EXPOSURE DRAFT EXPLANATORY MATERIALS

Issued by authority of the Minister for Superannuation, Financial Services and the Digital Economy

Competition and Consumer Act 2010

Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021

Section 56BA of the *Competition and Consumer Act 2010* (the Act) provides that the Minister may, by legislative instrument, make consumer data rules for designated sectors in accordance with Division 2 of Part IVD of the Act.

The Consumer Data Right (CDR) is an economy-wide regime which gives consumers access to and control over their data, and the ability to obtain products and services from accredited persons using CDR data.

The *Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021* (the Rules) amends the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules) to give effect to the Government's intention to: facilitate greater participation in the CDR regime by participants and consumers; provide greater control and choice to consumers in sharing their data; promote innovation of CDR offerings including intermediary services; and enable services to be more effectively and efficiently provided to customers.

The Rules:

- empower consumers to share their CDR data with certain classes of 'trusted adviser' (such as their account, lawyer, tax practitioner, BAS agent, licensed financial adviser or planner, financial counsellor or residential mortgage broker), or to share limited 'insights' obtained from CDR data
- support new pathways for participation in the CDR by allowing an accredited person to sponsor other parties to become accredited or allow their agents to participate in the system
- amend the settings that apply to data sharing for joint accounts to enhance consumer experience and convenience by enabling consent to sharing CDR data about joint accounts to be provided in a manner that aligns more closely with the existing ability of joint account holders to view and share joint account data.

Schedule 1 to the Rules implements the sponsored accreditation model which reduces the cost of accreditation by altering certain obligations to establish information security capability as part of the accreditation process and ongoing accreditation obligations.

Schedule 2 to the Rules establishes the CDR representative model which allows eligible participants to access CDR and use data without the need for accreditation in circumstances where they offer CDR-related services to consumers as a representative of an ADR.

Schedule 2 to the Rules also enables an accredited person to rely on unaccredited outsourced service providers to collect CDR data and thereby reduce the cost of building and operating application programming interfaces that connect to data holders.

Schedule 3 to the Rules allows consumers to nominate persons as ***trusted advisers*** to whom an accredited person may disclose the consumer's data outside the CDR regime. The classes of trusted advisers are professions that are sufficiently regulated to ensure a strong level of consumer protection is maintained.

Schedule 3 to the Rules also introduces the concept of a CDR insight, which allows CDR consumers to consent to their data being shared outside the CDR regime for prescribed purposes that are considered low risk and that are designed to limit the data shared to only what is necessary for the consumer to receive a service.

Schedule 4 to the Rules provides for joint accounts to be in scope for data sharing under the CDR by default (a 'pre-approval' setting). Sharing of data on a joint account can only occur with the explicit consent of a joint account holder and the Rules set out the mechanisms by which a joint account holder may adjust or change the pre-approval option. Any joint account holder will be able to withdraw a consent for data sharing on an account at any time.

Schedule 5 to the Rules provides for staged implementation of rules relating to joint accounts and direct to consumer obligations in the banking sector.

Schedule 6 to the Rules sets out transitional matters.

Details of the Rules are set out in Attachment A

The Rules are a legislative instrument for the purposes of the *Legislation Act 2003*.

The commencement of the Rules is to be confirmed. The Schedules provide further information on commencement where a delayed commencement is proposed.

ATTACHMENT A

Details of the *Competition and Consumer (Consumer Data Right) Amendment (No. 1) Rules 2021*

Section 1 – Name of the Rules

This section provides that the name of the Rules is the *Competition and Consumer (Consumer Data Right) Amendment (No. 1) Rules 2021* (the Rules).

Section 2 – Commencement

The commencement of the Rules is to be confirmed.

Section 3 – Authority

The Rules are made under the *Competition and Consumer Act 2010* (the Act).

Section 4 – Schedule(s)

This section provides that each instrument that is specified in the Schedules to this instrument will be amended or repealed as set out in the applicable items in the Schedules, and any other item in the Schedules to this instrument has effect according to its terms.

Increasing pathways to participation

The Rules implement new data access models to encourage greater uptake of the CDR by both participants and consumers while maintaining trust in the security and integrity of the CDR system.

The consumer benefits of the CDR are intrinsically linked to establishing a vibrant ecosystem of accredited data recipients (ADRs) and other participants. Stakeholders have indicated that current barriers to enter the CDR (including the cost of accreditation) are deterring many businesses from participating. Addressing this concern has the potential to increase the range of ADRs making products and services available to consumers via the CDR and expand the overall benefits of the CDR regime.

