CDR RULES EXPANSION AMENDMENTS - SUBMISSION

Jamie Leach – OCT 2020

FDATA A&NZ www.fdata.global

Contents

1. Foreword

Open Finance, 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 to be able to share this data with businesses of their choice digitally. It is part of a broader suite of Open Data initiatives, aimed at empowering 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 around the world are assessing, adopting or implementing 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, Open Finance and Data Portability to unlock economic potential and to improve the financial wellbeing of customers. 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 and regulatory reform moving forward.

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

FDATA wishes to commend the efforts of the Australian Government in the continuing consultation with Industry and the release of the latest version of rules that will form Australia's Consumer Data Right. Various groups have supported these works intending to design and develop a fit-for-purpose solution.

To arrive at the most suitable solution for Australia, working with such groups of expertise and enthusiasm, along with a comprehensive suite of participants, is essential. Globally, FDATA has provided comprehensive research and advisory to Federal Regulators and their Government's alike. The design of the following sections provides targeted feedback in response to this final round of consultation. FDATA would be pleased to provide additional feedback or Global research to the Australian Government if required to progress the formalisation of CDR rules.

Australia has proven to be a world leader in legislative reform and its unique approach to adopting a Consumer Data Right. FDATA commends your attempts to learn from other jurisdictions and consider all options before deciding on the right path forward.

2. Executive Summary

FDATA is pleased to offer this submission in response to the request for feedback on the latest version (version 2) of the Rules. In light of the call for succinct (short-form) and direct feedback to a series of questions, please accept this shortened submission. 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 the 42 questions considering the:

- **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 in respect of the management of consumer consents to collect and use CDR data, joint bank accounts, and accounts that have additional cardholders.

Within this submission, FDATA would also like to expand on issues such as Digital Identity, Consumer Trust, Consumer Consent Management and the Monitoring and Health of the API Network.

3. Timeline for proposed rules to take effect and overview of key proposed rules

Consultation questions

1. We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

FDATA Response

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 stresses 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 between six and twenty-four months from the time that 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 of 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. Several of 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 affecting many potential ADH's and ADR's, impeding their potential development and compliance responses. This may result in their prioritisation of core operational functionality away from previous CDR focus. Any delay, in turn, may slow CDR participation or readiness for market participation.

Also, this paper has raised several items that were deemed inappropriate for the initial phase of CDR rules due to their complexities and the ensuing challenges of implementation.

These items include:

- Applying CDR to businesses,
- The provisions for joint accounts and variable consent,
- The potential for additional tiered accreditation models, and;
- The provisions for affiliates and trusted advisers

While FDATA concurs with the rationale for omitting these elements from the initial rules discussions, any delay in their design finalisation and their inclusion in the final rules may once again negatively impact the consumer experience of the regime. Besides, any lag may have a lasting and negative impact of CDR participation going forth.

Given the imminent findings of the recent Senate Select Committee in combination with the pending Scott Farrell review report, FDATA believes there are some overlapping points of interest and concerns that should be considered in parallel when formalising the CDR rules.

We invite the ACCC to review the Senate Committees recommendations and those of the Scott Farrell report in conjunction with this round of Industry feedback. This exercise will impact the prioritisation of development and compliance, thus affecting the formal timeline further.

FDATA supports the continuation of a phased approach to the implementation of rules in principle. We advise the ACCC that clarity needs to be conveyed to both market participants and the broader data portability ecosystem at the earliest possible timeframe to maximise the accreditation rate of accredited entities and to raise their confidence in and readiness to go live within this regime.

4. Increasing the number and types of businesses that can participate in the CDR

Consultation questions

2. *The proposed rules include three discrete kinds of restricted accreditation (i.e. separate affiliate, data enclave or limited data restrictions). We welcome views on this approach and whether it would provide sufficient flexibility for participants. In responding to this question, you may wish to consider whether, for example, restricted accreditation should instead be based on a level of accreditation that permits people to do a range of authorised activities.*
3. *We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation.*

FDATA Response

In principle, FDATA supports the attempt of the ACCC to remove barriers for participation and to 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, whilst removing potential barriers to entry. 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.

FDATA supports the inclusion of these three discrete levels of restricted accreditation. The introduction mirrors the findings of the Senate Issues Paper in the introduction of tiered accreditation, promoting broader access without raising the level of risk.

There is a falsehood that by narrowing the focus of rules, inherent risks can be potentially removed or contained. However, these actions may also reduce the viability of participant's operating model, or their ability to expand their offering in time.

