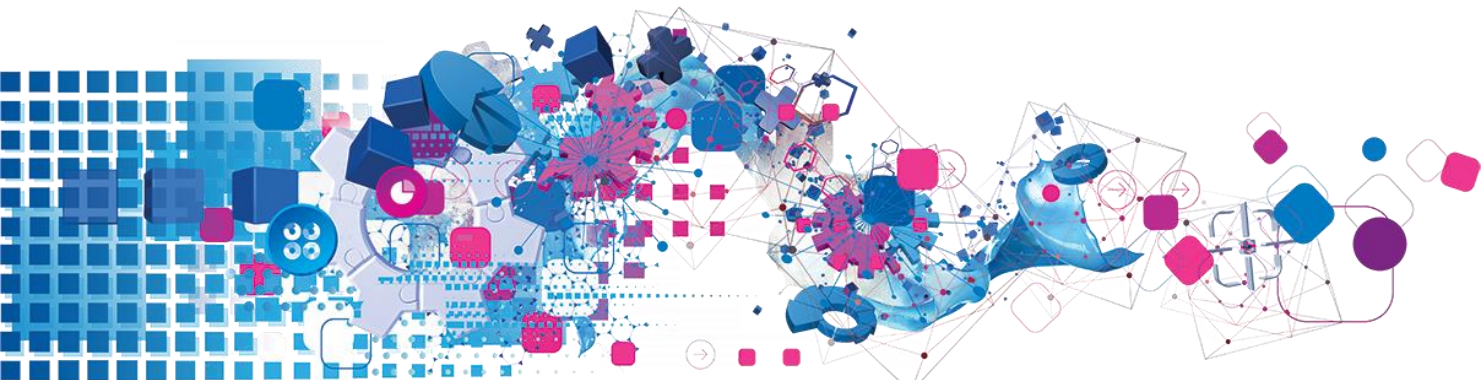
Experian Australia Pty Ltd
Level 6, 549 St Kilda Road
Melbourne VIC 3004
ABN 95 082 474

# Consumer Data Right

## Consultation on how to best facilitate participation of third-party service providers

Experian Australia response
3 February 2020



# Contents

# 1. Executive summary

The Australian Competition and Consumer Commission (ACCC) introduced the foundational rules for the Consumer Data Right (CDR) regime in the lock-down version of the rules, released in September 2019 (rules). Consistent with the position in the Rules Outline, the rules do not provide for the use of third-party service providers who collect or facilitate the collection of CDR data on behalf of accredited persons (Intermediaries). The ACCC noted that it intended to develop rules to accommodate business models that use Intermediaries in a subsequent version of the rules.

Experian welcomes the opportunity to provide feedback to the ACCC through the consultation paper around the opportunities, benefits and considerations of third-party service providers within the CDR regime.

Many of the G8 countries where Experian operates are launching Open Data initiatives, including Australia, the United Kingdom (UK), and the United States (US). Experian supports the adoption of an Open Data regime in Australia and encourages the Australian banking and financial services industry to become an early adopter of CDR. These initiatives will develop over time, and consumers will be at the centre of deciding how their customer account information with any given financial entities can be accessed, transferred, used and shared to their benefit.

We support the ACCC's approach both in taking a consumer centric approach, and in building on the Open Banking framework by developing a better understanding of the technology ecosystems that drive innovative digital solutions today and their capabilities. To this end, the feedback provided below, is intended to consider how the principles of accreditation can be best built on while allowing for third party service providers (Intermediaries) to participate and drive innovation to ensure that the potential for unintended consequences to consumers, impacting the value of this regime, is minimised.

Experian recognises that accredited Intermediaries will play a key role in enabling wider access to CDR data along with increasing consumer adoption of CDR through the digitisation of existing processes and the creation of compelling new product and service propositions.

We support the extension of the rules to provide for the use of third-party service providers who collect or facilitate the collection of CDR data on behalf of accredited persons (Intermediaries) however there will need to be careful consideration given to both the accreditation that the Intermediary would need to go through along with consideration for an Intermediary making CDR data available to non-accredited parties.