The proposed models seek to lower barriers to participation by creating new pathways by which participants can engage with the CDR regime:

- requiring self-assessment and attestation to establish information security capability rather than an independent third-party assurance report for persons with an unrestricted accredited sponsor (the sponsored level of accreditation);
- removing the requirement to become accredited for participants that are subject to an arrangement with an unrestricted person that is liable for them (CDR representative model); and
- enabling participants to rely on unaccredited third parties to collect CDR data and therefore reduce the cost of building and managing connections to data holders (collecting outsourced service providers (OSPs)).

The models provide flexibility for CDR participants to manage risk and liability through commercial arrangements. The models are also designed to maintain trust and confidence in the CDR because any use or disclosure of CDR data by sponsored affiliates, CDR representatives or OSPs is subject to the same requirements and protections that apply to unrestricted accredited persons.

The intention is that the Rules for the three models will commence as soon as they can be technically supported by the Register and Accreditation Platform. Treasury is working closely with the Australian Competition and Consumer Commission (ACCC) to determine the appropriate implementation timeframes for each model, taking into account required build impacts for the Register and changes to accreditation processes. Commencement dates for these models will be determined having regard to this analysis and consultation submissions, and stakeholders will be updated accordingly.

Schedule 1 - Sponsored accreditation

Background

The sponsored level of accreditation is for persons with or who intend to have an arrangement with an unrestricted accredited person who is willing to act as their sponsor in the CDR regime.

A person accredited to the sponsored level and in a sponsorship arrangement would be known as an affiliate of its sponsor.

Persons who wish to participate in the CDR system as affiliates must have both sponsored accreditation and a sponsorship arrangement in place before they can access CDR data.

An affiliate is an accredited person and is required to fulfil the obligations of an accredited person in the CDR regime. This includes (but is not limited to) compliance with dispute resolution obligations, the privacy safeguards and consent rules. To the extent civil penalties attach to those obligations, they may also apply to an affiliate.

The accreditation criteria for sponsored accreditation will be the same as for unrestricted accreditation. However, an affiliate will not be required to provide an assurance report to establish that it meets the information security criterion once accredited. Instead, an affiliate will be required to provide a self-assessment and attestation to the Data Recipient Accreditor (DRA). The evidence that is provided at the accreditation application stage in order for the DRA to be satisfied that the accreditation criteria are met is currently outlined in the Accreditation Guidelines, published by the ACCC. If the rules for sponsored accreditation are made, the relevant self-assessment and attestation forms and updated accreditation guidelines will need to be approved and published by the DRA.

The key differences between sponsored accreditation and unrestricted accreditation (as set out in more detail below) are:

Issue	Unrestricted	Sponsored
What is the evidence needed to establish information security when applying for accreditation and on an ongoing basis?	Independent third-party assurance report (for further information, including on partial acceptance of industry standards, see the 'Supplementary Accreditation Guidelines' published by the DRA).	Self-assessment and attestation against accredited person's ability to comply with Schedule 2.
When can the accredited person be an active participant in the CDR system?	Upon accreditation.	Must be accredited and in a sponsorship arrangement with an unrestricted accredited person. May not access CDR data or provide goods or services unless it has a sponsorship arrangement in place.
Who can the accredited person collect CDR data from?	Data holders and other accredited data recipients.	Cannot collect data directly from data holders. May request its sponsor to collect data from a data holder and pass that data to the affiliate. May also collect data from another accredited person who is not their sponsor, relying on the AP disclosure rules (see rule 1.10A).
Can the accredited person use outsourced service providers (OSPs)?	May use OSPs to collect data under a CDR outsourcing arrangement. May disclose data to OSPs under a CDR outsourcing arrangement.	May not enter into a CDR outsourcing arrangement to collect CDR data. May request its sponsor to use the sponsor's OSP to collect CDR data. May disclose data to OSPs under a CDR outsourcing arrangement.
Can the accredited person have CDR representatives?	Yes.	No.

Becoming accredited at the sponsored level

Schedule 1 amends rule 5.2 which allows persons to apply to the DRA for sponsored accreditation. The application must be in a form approved by the DRA and specify that the person seeks sponsored accreditation.

Applicants for sponsored accreditation must meet the same accreditation criteria as persons with unrestricted accreditation (see rule 5.5). This includes complying with the obligations of an accredited person in rule 5.12 (as amended by Schedule 1).

An affiliate's accreditation will lapse if it is not in a sponsorship arrangement for four months (see rule 5.1B(5)).