One example may be Fintech A that launches its brand with a single targeted service offering. I.e. to provide Income confirmation for serviceability exercises. To complete this service, a simple application of CDR is required, and by applying as a limited data participant, they may only deal with a single form of CDR data. The risks are considered to be lower, and thus, they satisfy this lower entry point.

One issue with this approach is should that entity wish to expand their offering, or enter into a commercial arrangement to provide an additional service; the initially limited restriction is no longer adequate. There is a risk that the initial accreditation may limit the growth of the organisation or their ability to pivot. The exercise of upgrading their accreditation will require resources and funds and may prove a barrier to expansion.

However, an even greater issue exists with the consideration that any identifiable data, even those considered to be of lower risk, if accessed by a nefarious party, or breeched, mishandled, or incorrectly distributed, can still yield significant impact to the consumer. There is a danger of complacency in labelling a limited, restricted accreditation as representing a lower risk in the ecosystem, than a party with full unrestricted accreditation.

FDATA agrees that:

- Base-level customer data is an example of a limited data set that may be available to a lower tier participant.
- Specific types of data required to perform a simple of single-action may be suitable for lower-tier participation. These may include serviceability calculations or proof of income.
- A lower-tier participant must meet the minimum technical, insurance, information security, compliance requirements, and so forth. In the case of a smaller, boutique entity, these requirements are crucial to protect against the potential for data breaches and cyber targeting. The specific nature of the data they may receive/share does not reduce these genuine dangers.

As per the feedback that FDATA and our members have contributed throughout the various consultation rounds, we support the efforts to reduce barriers to entry and to tailor the participation definitions to align to relevant use-cases and industry nuances.

We caution against unnecessary complexity and the genuine potential to confuse not only participants but the end-user of the right, the consumer. While the consumer will not be expected to digest the nuances of the scheme, they are taught to seek the badge of compliance. The difference between participant's accreditation may represent a deterrent for consumer use if considered overtly complex.

Transparency will lead to confidence which will, in turn, promote trust in the Consumer Data Right.

Additional points for consideration:

- The consideration for external accreditation, and
- The recognition of like-frameworks in the issuing of accreditation, are concepts that FDATA support.

A number of our members have raised the concept of compliance as a service, and the provision of an independent organisation to test, monitor and advise on the 'health' of the technical environments. These options may also boost the security and ability for the lower tiers of accreditation to maintain a sufficiently high level of compliance while focusing on targeted or specific actions relating to CDR data.

3.1. Restricted level: limited data restriction

Consultation questions

4. *What are your views on the low to medium classification of risk for the data set out in Table 1?*
5. *Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?*
6. *Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?*

FDATA Response

While FDATA supports Table 1 in principle, we repeat an element of our response from the previous question.

There is also the consideration that any identifiable data, even those considered to be of lower risk if accessed by a nefarious party, or breeched, mishandled, or incorrectly distributed, can still yield significant impact to the consumer. There is a danger of complacency in labelling a limited, restricted accreditation as representing a lower risk in the ecosystem, than a party with full unrestricted accreditation.

That risk level applies when accredited participants are operating adequately within the expected parameters. However, even the lower risk data may represent a significant inconvenience, financial loss, or identity theft to a consumer.

All data classified within the CDR and all participants operating within the CDR must achieve and maintain a minimum acceptable level of security and procedure irrespective or role of classification.

Transparency will lead to confidence which will, in turn, promote trust in the Consumer Data Right.

Additional points for consideration:

- The consideration for external accreditation, and
- The recognition of like-frameworks in the issuing of accreditation, are concepts that FDATA support.

A number of our members have raised the concept of compliance as a service, and the provision of an independent organisation to test, monitor and advise on the 'health' of the technical environments. These options may also boost the security and ability for the lower tiers of accreditation to maintain a sufficiently high level of compliance while focusing on targeted or specific actions relating to CDR data.

3.2. Restricted level: data enclave restriction

Consultation questions

7. *Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.*
8. *Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?*

9. *Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?*

FDATA Response

We support the inclusion of the Data Enclave Model as a limited tier of accreditation with the CDR in the context of a principle leveraging the information security capability of the enclave provider.

We agree that the provided example in the consultation document, of Polis, is a suitable example of the data enclave arrangement, and may provide the model for the entry that some service providers and fintech seek.