We believe that an accredited Intermediary should undergo a similar accreditation process to that of an accredited recipient in the current CDR rules while careful consideration would need to be given to Consent, Privacy, Data Security, Liability and Contractual agreements for any non-accredited party looking to receive CDR data from an Intermediary.

# 2. The role of Intermediaries

Experian supports the extension of the CDR rules to provide for the use of third-party service providers who collect or facilitate the collection of CDR data on behalf of accredited persons (Intermediaries). We see a number of benefits to the CDR ecosystem and consumers as a consequence:

- Provides access to data and value add services that ultimately benefit the consumer.
- Reduces cost, effort and complexity for Data Recipients in gathering data on behalf of the consumer in a compliant and sustained manner. This will allow Data Recipients to spend more resource on consumer services and allow smaller organisations to participate.
- Facilitates unified access to CDR data and promotes scalable and trustworthy connections.
- Supports technical simplicity and secure access to compliant and regulated environments.
- Lowers overheads as a result of centralised services / gateways that are maintained by the Intermediary.
- Provides access to a wider pool of innovation and competition as well as access to specific areas of expertise that may be accessed rather than replicated.
- Allows for faster launching of new products and services for consumers.

We also recognise and take seriously the need for the protection of data. A data ecosystem of any kind is made more complex by the number of participants and data handoffs. The threats that arise in relation to Intermediaries receiving, holding, using and disclosing data is well documented and mirrors those of Data Recipients. However, the allowance of accredited Intermediaries will likely provide for greater scalability and trust within the CDR environment.

Data chain of custody, mobility and portability are important considerations and appropriate standards must be applied across all participants. When a Data Recipient provides a product / service to a consumer there will likely be more than one participant (Intermediary, Outsource Provider, Data Holder) providing constituent parts of what the customer is provided. For example:

- ID services.
- Data storage and computing (i.e. cloud).
- Data access (APIs).
- Data aggregation.
- Consumer dashboards.
- Data enrichment services (summary, analytics, de-identified, value add).

Varying levels of accreditation at a participant level may be beneficial to the overall capability of the CDR ecosystem. For example, current provisions allow for a Data Recipient to use an Outsourced Service Provider to provide storage and computing (cloud) services. Other variants with restricted access such as to de-identified data only may have merit. The primary consideration is building and maintaining the trust of the consumer. To this end, where Primary CDR Data is exchanged, stored or processed then the same standards that apply to Data Recipients should apply to all participants that have a corresponding access to CDR data.

# 3. Experian as a responsible data custodian

For more than 125 years, Experian has helped people and businesses to prosper and communities to flourish. Experian operates in 55 countries globally, with consumer credit reporting bureaus operating in 22 countries.

Experian considers itself a steward of the information it collects, maintains and utilises. Our responsibility is to ensure the security of the information in our care and to maintain the privacy of consumers through appropriate, responsible use. We provide services based on information about millions of individuals and businesses. This information is coupled with an extensive range of industry accredited solutions, and data governance capability, so we sit at the forefront of the relationship between brands and the consumer.

All data use is guided by our Global Information Values. These Information Values form the foundation for Experian's belief that information use must benefit both businesses and individuals while meeting consumers' privacy expectations.

Information policies, built on our values, more specifically define how information may be used. The policies vary to meet the legal requirements and consumer expectations in the area in which the information product or service is being used. Underlying these policies is Experian's commitment to provide consumers notice, choice and education about the use of personal information. Educated consumers are better equipped to be effective, successful participants in a world that increasingly relies on the exchange of information to efficiently deliver the products and services consumers demand.

Today, our business clients' needs and consumers' expectations are constantly changing, and technology is constantly evolving. Our approach to privacy, rooted in these Global Information Values, enables Experian to respond to those constantly changing needs and expectations and provides the flexibility to implement new processes and policies to resolve information issues in this dynamic environment.