The sponsor and affiliate relationship

Schedule 1 inserts new rule 1.10D which defines the new terms 'sponsored accreditation', 'sponsor', and 'affiliate' and establishes the minimum required terms in a sponsorship arrangement.

A sponsorship arrangement must be a written contract between a person with unrestricted accreditation and another person. The other person may have sponsored accreditation at the time they enter into a sponsorship arrangement, however, they may apply for and be granted sponsored accreditation before having a sponsorship arrangement in place.

The sponsorship arrangement must provide for the sponsor to disclose CDR data to its affiliate, in response to a consumer data request.

The arrangement must also require the affiliate to provide the sponsor with the appropriate information and access to its operations as needed for the sponsor to fulfil its obligations as a sponsor.

The parties may agree for the sponsor to make consumer data requests, or to use or disclose CDR data, at the request of the affiliate. In this case, the sponsor would be acting on its own behalf, and be liable for its actions, when it makes consumer data requests, uses or discloses the data. This can be compared to outsourcing arrangements, where an ADR that uses OSPs for collection is ultimately liable for them.

Similarly, the affiliate would be acting on its own behalf when it uses or discloses CDR data to provide goods and services.

Collecting and using data

Rule 5.1B as inserted by Schedule 1 restricts persons with sponsored accreditation from making consumer data requests unless they are a party to a sponsorship arrangement.

Similarly, an affiliate cannot make a consumer data request otherwise than:

- through its sponsor (rule 5.1B(2)(b)), or
- to an accredited data recipient (rules 5.1B(2)(a) and 4.7A)

This means an affiliate cannot make a consumer data request directly to a data holder.

When seeking to access data, an affiliate must comply with the consumer data request requirements in Part 4 as amended by Schedule 1. In particular, when an affiliate seeks a collection consent from a consumer, and the consumer's CDR data will be collected by the sponsor at the affiliate's request (Mechanism 1), this fact must be disclosed to the CDR consumer (rule 4.3(2A)).

Conversely, where an accredited person seeks consent from a consumer and the data will be collected by the sponsor at the request of its affiliate, the accredited person must also state that fact to the consumer before disclosing the data to the sponsor (rule 4.11(3)(i)).

The AP disclosure consent rule (rule 4.7B) applies to both sponsors and affiliates. Where an affiliate seeks to rely on AP disclosure to access CDR data, it must comply with rule 4.7B in obtaining an AP disclosure consent.

Potential applications of sponsored accreditation

Example: customer-facing affiliate accesses CDR data through non-customer-facing sponsor

iAggregate, an SME, wants to provide an account aggregation service to customers using CDR data and applies for accreditation at the sponsored level. Best Bank is accredited to the unrestricted level and enters into a sponsorship agreement to sponsor iAggregate as its affiliate in the CDR, enabling iAggregate to use CDR data for the new service. Consumers have a direct relationship with iAggregate to receive the account aggregation service. However, iAggregate relies on Best Bank to collect CDR data from data holders. Many consumers that use iAggregate do not otherwise have a direct relationship with Best Bank. Due to the interconnected nature of Best Bank and iAggregate's infrastructure, Best Bank takes steps to ensure iAggregate's information security is adequate by assisting iAggregate with tailored technical advice and assistance, both before entering into the sponsorship arrangement and on and ongoing basis.

Example: affiliate relies on AP disclosures of CDR data

Podium is a platform service provider that offers consumers a good or service as well as the ability to download apps from its add-on marketplace and share their data with them. Podium is a person accredited to the unrestricted level that acts as a sponsor in the CDR, collects CDR data from data holders on behalf of consumers, and retains that data as an ADR. Podium relies on the AP disclosure rules to then share the data it holds with its affiliates, at a consumer's request, in situations where a consumer downloads the affiliates' apps from its marketplace. Before deciding whether to sponsor affiliates, Podium undertakes an assessment of whether they are appropriate partners for its platform. In the context of Podium's platform, and having regard to its risk appetite, this includes evaluating their general security posture as well as their reputation, business case and general business sophistication.

Example: Data enclave

An unrestricted accredited person may be willing to sponsor an affiliate on the basis the affiliate only uses CDR data within a secure 'data enclave' provided by the sponsor (for example, secure technical infrastructure that is managed by the sponsor). This could be given effect through a commercial arrangement between the parties. It is not a mandated element of the CDR sponsorship arrangement required by the rules (but may, in practice, be in the same document).