Irrespective of the distribution of roles within the enclave relationship, all data classified within the CDR and all participants operating within the CDR must achieve and maintain a minimum acceptable level of security and procedure irrespective or the role of classification.

3.3. Restricted level: affiliate restriction

Consultation questions

10. *Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.*

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

12. *Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?*

13. *The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.*

FDATA Response

The proposed inclusion of the Sponsor/Affiliate model may well increase participation within the CDR. By granting clarity over the technical/compliance/dispute resolution/information security requirements within the Schedules, this option should reduce the number of barriers to entry for participants.

In regards to marketplace participants, concerns over attestation requirements have been raised where comparative frameworks of equal of greater compliance than Schedule 2 already exists. Two scenarios have been raised as possible additions to the rules or alternatives that deserve consideration:

- The potential to create a separate CAP participant category of a Trusted Provider – The trusted provider is an entity that provides a product or service directly to a customer/business. Where a customer directs their data to be shared with this provider, an ADR may share CDR Data within the regime, without fear of sharing consumer data with unaccredited third parties. The Trusted Provider would have a relationship with the ADR and may already be pursuant to complimentary contractual arrangements to provide products or services within a controlled environment. This option would differ from both the Trusted Advisor category, and the Sponsor/Affiliate model as self-declaration from the Trusted Provider would replace the need for Attestation from the sponsor.
- A provision for each marketplace participant to apply for accreditation with leniency to be granted upon presentation of a Nationally Recognised Framework accreditation, i.e. SSAM, existing DSP participation, or alternate comparative frameworks. The advantage to this approach would be each individual participant would apply for, maintain and operate as an accredited data recipient in their own right, without presenting onerous barriers to entry. By approaching existing framework recognition, this classification of ADR could be publicly displayed on the CDR register and their compliance obligations monitored in the alignment of other ADR participants.

5. Expanding how accredited persons can work together

4.1. Combined Accredited Person arrangements

Consultation questions

14. We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.

FDATA Response

We support the rule proposed by the ACCC that the principal in a combined accredited person (CAP) arrangement should retain all responsibility for the customer-facing delivery, as they have the relationship with the consumer and the consumer has engaged their brand to provide the data.

That being said, both the restricted accredited data recipient and the unrestricted accredited data recipient must retain accountability for meeting their respective CDR obligations at all times, with precise requirements between each role within the relationship. This compliance will exceed the contractual commitments between the two entities necessary to satisfy their co-dependent relationship.

4.2. Transfer of CDR data between accredited persons

Consultation questions

15. Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data?

a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate?

b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the consumer and, if so, to what extent?

FDATA Response

FDATA does not support the creation of new rules specifically for data held by an ADR. We recommend that ADR's seeking to share a consumer's data with another ADR should be treated as data holders and be subject to the same requirements as an ADH. There should be one single minimum acceptable standard, rather than differing rules for each participant. This approach of simplicity echoes best practice in both Data Governance and Data Sharing scenarios.

It is unclear why there is a need to have one set of rules for transferring a consumer's data from an ADH to an ADR and a different set of rules for transferring a consumer's data from an ADR to a second ADR.

By definition, a participant that shares data is a Data Holder and a participant that receives data is a Data Recipient. This concept must remain fluid as multiple value chains between participants, service provision, and fintechs enter the framework. The logical treatment of rules would be to apply a single overarching treatment of data to all classification of participants, irrespective of their position upstream or downstream. This would require the transfer of regulation for data holders to any ADR seeking to transfer data to another ADR.

The consultation paper notes that an ADR would not be prohibited from charging a fee for the transfer of CDR rate to another ADR. It is essential to distinguish between the charging of a fee for sharing 'raw' CDR data, opposed to charging of a fee for sharing 'enhanced', 'derived', 'insights-driven', or 'value-added' data. CDR should not preclude entities from providing additional services and creating commercial revenue streams for their services if adding value to the data in the stream.

FDATA does not support the proposition of a participant charging to share raw data at any stage in the ecosystem. This phenomenon is considered different from an event where an entity offers additional value in their processing and sharing of consumer data. Current commercial protocols allow for the provision of a service, and value-add of data be purchased. The CDR framework should not contravene this. FDATA does, however, believe that all actions involving a consumer's data must meet the protections of the Privacy Act and should remain transparent to the consumer. In line with the GDPR introduction, each action performed by an entity on consumer data should require visibility to or initiated consent from the consumer.