Experian has been leading global studies and thought leadership at the intersection of business, technology and consumer experience. We were at the forefront of shaping the Open Data framework in the UK and are localising solutions across the globe developed on these principles and technology best practices.

# 4. Experian Australia service models

Experian provides Open Banking and Open Data Services in a number of countries globally. It is our intention to provide similar services within Australia and therefore within the CDR framework. As we have seen in other markets there is continual change and evolution of use cases within markets that enable the sharing of data. Similarly, the number and type of participants and their services has evolved. For the purpose of this submission a high-level explanation of our initial service delivery models are as follows.

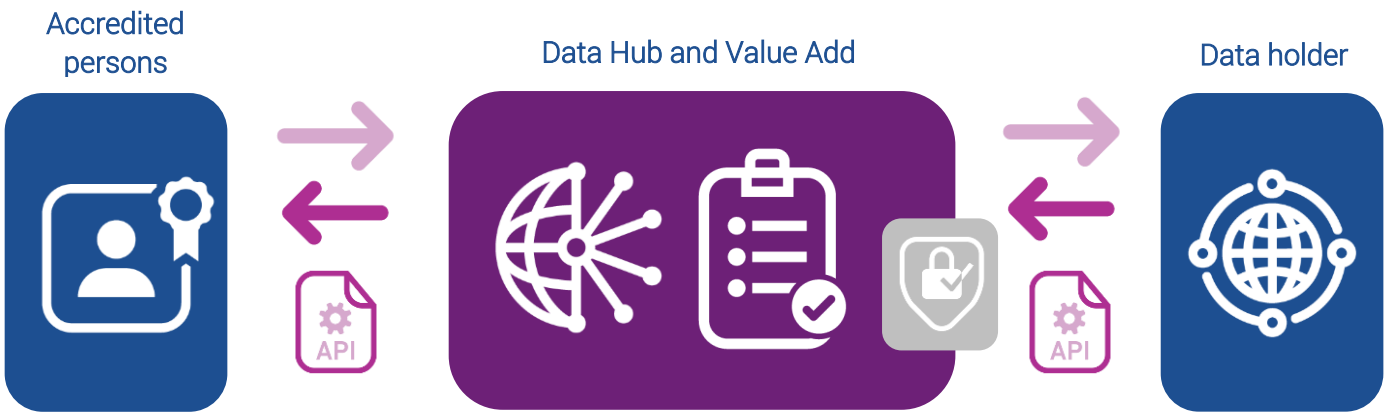
## 4.1 Data Hub with Value Add, B2B – (Data Sourcing and Value Add)

The provision of a centralised Open Data service platform that has the ability to receive requests for both CDR Data and Value Add Services via API. CDR data would be sourced from one or more Data Holders. Collected CDR data would be made available to the Accredited Person as well as the option to consume derived value add data.

This model would be consumed as a B2B offering and not directly to the consumer. The capture of consumer consent(s) would be performed upstream of the Experian service (by the Accredited Persons / Data Recipient). The Experian service would however record consent and validate before accessing data held by Data Holders. Similarly, the final delivery / presentation of data to the consumer would be performed by the Accredited Persons / Data Recipient.

Within this model Experian would also offer services that add value to the CDR data retrieved on behalf of Accredited Persons and ultimately the consumer. One such example would be to analyse de-identified bank account transaction data and return summarised data indicating income, expense and affordability metrics. We see such data as being valuable in streamlining and more accurately complying with responsible lending regulation and improving customer service. Other use cases such as powering downstream financial management applications would also be facilitated by such services.