Example: sponsor provides white-labelled CDR infrastructure services to the affiliate

The sponsored level may also support CDR as a service or 'white labelled' CDR products/services in instances where an unrestricted person is willing to sponsor affiliates on the basis they use the unrestricted person's CDR as a service offering. For example, an unrestricted accredited person may act as an intermediary under Mechanism 1, collecting CDR data for its affiliates, and may also provide the infrastructure for consent, storage, and dashboards that an affiliate uses. In this instance, the unrestricted person does not take on liability for the affiliate's use of data or activities generally within the regime.

Responsibility and liability for affiliates' use and disclosure of data

Affiliates are responsible for their use and disclosure of CDR data they receive. Like all accredited data recipients, affiliates must not use or disclose data collected under a

consumer data request made under Part 4 otherwise than for a permitted use or disclosure (rule 7.6(1)). This applies whether the affiliate accesses CDR data through its sponsor or through AP disclosure.

To ensure that affiliates are appropriately liable for their use and disclosure of data, Schedule 1 inserts a deeming provision into rule 7.6 to ensure that any data collected by a sponsor at the request of an affiliate is taken to have also been collected by the affiliate (rule 7.6(3)). This amendment ensures rule 7.6 applies to affiliates when they have used their sponsor to collect data from data holders.

The affiliate's obligations

As accredited persons, affiliates must comply with all existing obligations on accredited persons in the CDR Rules. However, Schedule 1 adjusts some of these obligations specifically for persons with sponsored accreditation. Relevant instances are set out below.

The ongoing reporting requirements in Schedule 1 to the CDR Rules, which are default conditions on accreditation, have been adjusted for persons with sponsored accreditation. A person with sponsored accreditation must provide a self-assessment against the requirements in Schedule 2 to the CDR Rules (with respect to information security) and an attestation statement every two years (clauses 2.1(1), (2) and (3) in Schedule 1 to the CDR Rules).

Rules relating to privacy safeguards in Part 7 of the CDR Rules are also amended to reflect specific obligations for affiliates. In particular:

- Rule 7.2 relating to privacy safeguard 1 is amended to require the accredited person's CDR policy to include a list of the persons with whom the accredited person has a sponsorship arrangement, and to provide information about the nature of the services one party provides to the other for each such sponsorship arrangement; and
- Rule 7.4 relating to privacy safeguard 5 is amended to require information about whether CDR data was collected by a sponsor at their affiliate's request to be included in the consumer's dashboard when notifying of the collection of CDR data.

Schedule 1 also inserts new obligations that only apply to affiliates or persons with sponsored accreditation.

Specifically, affiliates are prohibited from accessing data directly from data holders (rules 5.1B(2) and 4.7A).

Affiliates must also provide their sponsor with the information and access to their operations it needs to fulfil its obligations as a sponsor, under the terms of the sponsorship arrangement (rule 1.10D).

The sponsor's obligations

Schedule 1 amends the CDR Rules to insert additional obligations on sponsors with respect to their sponsorship arrangements and their affiliates.

Schedule 1 inserts new default conditions on accreditation for sponsors and potential sponsors in Schedule 1 to the CDR Rules. Sponsors and potential sponsors must:

- before entering into a sponsorship arrangement, undertake due diligence to ensure the proposed affiliate is a suitable person for that role (clause 2.2(1) in Schedule 1 to the CDR Rules);
- before entering into a sponsorship arrangement, provide assistance to the proposed affiliate on technical and compliance matters (clause 2.2(1) in Schedule 1 to the CDR Rules);
- once the sponsorship arrangement has commenced, continue to provide the assistance and training in technical and compliance matters to affiliates (clause 2.2(2) in Schedule 1 to the CDR Rules); and
- take reasonable steps to ensure affiliates comply with their obligations as accredited persons (clause 2.2(2) in Schedule 1 to the CDR Rules).

These obligations are intended to be principles-based and scalable, with what constitutes reasonable steps and appropriate due diligence or assistance depending on the nature and context of the services being provided by affiliates using the CDR and under the sponsorship arrangement.

Sponsors also have a new obligation under Schedule 2 to the CDR Rules to implement a third-party management framework. This applies as a minimum information security control. The new rule requires sponsors to manage their affiliates in line with the third-party management framework (table item 7 in clause 2.2 in Schedule 2 to the CDR Rules).

Sponsors must also comply with the rules relating to privacy safeguards in Part 7 as amended. Rules 7.2 and 7.4 as described above apply to sponsors in the same way as they do to affiliates.