In principle, FDATA supports the issuing of multiple consents by a consumer concurrently for a variety of data sharing applications, providing that consent if

expressly received for each action, and the customer must be informed of their full rights before providing their consent.

One area that has received attention within the financial services industry is the practice of recommendations and third-party referral without KYC provisions and restricting the ability to profit from such recommendations. This issue has affected investments, loans and mortgages, stock trading, financial planning, etc. Any rules permitting third-party recommendations must consider the adequacy and effectiveness of disclosure of commercial arrangements before consent can be sought and the provision for satisfying the consumer comprehension of the practices.

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, materially enhanced, and value-added data, are no longer treated as CDR 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 has been altered by a service provision at the request of the consumer 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 over privacy concerns for individuals and entities.

6. Greater flexibility for consumers to share their CDR data

Consultation questions

16. *To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession's regulatory regime in your response.*

17. *Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?*

18. *Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding 'raw' CDR data as disclosed by the data holder)?*

19. *What transparency requirements should apply to disclosures of CDR data insights? For example, should ADRs be required to provide the option for consumers to view insights via their dashboard, or should consumers be able to elect to view an insight before they consent for it to be disclosed to a non-accredited person?*

FDATA Response

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

As existing practices currently stand, the directive of a consumer 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 would work appropriately to protect the consumer and to create a monitored environment.

The issue remains when a consumer requests the sharing of their data with an unlisted class of professional, a business, or for a rare use-case. Currently permitted, the introduction of CDR will require that current practices cease or materially change.

There appear to be two issues at hand;

- Firstly, should a consumer be able to direct a CDR participant to transfer data to a non-accredited data recipient?
- Secondly, should rules be made to allow an ADR to transfer data to a non-accredited data recipient?

Transfer of data to non-accredited data recipients

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.

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 may event in reduced participation from consumers.

The presentation of an initiated consumer consent should be accepted. 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.

FDATA supports the concept of an alternative approach of establishing a tiered accreditation category for professionals and trusted advisors that meet specific minimum requirements concerning compliance with privacy and information security standards.

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 apply to become an accredited data recipient for this tier.

In adopting this approach, consideration should 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. Schedule 2 of the rules may need to involve the minimum acceptable privacy and security requirements for this classification tier.

Transfer of data by an ADR

In echoing our earlier responses, it is unclear why the ACCC is seeking one set of rules for data sharing by an ADH to an ADR, and another set for data shared by an ADR.

These new rules proposition that the ADR holds data that a consumer wishes to transfer to another party. However the CDR regulatory framework already has a category of CDR participant that holds data – that of a data holder, not specifically an ADR.

It is unclear why the ACCC would seek to have one set of rules for transferring a consumer's data from one class of CDR participant (a data holder). As to why they would introduce a different set of rules for transferring a consumer's data from another class of CDR participant (an ADR).

An alternate approach is to make it clear in the rules that an ADR that holds consumer data is re-designated as a data holder, and that a consumer can direct an ADR that holds consumer data to share that data with another ADR.

This would still require an additional discussion as to the right's of a consumer to request their data be shared with an entity/individual that does not satisfy the definition of an accredited recipient, be it an ADR or a Trusted Advisor.

7. Extending the CDR to more consumers

6.2. Specific rules for business partnerships

Consultation questions

20.We are seeking feedback on the proposal for enabling business consumers (both non-individuals and business partnerships) to share CDR data.

21.In particular, we welcome comment on the proposal to require a data holder to provide a single dashboard to business consumers which can be accessed by any nominated representative to manage CDR data sharing arrangements.

22.Are there other implementation issues the ACCC should be aware of in relation to the proposed rules for CDR data sharing by non-individuals? CDR rules expansion amendments 36

23.We welcome comment on the proposed approach to require data holders to treat business partnerships in line with the approach for dealing with business consumers? Do you foresee any technical or other implementation challenges with taking this approach for business partnerships that the ACCC should take into account?

24. Should additional protections be introduced for personal information relating to business partners who are individuals?

25.Are there other aspects of the rules that may require consequential changes as a result of the enablement of business consumers? For example, are the internal dispute resolution requirements appropriate for business consumers?

FDATA Response

FDATA supports the ACCC's proposal to extend the CDR to classification to entities other than individuals. This may include the proposed classification of businesses, corporate entities, partnerships, trusts or joint accounts. This expansion is in keeping with the timeline set out by the ACCC in December 2018.