Figure 1.0 – Data Hub and Value Add

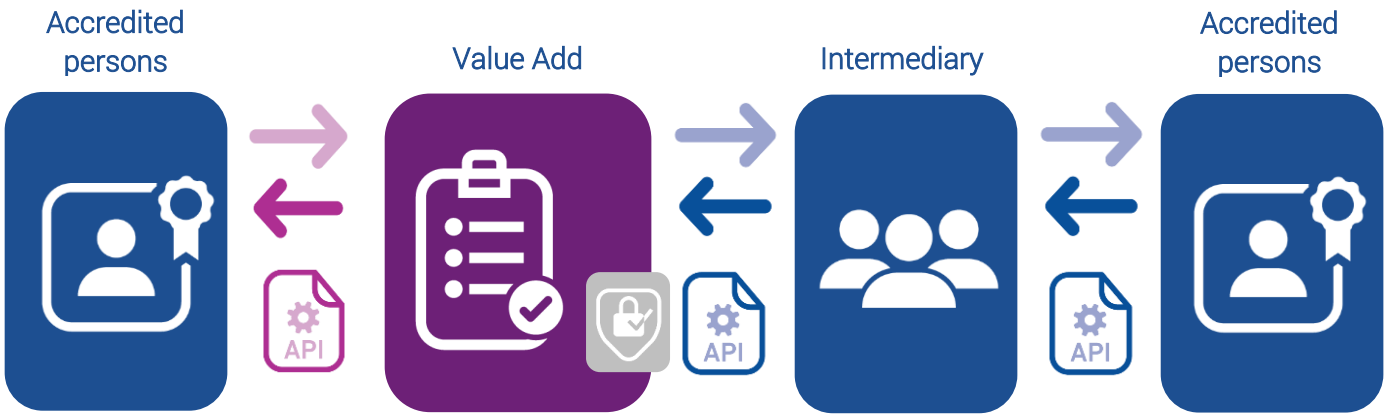



## 4.2 Value Add, B2B

As per the above model but only providing value add services on top of CDR data already sourced by Accredited Persons / Data Recipients. Similarly, this service could be consumed by an accredited Intermediary that is in turn sourcing data for an Accredited Person. Under this model the CDR Data would be sourced outside of Experian services however Experian

services would be used to add value to that pre-sourced data. For example, an Accredited Person may send in de-identified CDR data and receive value added data in response.

Figure 2.0 – Value Add – B2B




## 4.3 CDR data handling

It is envisaged that data would be held by Experian for the purpose of Audit and Dispute Resolution. Any data held would be in compliance with the CDR rules and any Privacy Regulations. Similarly, data de-identification and deletion would be in line with accreditation requirements.

As a leading global information services company, Experian is well qualified in ensuring data is secure and handled appropriately. Being a trustworthy and responsible custodian of data is central to our operations. We also recognise that there may be more than one Intermediary used in the provision of services to Accredited Persons / Data Recipients and ultimately consumers for a given use case. In relation to the services offered by Experian we may, as use cases develop, consume services from other Intermediaries as part of fulfilling a request from an Accredited Person / Data Recipient. For example, in servicing a given request (post consent) Experian may call both CDR APIs of Data Holders directly as well as APIs exposed by other accredited Intermediaries.

We suggest that the ACCC consider the handling and use of CDR data as it pertains to providing services that are underpinned by Machine Learning and Artificial Intelligence (AI). Commonly, such models are trained using de-identified data both for initial development and ongoing.

# 5. Experian responses to consultation questions: Intermediaries

**Q1. If you intend to be an Intermediary in the CDR regime, or intend to use an Intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an Intermediary. Do you intend (or intend to use an Intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that Intermediaries can bring to the CDR regime and for consumers?**

As per "the role of Intermediaries" section above we see benefit in extending the CDR rules to cater for Intermediaries. Additionally, as described in the "Experian service models" above we are likely to use Intermediaries.

Just as the CDR framework is based on re-usable APIs that promote standardisation and efficiency, the use of Intermediaries has the potential to provide similar efficiencies on a wider scale for the regime and ultimately consumers. An Intermediary can provide technical expertise, focused solutions, infrastructure and managed services that may not be part of the core business model or operationally feasible to Accredited Persons business process. Similarly, Intermediaries may utilise services of other Intermediaries in providing an end solution.

Accredited data recipients gain efficiency to bring new products to market for their customers. Intermediary provided products and services that manage and maintain the technical overhead of data access, aggregation, storage and innovation can offer more commercially viable solutions for new entrants as well as existing service providers. The inclusion of Intermediaries fosters continued innovation in specialised areas that can be made on offer to consumers through accredited persons.