Sponsors also have new obligations to provide information about the sponsorship arrangement to the DRA in accordance with Part 5 as amended by Schedule 1 (rule 5.14).

Schedule 2 - The CDR representative model

The CDR representative model enables unaccredited persons to provide goods and services to consumers using CDR data in circumstances where they are in a CDR representative arrangement with an unrestricted accredited person who is liable for them.

An unaccredited person who is in a CDR representative arrangement would be known as the CDR representative of the principal accredited person.

CDR representative and principal relationship

Schedule 2 inserts new rule 1.10AA which defines the new terms ‘CDR representative’, ‘principal’ and establishes the minimum required terms in a ‘CDR representative arrangement’.

A CDR representative arrangement must be a written contract between the principal (a person with unrestricted accreditation) and a CDR representative (a person without accreditation). The arrangement sets out the key elements of how a consumer data request is made under the CDR representative model and the obligations of both the principal and the representative.

The principal's obligations under the arrangement are, where a representative has obtained the consent of a CDR consumer to collect and use CDR data, to make a consumer data request and disclose the CDR data (service data) it obtains through the request to the representative.

The principal must notify the DRA of new or proposed CDR representative arrangements within 30 business days of entering into the CDR representative arrangement (Schedule 2: (schedule 1, clause 2.3)). The principal must also include details about the representative in their CDR policy upon entering into the representative arrangement (rule 7.2(4)(ac)).

The CDR representative's obligations under the arrangement are to: not enter into a CDR representative arrangement with another principal; comply with privacy safeguard 2 (giving the CDR consumer the option of a using a pseudonym, or not identifying themselves), privacy safeguard 4 (destroying unsolicited CDR data), privacy safeguard 11 (ensuring the quality of CDR data), privacy safeguard 12 (security of CDR data), and privacy safeguard 13 (correction of CDR data) as if it were the principal; take the steps in Schedule 2 to the CDR Rules to protect the service data; not disclose the service data other than in accordance with the contract with the principal, delete service data when directed to by the principal and provide records of the deletion, and to adopt and comply with the principal's CDR policy in relation to the service data.

CDR representatives may offer goods or services on behalf of their principal ADR, or they may offer goods or services on their own behalf. In either event, the collection, use and disclosure of CDR data is an input to the provision of the goods or services to the consumer and the liability structure under the CDR regime remains the same. This flexibility is intended to ensure the model fits a broad range of stakeholder business models.

How a principal-CDR representative relationship is structured may depend on the principal's business model and the type of commercial arrangements it is willing to offer given the responsibility (and potential liability) that a principal will have for its representatives under the rules. For example, this kind of model could support a data enclave business – where a principal is only prepared to use CDR representatives if those clients use CDR data within the confines of the principal's data enclave, as a risk mitigation strategy. However, the model does not preclude more arm's length relationships – where a principal is prepared to assume responsibility and liability for the actions of a third party whose systems operate independently of the principal's.

Rule 1.16A provides that the principal must ensure its CDR representatives comply with their requirements under the arrangement, and keep records that explain each CDR arrangement, the use and management of the data by the CDR representative, and steps the principal has taken to ensure their CDR representatives comply with the arrangement. In addition, where a representative fails to comply with a relevant privacy safeguard this is also deemed to be a breach of the privacy safeguard by the principal (rules 7.3(2), 7.3A(2), 7.10A(2), 7.12(3)).

Importantly, any use or disclosure of service data by a CDR representative will be taken to have been by the unrestricted ADR principal, including any use or disclosure that occurs outside the scope of the CDR representative agreement (rule 7.6(4)). This means that if a CDR representative uses or discloses CDR data other than for a permitted purpose, it is the principal that will be liable for the contravention of the

existing civil penalty provision in rule 7.6(1). Under section 76 of the Act, the maximum penalty applicable for a contravention of rule 7.6(1) by a body corporate is the greatest of: $10,000,000; three times the benefit derived from the contravention; or ten per cent of the annual turnover of the body corporate during the period of 12 months before the contravention.

The principal is responsible for dispute resolution as the accredited person (rule 5.12). While this obligation sits with the principal, how dispute resolution obligations are met by the principal could be agreed between the parties to a CDR representative arrangement. For example, it may be that the representative conducts internal dispute resolution processes because the representative is best placed to respond to complaints in the first instance.

