1 (see sc 6.4(3))~~	~~All product phases~~	~~All product phases~~	~~All product phases~~

Proposed Timeline for Implementation:

Data holder	Data sharing obligations	Start date to 31 Jan 2021	1 Feb 2021 to 28 Feb 2021	1 Mar 2021 to 30 Jun 2021	1 Jul 2021 to 31 Oct 2021	1 Nov 2021 to 31 Jan 2022	1 Feb 2022 to 31 Mar 2022	1 Apr 2022 onward
Initial data holders (NAB, CBA, ANZ, Westpac branded products)	Part 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	Phase 1 Phase 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
Any other relevant ADI and initial data holders for non-primary brands	Part 2	Phase 1	Phase 1 Phase 2	Phase 1 Phase 2	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	-	-	-	Phase 1 JAE CODE	Phase 1 Phase 2 JAE	All product phases JAE	All product phases
Accredited ADI and accredited non-ADI (reciprocal data holder)	Part 2	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases	All product phases
	Part 3	-	-	-	-	-	-	-
	Part 4	-	-	Phase 1 JAE CODE	All product phases JAE	All product phases JAE	All product phases JAE	All product phases

There is a need to finalise this sector, banking, ahead of diverting resources to other subsequent sectors. For this reason, we urge the Treasury Department to present a tight timeline to encourage compliance, participation, and a well-lit environment for encouraging innovation and Competition in this region. One approach, for example, providing guidelines that come into a specified number of months from the date of rules and standards finalisation.

11. Emerging Models for Data Sharing

Globally, there has been a fragmented movement towards Data Portability, Data Mobility and Personal Data Sharing Platforms. The Personal Sharing of Data is a revolutionary market model that enables individuals to be active, empowered participants in their future digital lives in a sustainable digital economy that they can trust.

Not dissimilar to the CDR, Personal Data Mobility enables data to flow between entities in a trusted and lawful manner that protects and respects the data protection rights of individuals, is widely recognised as critical to the growth of digital economies and the unlocking of significant public and social value. Notably, the Data Portability right in the GDPR enshrines this in law for EU citizens, creating increased trust, transparency, and control for individuals. In other jurisdictions, rights to data portability are either in place or in development.

A 2018 economic study from Ctrl-Shift and the UK Digital ministry investigating the growth opportunities from data portability points to significant productivity and efficiency opportunities and even greater opportunities for innovation, creating never before seen services for consumers that help them manage their lives better and make better, more informed decisions. In turn, this offers opportunities for sustainable business growth for organisations and efficient and productive societies.

Without enabling infrastructure, the introduction of data portability opens up new risks for consumers, organisations and governments alike. Only by working together can these stakeholders create a market that will enable us to grasp these benefits.

Global trends towards adopting decentralised personal data platforms see wide-spread adoption across multiple sectors, such as finance, health, utilities, accounting, and travel. Large tech firms are actively investing in a platform that exceeds the CDR slated sectors and will enable consumers to access and retain and control their personal data. This is in addition to the wide-spread digital wallets that brands such as Apple, Google and Facebook are developing.

This industry and global standards move towards decentralisation of consumer personal/sensitive data plus the woven in impact of SSI (Self Sovereign Identity -W3C) will stage the on-flow effect and the ability for true economy-wide data-sharing via digital data wallets that will also impact sectors and Finance will be targeted for a host of cyber/security and privacy reasons.

Models such as these are being extended to SME's and complex entities, introducing the benefits of Artificial Intelligence and Data Minimisation, plus an embedded consent stack equal to, or in some cases, higher than the stipulated CDR infosec Framework.

A recent privacy and cybersecurity bulletin showcased an ambitious new bill that aims to protect Canadians' privacy whilst promoting data-driven innovation. "The Canadian Government Proposes Significant Changes to Privacy Law: Key Features include New Requirements, Orders, Penalties and a Private Right of Action". This is considered to be related to the march of GDPR enabled technologies outside of Europe.