A range of considerations are important:

- The presentation and management of consumer consent. Finding a balance between informing customers on how their data will be used and who will access it, and not confusing them to the point of not wanting to utilise CDR. Similarly, gaining and maintaining consumer trust.
- Regulating and enforcing standards across a potentially wider group of participants in the regime.
- Contractual liability complications as a result of additional entities.

**Q2. How should Intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.**

In our view there should be provision for both an accreditation model and an outsourcing model. In each case appropriate protections would need to be in place covering data security, data privacy, governance, liability and insurance and contracting requirements.

Specifically, that Intermediaries should require accreditation. Where Primary CDR Data is exchanged, stored or processed then the same accreditation standards should apply to Intermediaries as they do to Accredited Persons / Data Recipients since the risks/threats are the same.

The existing allowance within the CDR rules that permit disclosure of CDR data by an accredited person to an outsourced service provider, provided certain conditions are met should remain. This will facilitate the inclusion within the regime of

non-accredited service providers (e.g. cloud platform providers) but with the regulated coverage of the accredited person who contracts with them and acting as the accredited participant. In the same vain, an accredited Intermediary would also be permitted to contract with an outsource service provider.

Consideration:

- Review the UK model that includes both accredited participants e.g. Account Information Service Providers – (AISP) and non-accredited participants (Technical Service Providers (TSP), although the latter requiring registration.
- Consumer confidence will likely be higher where participants, i.e. those who will have access to a consumer's data are formally accredited.

**Q3. What obligations should apply to Intermediaries? For example, you may wish to provide comment on:**

a. **If Intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which Intermediaries should be responsible for complying with the existing rules or data standards;**

It is imperative for the success of CDR that consumer confidence is gained and maintained. Both data security and customer control over access and use of their data are paramount in achieving this.

Where Primary CDR Data is exchanged, stored or processed then the same accreditation standards should apply to Intermediaries as they do to Accredited Persons / Data Recipients since the risks/threats are the same. This encompasses data access methods and security standards (i.e. Data61 standards, Schedule 2 – security of CDR data held by accredited data recipients) as well as rules around consent. For this reason, the same criteria that applies to the current 'unrestricted' level should apply.

Additional considerations:

- Within the criteria for accreditation, consideration also needs to be given to the consent process to enable the use of de-identified data in the supply of services to consumers as well as the rules for the de-identification and deletion of data. For example, where data is used in the learning process of Machine Learning models the learnings are not deleted even though the input data supplied to them is deleted. Noting that data informs/trains the model and cannot be re-identified. Such models are becoming more and more prevalent and can provide significant benefit to consumers and organisations. The supply of such services may be by Intermediaries who receive data disclosed to them by Data Recipients or from Data Holders in the process of fulfilling a request by a Data Recipient.
- Accreditation should allow for participants to provide additional data such as derived data. In effect this would supplement rather than disrupt the regulated Data61 data standards. For example, an accredited Intermediary would be permitted to expose their own APIs to facilitate value add services.
- To ensure fairness across participants, confidence by consumers, and consistency within the regime intermediaries must be responsible for compliance to rules and standards. Additionally, the ongoing oversight of such adherence is vital in maintaining consumer confidence.

b. If Intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and Intermediaries;

As per Q2 above our view is that Intermediaries should be regulated under an accreditation model.

c. If the obligations should differ depending on the nature of the service being provided by the Intermediary.

The obligations would not differ based on the service being provided by the Intermediary to the Accredited Person / Data Recipient.

Q4. How should the use of Intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.

The topic of consent should consider how to inform a consumer that they are being provided a product or service of value that requires their data and an ability to determine where their data is being sent and how it will be used. Consent information should seek to balance informing the customer whilst not confusing them. In other markets Experian has observed that there has been an increasing demand from consumers in wanting control over not only consent but what happens to their data.