We support the proposal for a single dashboard, thus enabling multiple parties or authorised representative to transact on a specific business account. Dashboards allow not just visibility over the data, but also maintenance and compliance over access and

authorisations of who can transact on the account, held within a single dashboard. The ability of visibility over a complex and multi-faceted functionality is vital.

We commend the proposed expansion outlined in Phase 3 allow for product and transactional data for additional users, including:

- Business Finance,
- Lines of Credit
- Overdrafts, and
- Asset Finance

We acknowledge that additional preparations will need to be made by the ADI's and ADH's to allows the sharing of these newly introduced datasets; however, the existing timeline allows sufficient notice, over two years, for development preparation and compliance activities to be met.

Concerning the treatment of a partnership from a legal perspective, we consider the nature of a business partnership similar to that of a joint account. As with any banking product, authorisation to access, review and transact would be agreed by the parties and recorded within the bank. We see no reason to deviate from this principle of aligning the consent protocols and dashboard access to the wishes of the users.

The broadening of the scope to permit anyone with account privileges is in alignment to that of accepted banking and financial systems provisions. This inclusion continues to elevate the consumer experience and enhance understanding and trust.

FDATA does not support the requirement for additional protections for personal information relating to business partners who are individuals. Under the CDR, in alignment with the Privacy Act, existing protections surrounding the access and transaction of financial data are sufficient. Should an individual business partner not wish to allow their business's data to be shared via the CDR, this matter should be addressed internally, between the partners. This concept of account authority should not be a matter for the CDR as long as the ADR receives the full and conforming account request.

6.3. Secondary users

Consultation questions

26. We welcome feedback on the proposals for enabling authorised users to share CDR data.

27. Should persons beyond those with the ability to make transactions on an account be considered a person with 'account privileges' in the banking sector?

28. How should secondary users rules operate in a joint account context?

29. As well as having the ability to withdraw a 'secondary user instruction', should account holders be able to have granular control and withdraw sharing with specific accredited persons that have been initiated by a secondary user?

FDATA Response

FDATA supports the position of the ACCC in not proposing that every individual who is authorised to transact on behalf of a non-individual consumer should automatically be authorised to share CDR data. Irrespective of businesses granting different levels of authority over access, visibility and the authority to share a business's CDR data, consideration must be given to the feasibility of levels of authority and the technical requirements of building this capacity.

Intrinsically, provisions enabling a business to access a dashboard/portal to nominate authorised individuals, make data sharing requests and revoke data sharing requests will encourage a self-service environment. This dashboard/portal will allow businesses to align account privileges to that of tradition operations and to monitor and maintain their CDR provisions.

A proposal to allow businesses to define the characteristics of someone who can transact on the account will represent an additional transferal of the business's CDR account oversight to the CDR participants. It may be considered appropriate that non-individuals such as business customers have a responsibility to keep their authorisations current and to maintain correct security procedures in maintaining their dashboard/portal. Provisions must be made then if a CDR participant acts contrary to the authorisations of the businesses, i.e. allows a non-authorised individual to request data sharing.

As per FDATA position on previous questions, we do not support the concept of the ACCC developing specific rules, or additional rules for secondary users. Any rules developed within the CDR legislative framework may conflict with rules and accepted practices already adopted with a sector. These scenarios will apply to each sectoral introduction of CDR.

In keeping with the movement of data matching the movement of funds, any rules that exist for account access and transaction within the banking sector or subsequent sectors could apply to CDR provisions. There is no need to create new prescriptive rules to police the behaviour of consumers and businesses.

In traditional banking, the ability for an account holder to nominate multiple account signatories may come down to two factors.

Firstly, the structural and regulatory nature of some accounts and some business services may require multiple signatories. There may be a requirement for one, or more than one authorised party to move funds, open an account, authorise over a specific limit to be transferred, etc.

The second factor involves the personal preferences of the account holders and their trust parameters within the relationship or organisation. Any underlying access and requirements for specific behaviours must be mirrored in accessing and transferring data, as it does for a request for account transaction.

8. Facilitating improved consumer experiences

7.1. Sharing CDR data on joint accounts

Consultation questions

30. We are seeking feedback on our proposals relating to sharing CDR data on joint accounts, including:

a. the proposed approach to require data holders to allow consumers to set their preferences (a disclosure option) as part of the authorisation process

b. the proposed approach of allowing 'joint account holder B' to withdraw an approval at any time

c. the expansion of the rules to include joint accounts held by more than two individuals

d. the proposal that joint account holder B does not have to 'approve' amendments to authorisations

e. the proposed approach that the rules do not require (but do not prohibit) the history of disclosure option selections being displayed to consumers as part of the joint account management service or data holder consumer dashboard.