12. Ongoing Monitoring and Health of the API Network

Several international jurisdictions and cross-over sectors are exploring/adopting technology solutions to monitor and appraise the health of API ecosystems. In New Zealand, the MBIE has run several assessments to evaluate the external monitoring of key API's.

The critical requirements were:

- Ability to get notification of issues in production and test environments
- Support for SOAP and REST APIs
- Ability to monitor from regional and international locations
- Ability to have multiple users under one account
- Reporting on the API performance – Including volumes, data quality, availability, response times, etc., all benchmarked against predefined thresholds.

Case study of APImetrics

New Zealand's MBIE evaluated several cloud services for API monitoring and found APImetrics the best fit for their requirements based on:

- APImetrics responsiveness to questions and requests,
- Comprehensive documentation,
- Tailoring of their delivery to ensure that the capabilities of the product were well understood and
- Monitoring was set up to provide maximum effectiveness.

A digital solution for a digital problem. A comparative solution would augment the ACCC Compliance and Risk teams in monitoring and maintaining the health of the API ecosystem, not just for Open Banking, but for any subsequent sector that is introduced. These works would complement the compliance and enforcement works of the ACCC. Several local organisations have developed such tools and would benefit from Federal Investment to assist in providing independent market oversight.

API call failures and issues relating to the inconsistency of design, payload and non-functional parameters plagued the United Kingdom ecosystem, depleting confidence by participants and consumers alike. By employing a technological solution to augment the work of the

compliance and risk teams, targeted focus on breeches, deficits, and infringements can occur. Also, the platform's output could be easily translated and visualised as per the ACCC's objective to make key performance statistics publicly available.

As per our previous responses:

FDATA supports and encourages a CDR that closely aligns to traditional practices as familiar to accredited participants, but most importantly, as familiar to the consumer. Keeping the consumer, choice, convenience, and confidence at the centre of CDR development, we commend the government and the market's continued efforts to deliver a fit-for-purpose, secure and consumer-led solution.

The ability for consumers to choose their operating practices, coupled with the instant nature of digital banking, will enforce the consumers choice to share any or all of their data for any purpose that they believe will enrich their experience or enhance their life. In addition to suitably informed account holders, the real-time nature of data-sharing will increase the adoption of open banking and enable growth in product/service offerings for consumers and businesses alike.

The CDR is a pivotal opportunity to promote digital transformation, enhancing Australia's economy, and we highly encourage the CDR to be finalised with haste to achieve these momentous objectives.

Please do not hesitate to contact me should you have any questions or request further input.

Kind regards,

Jamie Leach
Financial Data and Technology Association | Australia/New Zealand
Mobile: +61 413 075 671
Email: Jamie.leach@fdata.global | Web: fdata.global | Twitter: @FDATAglobal

Acknowledgements:

Authors: Jamie Leach,

Editor: Jamie Leach, Richard Prior

Design: FDATA ANZ

© 2021 Financial Data and Technology Association (Australia/New Zealand)

All rights reserved. Reproduction in whole or in parts is permitted, providing attribution is given to Financial Data and Technology Association (Australia/New Zealand) (FDATA ANZ) and provided that any such reproduction, in whole or in parts, is not sold or incorporated in works that are sold. Written permission must be sought from Financial Data and Technology Association (Australia/New Zealand) if any such reproduction would adapt or modify the original content.

Published May 2021.

© Cover photo: Adobe Stock 2020

Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of May 2021. Nevertheless, Financial Data and Technology Association (Australia/New Zealand) cannot accept responsibility for the consequences of its use for other purposes or in other contexts. Data Portability analysis, recommendations and best practice guidance reflect FDATA's opinion. They should not be taken to represent the views of those quoted, interviewed or surveyed unless expressed in writing. FDATA assumes no liability to any third party for the information contained herein, its interpretation or for any reliance of any third party. This document should not be construed as a recommendation, endorsement, opinion or approval of any kind. This Guidance has been produced for information and should not be relied on for legal purposes. Legal advice should always be sought before acting based on the information provided.