Considerations:

- The use of standard wording across the industry would help minimise confusion especially as customers move from service to service. For example, where a consumer utilises CDR data for the purpose of applying for credit at more than one organisation the consent wording should aim to be the same.
- How to reference multiple parties that may be involved in the supply of the service for which consent is being requested. This could include several parties including Data Recipients, Outsource Service Providers, and Intermediaries. An overly legal approach that aims to protect the industry participants will work against providing an acceptable user experience.
- Where participants that are accredited apply, this will likely help garner trust from consumers and increased participation in CDR.
- Informing the customer of the use of Intermediaries (and other participants) should be easily accessible and not for example buried within terms and conditions.
- Having easy access to an accreditation register within user journeys, at the time of giving consent, should be included.
- The ongoing policing of conformance to standards including consent is vital. From the work we have done in other markets we have seen that customer trust and adoption is fragile.
- Standards of accreditation regardless of the provider of the service will help build trust with consumers. Consumers will be less concerned with the details of the provider, or one provider versus another if they are accredited and by implication meet the standard.
- Consent dashboards could also include notifications that detail the associated participants in the chain of custody of consumer data for a given consent. This would provide full transparency as well as audit for the consumer.
- Consider notification alignment with Australian Privacy Principles – APP5.

**Q5. How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.**

It is imperative for the success of CDR that consumer confidence is gained and maintained. Both data security and customer control over access and use of their data are paramount in achieving this.

Where Primary CDR Data is exchanged, stored or processed then the same accreditation standards should apply as they do to Data Recipients since the risks/threats are the same. This encompasses data access methods and security standards (i.e. Data61 standards, Schedule 2 – security of CDR data held by accredited data recipients) as well as rules around consent and data deletion/de-identification.

Disclosure between accredited persons should be permitted via consumer consent. By implication, if the persons are accredited, then they will have met the required accreditation criteria.

Consent revocation or expiry should apply to each custodian in the chain of custody of the data for the given consent. So, for any consented use case, data would be either be deleted or de-identified at each point of storage (e.g. Data Recipient, Intermediary, Outsource Service Provider). It would be sensible to channel notifications of such deletions back to the Data Recipient inclusive of audit and reporting details.

Notifications should also extend to customers, so they are aware that their consent instructions have been carried out. Additionally, consideration should be given to the ease at which a consumer can see all consents and status of their interaction with the CDR regime inclusive of who has accessed their data. Essentially, the disclosure of data between accredited persons for the benefit of the consumer should be permitted. However, unless consumers are confident that their data is secure and that they are not taken advantage of by allowing disclosure consent won't be given in the first place.

**Q6. Should the creation of rules for Intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited Intermediary is used?**

As per Q3a. where Primary CDR Data is exchanged, stored or processed then the same accreditation standards should apply to Intermediaries as they do to Accredited Persons / Data Recipients since the risks/threats are the same. This encompasses data access methods and security standards (i.e. Data61 standards, Schedule 2 – security of CDR data held by accredited data recipients) as well as rules around consent. For this reason, the same criteria that applies to the current 'unrestricted' level should apply.

# 6. Experian responses to consultation permitting CDR data to be disclosed to non-accredited third parties

Q7. If the ACCC amends the rules to allow disclosure from accredited persons to nonaccredited third parties and you intend to:

a. Receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers;

Experian intends to seek accreditation within the CDR framework. However, as stated in Q1, Experian will be offering a multitude of solutions to facilitate data access, data aggregation and data enrichment and act as a technical service platform between participants within the CDR framework to facilitate the transmission and delivery of value-added products and services based on CDR data. These services may fall under the outsourced service provider where contractual agreements defining data management may be the presiding legal governance.

b. Be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.

Experian sees an opportunity to play a role in supporting the delivery of services to the consumer via non-accredited third parties. For example, by providing derived and additive value data we envisage that consumers will have access to a wider range of products and services and be able to consume them in a more streamlined manner compared to today's environment; we also recognise that some of these services may ultimately be delivered via non-accredited third parties. Not only is there potential to make data more available and more usable for both customers and organisations but also to streamline and enhance customer experience. Facilitating the responsible inclusion of non-accredited third parties that may otherwise be excluded from the CDR regime will likely only benefit the consumer.