Collecting, using and disclosing data

Rule 4.3A provides that a CDR representative may, when necessary to provide requested goods or services to a consumer, ask the consumer for a collection consent for the principal, and use consents for the principal to provide the CDR data to the representative, and for the representative to use the CDR data to provide the requested goods and services. In giving the consent to the CDR representative, the consumer is deemed to have given the principal a valid request to collect the data

Schedule 2 inserts rule 4.3B which requires the CDR principal to ensure that, when its CDR representative asks for the required consents from a consumer in order to provide goods and services, the CDR representative does so in accordance with Division 4.3 of the CDR Rules. Rule 4.3B furthermore modifies specific provisions of Division 4.3 to ensure it can apply to CDR representatives and operate consistently with the principal-CDR representative relationship and liability framework (rule 4.3B(1)).

Rules 1.10A(4) and (5) clarify that where a consumer gives a consent to a CDR representative for their principal to collect CDR data and disclose it to the CDR representative, this is also taken to be a collection consent.

Rule 7.5(1)(d) provides that the disclosure of CDR data from the principal to the CDR representative is a permitted disclosure.

The principal must update and maintain the consumer dashboard for requests (although the principal may delegate this responsibility to the representative in the CDR representative arrangement) (rule 1.14(5)).

Potential applications of the CDR representative model

> **White labelled banking services with CDR functionality**
>
> Bank A is an unrestricted accredited person. It provides goods and services directly to consumers under its Bank A brand. However, to grow its deposit base, Bank A is willing to take on liability for third parties that use its underlying banking infrastructure to provide consumers with banking products that also have added features that use CDR data.
>
> Bank A partners with Fintech B. Fintech B markets a service to consumers where they can open a Fintech B branded bank account which is white labelled by Bank A, and see all their existing bank account balances in their Fintech B

app (including from other banks). Bank A collects CDR data in order for Fintech B to display the aggregated accounts and balances.

Sponsorship does not suit Bank A and Fintech B because Fintech B does not seek to become accredited. However, Bank A is prepared to assume full liability for Fintech B's use of CDR data as part of its commercial arrangement with Fintech B and therefore agrees to register Fintech B as its CDR representative.

'CDR as a service'/white labelling

The CDR representative model could also support CDR as a service or 'white labelled' CDR products/services in instances where an unrestricted person is willing to use representatives on the basis they use the unrestricted person's CDR as a service products. This could be used as a mechanism by unrestricted persons to manage the risk of using CDR representatives (and the liability that attaches to this). For example, an unrestricted accredited person may provide the infrastructure for collection, consent screens, storing CDR data, and dashboards, and the use of these services by the representative when providing their good or service to consumers may be a condition of the CDR representative arrangement..

Schedule 2 - Unaccredited OSPs

Background

Under the CDR Rules, an ADR can disclose CDR data to an unaccredited OSP so the OSP can provide services to the ADR in accordance with a CDR outsourcing arrangement. The CDR outsourcing arrangement is a contract between the OSP and the accredited person and must include certain restrictions on how the OSP can deal with the CDR data. The CDR rules also state that any use or disclosure of the CDR data by the OSP is taken to have been by the ADR.

The CDR Rules also permit an OSP that is an accredited person to collect CDR data on behalf of another accredited person. However, the CDR Rules currently do not permit an unaccredited OSP to collect CDR data directly from a data holder to provide intermediary services to an ADR; an unaccredited OSP can only receive data from an ADR.

In December 2020, the Act was amended to allow the CDR Rules to authorise the collection of CDR data by parties who are not accredited on behalf of an accredited person. It is now possible for the CDR Rules to allow unaccredited intermediaries to collect CDR data on behalf of an ADR.

Collection of CDR data by unaccredited OSPs

Schedule 2 to the Rules also amends rule 1.10 to allow any OSP, whether accredited or not, to collect CDR data on behalf of an ADR and to use that data, or data the ADR has disclosed to the OSP, to provide goods and services to the ADR. This will allow ADRs to use the services of an unaccredited OSP to collect data directly from a data holder on their behalf.

Schedule 2 to the Rules removes the prohibition on subcontracting of collection services. This prohibition was required to ensure only accredited OSPs could collect CDR data on behalf of the principal under the existing rules, and is no longer necessary given the expansion to unaccredited OSPs.

Summary of Schedules 1 and 2: comparison of new pathways to participation

A fintech, iService, plans to provide 'CDR as a service' products and services to clients. Its service includes collecting CDR data for its clients, analysing and enhancing the data, and providing the underlying infrastructure and 'white-labelled' products for clients to use to manage consent, dashboards, and CDR data storing and management.