31. Do the benefits of requiring data holders to display on-disclosures to 'joint account holder B' outweigh the costs?

FDATA Response

As per our previous responses:

In keeping with the movement of data matching the movement of funds, any rules that exist for account access and transaction within the banking sector or subsequent sectors could apply to CDR provisions. There is no need to create new prescriptive rules to police the behaviour of consumers and businesses.

In traditional banking, the ability for an account holder to nominate multiple account signatories may come down to two factors. Firstly, the structural and regulatory nature of some accounts and some business services may require multiple signatories and

may dictate the requirement for one, or more than one authorised party to move funds, open an account, authorise over a specific limit to be transferred, etc. The second factor involves the personal preferences of the account holders and their trust parameters within the relationship or organisation. Any underlying access and requirements for specific behaviours must be mirrored in accessing and transferring data, as it does for a request for account transaction. These rules could be expanded to cover multiple party accounts. This could apply to accounts of more than two individuals assuming that appropriate instruction and authorisations are nominated at the commencement of establishing their profile.

In the case of additional sector inclusion, the provisions for account authorisations may not be as developed as that of the banking sector. It is common practice for joint account holders within the Energy or Telecommunication sector allowing either party to access and transact on a single account, as long as they are nominated and recorded on the file. The introduction of prescriptive rules may negate potential risks that may arise from a party wishing to withdraw the authorisation; however, the addition of prescriptive and exhaustive rules will lead to an overly complicated solution.

FDATA strongly encourages the public awareness and education program introduces the concept of consumer control over their data interactions and appraises the consumer/business with their rights and responsibilities in utilising the regime.

7.2. Amending consents

Consultation questions

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

33. We are seeking feedback on the proposed rules about the way accredited persons are able to invite consumers to amend their consents. Should a consumer be able to amend consent for direct marketing or research in the same way as amending consent for use of data in the provision of goods and services?

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

FDATA Response

FDATA supports the proposed range of changes to the rules relating to consents, including changes to allow:

- an accredited person to invite consumers to amend a consent
- an accredited person to offer multiple consent management options
- separate consents for the collection of CDR data and consents for the use of CDR data.

And for amending consents to involve multiple attributes, including:

- adding or removing uses
- adding or removing data types
- adding or removing accounts
- amending durations
- adding or removing data holders

Visibility of authorisations and allowing consumers to control consent dashboards will play a significant role in establishing trust in the regime. By increasing clarity and offering visibility, confidence and acceptance of data sharing will grow. Multiple reports and insights published by the Senate Inquiry Paper have raised the need to establish a method for consumers to keep track of, manager, or grant their consent for data sharing. As with each of the existing rules and provisions, any new inclusions or changes must not only serve the accredited participants but raise the understanding and acceptance of consumers.

One challenge remains around the need for initial consent, requesting additional consents and the timeframes around the lifecycle of consumers consent to share data. In deeming that each activity may attribute a suitable format for consumer consent, such as the length of time the consent remains current, clarity over these decisions is integral in establishing consumer trust in the regime. Any perceived obstacle, such as the prospect of establishing/re-establishing consents and authorisations, may result in barriers to consumer participation.

7.3. Separate consents approach

Consultation questions

35. We are seeking feedback on the proposed approach of separating the consent to collect from the consent to use CDR data (rather than combining consent to collect and use).

36. Should accredited persons be able to offer disclosure consents only after an original consent to collect and use is in place (with the effect that combining a use and collection consent with a disclosure consent would be prohibited)? See also the consultation questions in section 7.2 above.

FDATA Response

We support the consumer's ability to offer any consent they deem necessary to request that data sharing be provisioned in the pursuit of a service or product. The integral consideration in this response is the clarity and appropriateness of consent frameworks, not the specific act itself. Suppose a service provider offers to collect a dataset about a consumer. Once collected the provider analyses the data, or utilises the data in the provision of a different product or service to the consumer, the consumer should be able to offer a single consent to both elements in unison. In keeping with the principles of the GDPR; expressed and informed consent for each activity may be collected in unison, providing they offer sufficient clarity over the extent of activity.