Q8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

Experian agrees with the ACCC that the sharing of CDR with non-accredited certain parties will be important to the expansion of the regime. Consider services like financial planners, attorneys, financial counsellors, accountants and various other financial service providers who offer services that assist consumers in managing their finances and planning for life changes where financial information is required.

These entities would unlikely be capable of meeting accreditation requirements nor would be the sole handlers of data in the CDR framework. For example, Licensing for purposes of providing financial advice incorporate many consumer safeguards. A similar structure may be warranted as the intention is that the receiver of the data is a fit person and has some sense of liability if the data they receive is mishandled.

Another example may be a technology service provider that specialises in very specific data solutions in the data lifecycle that would have limited access to or exposure risk in handling the data but provides a critical service to the accredited

party. Contractual agreements and similar conditions to be met as defined in outsourced service provider may provide operating guidelines and liability thresholds and penalties under contract law.

A prudent approach may be to consider if the non-accredited person were receiving

- Complete sets of mandatory data
- A combination of mandatory and voluntary data, or
- If they are only receiving partial data that is derived, summarised, or in some way transformed from the original CDR data.

It should be considered that there is another form/level of accreditations, licensing or certification around the access and use of CDR data. In addition, responsible use of this data by an unaccredited third party should also be covered under the Privacy Act.

### Q9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

Consumer data today has certain protections under the Privacy Act and have been expanded under the Consumer Data Rights rules. Experian believes that in all cases where consumer data is transmitted, stored, transformed, derived, and displayed, the highest level of consumer protection and privacy should be applied. The success of the CDR regime depends on consumer trust in the ecosystem. Where CDR data is transmitted through the CDR regime, there are clear guidelines set out in the Privacy Safeguards.

Both the accredited person and the non-accredited third party assumes responsibility for consumer data when it is in possession. The level of liability and regulatory oversite would depend on type of data (mandatory vs voluntary, unrestricted vs summarised / derived data) and ultimate services provided through the use of that data, examples being a financial instrument product, financial advisory services, or product comparison services.

### Q10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

Transparency should be aligned to the topic of consent and should consider how to inform a consumer that they are being provided a product or service of value that requires their data and an ability to determine where their data is being sent and how it will be used. Consent information should seek to balance informing the customer whilst not confusing them.

Please see response to Q4 for additional details.

It should be considered that access to notices around terms and conditions of the services provided by the non-accredited third party as appropriate for the consumer, information around the consumer's rights to the handling of their data and any other regulations that may apply to the data as being handled by the non-accredited third party be made available.

# 7. Conclusion

As a firm believer in the power of customer data, and the benefit that this should bring to the consumers who are the rightful owners of this information, Experian is committed to providing products and services to assist individuals and corporations (as custodians of this information) to realise the opportunities that effective exchange of data holds.

Experian is supportive of changes to the CDR rules to enable the inclusion of Intermediaries as well as non-accredited third parties since this will likely provide for a wider range of products and services, greater innovation, and competition and therefore increase benefits for consumers. Further, we regard the responsibilities of Intermediaries as they pertain to primary CDR data to be equivalent to Accredited Data Recipients and therefore support a similar level of accreditation.

Our observation in completing this submission is that there are a number of key areas for consideration in any revision to the CDR rules and associated operation of the environment as a consequence of allowing for Intermediaries and non-accredited third-parties:

.

- Consent management and its impact on gaining and maintaining consumer confidence.
- Responsible access to CDR data and the ongoing compliance of this access given and increased range of participants.
- Management of the complexity in data management as a result of widening the chain of custody of CDR data.
- Ensuring appropriate consumer protection and liability frameworks.

As a wider organisation we have been an active participant in the establishment of Open Banking in other markets. We look forward to participating in further rounds of consultation for CDR and supporting the success of regime.