FinHealth is a company that wishes to provide consumers with a personal financial management product.

iService and FinHealth could partner with each other under each of the new models:

Model	**Key attributes of the model**
Outsourcing	• In an outsourcing arrangement, FinHealth would be an accredited person and use iService as an outsourced service provider to collect CDR data and assist FinHealth to provide consumers with the personal financial management product. • FinHealth would be fully liable for iService. • iService would not need to be accredited to act as an OSP for FinHealth.
Sponsorship	• In a sponsorship arrangement, iService would be accredited to the unrestricted level and engage with FinHealth, who would be accredited to the sponsored level, as its affiliate. • Both iService and FinHealth could be subject to civil penalty provisions, as accredited persons. • FinHealth would receive CDR data through its sponsor iService, rather than directly from data holders. • iService would have additional obligations in respect of FinHealth. For example, conducting due diligence on FinHealth and providing FinHealth with technical and compliance training and support. • FinHealth would be able to partner with other sponsors in the CDR system. For example, it may choose to do so if it wishes to launch its app on several different platforms.
CDR representatives	• Under the representative model, iService would be accredited to the unrestricted level and enter into an arrangement with FinHealth as its CDR representative. Therefore, FinHealth would not be accredited. • iService would be fully liable for FinHealth. While FinHealth would not be accredited, iService could be held accountable for any breach of CDR obligations by FinHealth.

Expanded data sharing arrangements

The Rules establish two new data sharing models which are intended to provide consumers with greater choice in who they can direct that their data be shared with, while maintaining adequate protections:

- The trusted adviser model will allow consumers to consent to an ADR disclosing their CDR data outside the CDR system with professionals that are sufficiently regulated to receive CDR data, particularly due to consumer protection mechanisms that form part of their regulatory framework. This will facilitate access to relevant data to those working within these professions, while ensuring that disclosure of data can only occur with a consumer's consent.
- The CDR insights model will allow consumers to consent to insights informed by CDR data being shared outside the system for a range of prescribed purposes that are considered low risk. This will increase consumers' ability to engage with non-accredited parties in a way that limits the data they share to only what is necessary to receive a good or service.

Schedule 3 - Trusted advisers

Background

Schedule 3 amends the CDR Rules to allow a consumer to consent to an accredited person disclosing a consumer's CDR data to a person within a specified class (referred to as 'trusted advisers'). The intention is to facilitate current consumer practices of sharing their data with trusted third parties in order to receive advice or a service, and increase convenience and control for consumers by enabling them to use the CDR to share their data with their chosen trusted advisers. In turn, this will encourage greater participation in the CDR by accommodating existing and new use cases which rely on the ability to disclose data to third parties to be accommodated in the CDR.

Trusted adviser disclosure consent

Rule 1.10A provides that a CDR consumer can consent to an accredited data recipient disclosing a consumer's CDR data to a nominated trusted adviser (***TA disclosure consent***). As with other CDR consumer consents, the accredited person's processes for asking a consumer to give a consent must accord with any consumer experience data standards, and the consent given must be voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn.

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

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

- mortgage brokers.

The accredited person cannot make the nomination of a trusted adviser or the giving of a TA disclosure consent a condition for the supply of goods and services requested by the CDR consumer.

Consumer protections

Trusted advisers do not attract the regulatory obligations that apply to ADRs under the CDR regime. However, these rules recognise that as members of a professional class, they are subject to existing professional or regulatory oversight, including obligations consistent with safeguarding consumer data (e.g. fiduciary or other duties to act in the best interests of their clients).

The following requirements strengthen the protections for CDR consumers that wish to disclose their CDR data to their nominated trusted advisers:

- An ADR cannot disclose CDR data to a trusted adviser unless it has taken reasonable steps to confirm the person to whom the data is to be disclosed is a member of a class of trusted advisers set out in the CDR Rules (rule 7.5A(3)). It is envisaged that what constitutes reasonable steps will be detailed in guidance material. However, these steps might include the ADR checking a register for the relevant class of trusted adviser or seeking confirmation from the trusted adviser.
- The transfer of the CDR data from an ADR to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules, including the requirement to ensure that data is encrypted in transit.
- Given the importance of CDR consumers understanding the effect of consenting to the disclosure of their CDR data to non-accredited persons, disclosures are subject to CX standards to be made by the Data Standards Body (rule 8.11(1)). This will ensure the CDR consumer is provided with adequate information to give informed consent, for example, information that the use of the data by the recipient will not be covered by the CDR regime and the recipient may not have obligations under the *Privacy Act 1988*.
- When the ADR discloses the CDR data to a trusted adviser, the ADR must update each consumer dashboard that relates to the request to indicate what CDR data was disclosed, when it was disclosed and the name of the trusted adviser it was disclosed to (rule 7.9(3)). This will enable the CDR consumer to monitor where their data is being sent, and if necessary, withdraw their TA disclosure consent.
- Rule 7.5A(2) provides that disclosure of CDR data under a TA disclosure consent is not a permitted use or disclosure until the earlier of a date to be determined or when the Data Standards Chair makes consumer experience data standards for disclosure of CDR data to trusted advisers. The specified date is expected to be three months after the commencement of the rules.