7.4. A 'point in time' redundancy approach and the impact of withdrawing authorisation

Consultation questions

37. We are seeking feedback on the 'point in time' redundancy approach.

38. We are seeking feedback on the proposed approach where a consumer withdrawing their authorisation for a data holder to disclose their CDR data results in removal of the ADR's consent to collect only.

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

FDATA Response

FDATA concurs that the proposed outcomes relating to the withdrawal of authorisation and the 'point in time' redundancy approach will create confusion for consumers and do not support consistent messaging about how deletion and de-identification works under the CDR regime.

Under the current rules, there may be different outcomes depending on the action taken by a consumer to withdraw authorisation. For example:

- if a consumer is sharing CDR data with an accredited person from one data holder, withdrawing the authorisation results in the consumer's consent to collect and use expiring and the accredited person is subsequently required to comply with redundancy requirements under privacy safeguard 12.
- if a consumer is sharing CDR data with an accredited person from multiple data holders, withdrawing an authorisation with a particular data holder results in the consent to collect and use expiring to the extent, it was associated with that particular data holder only. This means the accredited person is required to comply with redundancy requirements under privacy safeguard 12 concerning CDR data collected from that particular data holder only.
- If a joint account approval is withdrawn by joint account holder B, the data holder must stop disclosing CDR data on the joint account. However, no communication is made to the accredited person, so redundancy obligations under privacy safeguard 12 are not relevant, and the accredited person may continue to use the CDR data already collected on the joint account.

We support the ACCC proposal to move towards the 'point in time' redundancy approach within the proposed rules to minimise the impact to CDR participants. The focus of the CDR must be on consumer controlling their data, both throw visibility, but also in access to products and services. The consumer should retain the right to amend current consent.

7.5. Improving consumer experience in data holder dashboards

Consultation questions

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

FDATA Response

FDATA supports the proposal for data holders to present consumers with the name of the accredited person during the authorisation process, within the consumer dashboard. We support the requirement to display additional information to consumers, as much information on the data shared, authorisations, CDR participants, etc.

We caution the ACCC in adopting this principle without the comprehensive development of dashboard specifics, i.e. optional metadata. Any delay in clarity is prohibitive of development timelines for CDR participants and may present a barrier to operational readiness for CDR participants.

9. Clarifying rule amendments

8.1. Application of product reference data rules to 'white labelled' products

Consultation questions

41. We are seeking feedback on whether the proposed amendments place the obligation on the party best placed to meet the obligation.

42. Are there any technical or other implementation issues of which the ACCC should be aware?

FDATA Response

FDATA supports the inclusion of provisions for white labelled products and practices within the CDR. While the white labeller is often an ADI, this is not always the case. The practice of launching a product/service and distributing 'rights' for distribution amongst other entities is common within the financial sector and throughout data practices. In this example, the white labeller may be an ADR, i.e. a Fintech or Neo-Bank.

The proposed rule amendments specifically target the white label instance of ADI to ADI. As this practice may occur between any potential accreditation level, solutions must work for each possible scenario.

To provide clarity and certainty rule amendments should focus on;

(a) how the product data request rules apply where both the white labeller and the brand owner are data holders (e.g. where both are ADIs); and

(b) the information that must be provided concerning white label products such as credit cards, where there is no requirement to provide a product disclosure statement.

(c) how the product data request rules may apply when the white labeller and the brand owner may be accredited participants other than ADI's.

Acknowledging that the customer relationship is with the data holder who receives the product data requests and enters into the contractual relationship with the consumer will continue to provide clarity and continuity of the customer experience.

It is unclear of the benefit of the alternate data holder responding to a consumer product data request. The consumer may not be familiar with the brand of the other

white label brand, and allowing that entity to respond to the product data request, without the expressed consent of the consumer will be confusing and unexpected.

It is clear as to the benefit in allowing the two entities to reach an agreement on who will meet the obligation in practice while retaining clarity on which data holder must meet the regulatory obligations.

Where deficits exist in white-label products disclosure statements, such as credit cards, there is a need for further clarity of responsibilities of CDR participants. The types of data, the nature of the arrangement, the source of the product data are examples of items requiring further consideration if details must be presented within consent frameworks and on dashboards. Compliance with newly introduced requirements will take lead time to design, develop and launch. FDATA supports the earliest possible finalisation of rules and releasing of elements to support the continued application of participants and go-live products/services within the CDR.

Additional Response

There are four additional areas that FDATA would like to consider:

- Digital Identity,
- Consumer Trust,
- Consumer Consent Management, and
- Ongoing Monitoring and Health of the API Network

Digital Identity

A coordinated and standardised approach to identity is critical to the future of the Consumer Data Right. As of October 2020, there is no coordination amongst the significant range of actors tackling the digital identity issue across comparative jurisdictions, such as Australia, the United States and the United Kingdom.

When multiple actors work on competing services globally, it is left to the market to determine the identity framework. If Australia were to end up with multiple competing customer identity systems operating on different standards, this would inherently limit the customer's ability to direct their data to the service providers of their choice, irrespective of the sector or Industry. Not every service provider will select the identity solution framework best suited to enable the end customer to access and share identity claims across the ecosystem. The need for interoperability between Australia

and its partners is critical for trade. However, within the country, the need for a mutually agreed digital identity framework is critical for cross-sectoral productivity and ultimately, the customer's benefit.

Failing to unite puts the onus on the customer to manage more than one type of identity solution. It is tantamount to requiring the customer to have multiple adaptors for every different identity plug and socket on the market. The customer would end up having to manage a variety of identity keys, rendering the Consumer Data Right virtually useless.

When designing the Consumer Data Right, it is essential to consider: the customer must be part of the trust framework. Putting the customer back at the centre of the identity framework should be part of the mission of bringing Consumer Data Right to Australia.

Critical work is needed to develop identity standards and a more robust consent management model. Without establishing interoperable standards, the integrity of any identity management scheme is compromised. For an equanimous digital identity utility to exist, there are core principles that must be followed:

- Implement open standards instead of proprietary competitive systems
- Promote open data principles alongside privacy and security
- Support a range of customer journeys
- Allow competition in the provision of services built to common standards, rather than having competing standards

Consumer Trust

To establish Consumer Trust across any sector, it is essential to conduct consumer testing of any CDR data information, including fact sheets and education campaign materials, directly with consumers before release to ensure the success of any new initiatives. Communication across the community about policy reforms that impact consumers are most effective when they are broad and inclusive. This includes ensuring that vulnerable consumers are aware of their rights and options and understand the implications of their decisions.

An effective program of education and information materials is likely to be best developed when co-designed with a range of organisations that are experienced in engaging various segments of the community and with consumers themselves. The

Australian Government may benefit from the establishment of an *Open Banking Communications Steering Group* that is diverse and representative of the various parts of the Australian community when designing the public information and education campaign on CDR. This group would continue the work at each stage of the reform, as they prepare for launch, including telecommunications, utilities and future stages.

Established training programs and research and engagement with other reform processes projects have demonstrated the need for consumer education initiatives to be:

- Tailored to specific information needs of consumers, based on the research of what end-users want and need to know
- Designed in collaboration with a diverse group of end-users
- Varied in communication styles and channels to reach different parts of the community
- Collaborative in the distribution of materials across the community sector to ensure vulnerable members of the community are reached
- Consistently resourced and supported through time – effective education and information campaigns are not designed as one-offs.
- Consumer behaviour change requires consistent and ongoing engagement to raise awareness.

Consumer Consent Management

Feedback to FDATA has raised the concept of a single consumer dashboard/portal within which to view all current or past consent actions in one location.

Details of the dashboard may include;

- The type of consent
- The holder of the consent
- The duration of the consent
- The details of the consent granted
- The time remaining on the consent

With clarity, simplicity and understanding being at the cornerstone to introducing a Consumer Data Right, enabling the monitoring and maintaining of their consents in a single location would be to the benefit of the consumer. Once a single consent is

visible within the dashboard, the details of the ADH/ADR would be easily located, and this would, in turn, assist with managing the requests to amend or cancel a consent if requested by the consumer.

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
- Reporting on the API performance
- Ability to monitor from regional and international locations
- Ability to have multiple users under one account

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 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. A digital solution for a digital problem.

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 contraventions can occur. Also, the output of the platform could be easily translated and visualised as per the ACCC's objective to make key performance statistics publicly available.

The team at FDATA support Australia's continuing endeavour to design, develop and deliver a fit-for-purpose Consumer Data Right.

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

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

Kind regards,

Jamie Leach

Financial Data and Technology Association | Australia/New Zealand

Mobile: [redacted]

Email: [redacted] | Web: fdata.global | Twitter: @FDATAglobal

Acknowledgements:

Authors: Jamie Leach, Gavin Littlejohn

Editor: Jamie Leach, Richard Prior

Design: FDATA ANZ

Published October 2020.