Record keeping and reporting

ADRs are required to:

- maintain records that record and explain the disclosures of CDR data to trusted advisers, the trusted advisers to whom CDR data was disclosed, and the steps taken to confirm that a trusted adviser is a member of a class of trusted advisers (rules 9.3(2)(eb) and (ec)); and

- report the number of consents it received from CDR customers and for each category (class) of trusted adviser, and the number of trusted advisers to whom the CDR data was disclosed (rules 9.4(2)(f)(vi) and (vii)).

Schedule 3 - CDR insights

Background

Schedule 3 amends the CDR Rules to allow a consumer to consent to an ADR sharing certain limited 'CDR insights' using their CDR data to any person, provided the disclosure is for one of the specified purposes in the CDR Rules.

Allowing the disclosure of CDR insights is intended to enable a safer and more efficient way for consumers to share certain insights obtained from their CDR data to receive goods and services, reducing the need to share detailed records or passwords to facilitate access to their information. As consumer information is already shared through informal and unstructured ways, allowing CDR insights to be shared through the CDR could help improve the accuracy, credibility and security of existing information sharing practices, as well as enable entirely new services.

The CDR insights proposal would allow consumers to direct that CDR insights be shared outside the CDR system, meaning this data would no longer be subject to the protections of the Privacy Safeguards. As such, the CDR Rules limit the disclosure of insights by reference to specified purposes, and include protections to ensure consumers properly understand the nature of the insight they are agreeing to disclose.

Insight disclosure consents

A new type of disclosure consent is added in rule 1.10A(1), called an ***insight disclosure consent***.

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

- to identify the consumer[1]
- to verify the consumer's account balance
- to verify the consumer's income, or
- to verify the consumer's expenses

For these purposes, 'verify' means to confirm, deny or provide some simple information about the consumer's identity, account balance, income or expenditure based on their CDR data. These CDR insights would allow consumers to securely provide and confirm relevant factual information about themselves, while giving the recipient comfort in its authenticity and accuracy. These purposes are intended to support the sharing of information that the consumer could themselves confirm and understand.

ADRs would be responsible for ensuring that the CDR insights they disclose align with the purpose consented to by the consumer.

[1] Though CDR insights used to identify a consumer could bolster confidence about a consumer's identity, their use is not intended to substitute for formal proof of identity requirements (for example, proving someone is of age to buy alcohol or meeting know-your-customer requirements to set up a bank account).

For example, CDR insights could be used to:

- confirm with a 'yes' or 'no' that the personal information provided in an application matches the information held by a bank
- confirm with a 'yes' or 'no' that the consumer's account balance is or is not sufficient to meet a particular payment
- provide a consumer's actual account balance at a specific point in time
- provide an alert to a merchant if a direct debit payment will fail, or
- provide the consumer's average income over a specific period of time

> **Example: CDR insights to verify a consumer's identity**
>
> A consumer is signing up to a new service provider and manually gives the provider their name and address. Though the service provider does not have a legal obligation to identify their customer, they want to know that they are dealing with a real person. Instead of asking for copies of identity documents to confirm that the consumer is who they say they are, the service provider asks the consumer to verify their identity using an ADR.
>
> Through this service, the consumer agrees to the new service provider sharing the details they provided with the ADR. The consumer then also consents to the ADR securely collecting relevant details from their data holder through the CDR, and to the ADR passing a 'yes' or 'no' CDR insight to their new service provider to confirm that the details they receive through the CDR match those provided manually. This gives the provider greater confidence regarding the consumer's identity and allows the consumer to easily set up a new service.
>
> **Example: CDR insights to verify a consumer's account balance**
>
> An ADR partners with a gym to disclose insights, with consumer consent, that inform the gym if a consumer has insufficient funds in their account to meet their repayment obligations. Where the insight reveals the consumer has insufficient funds, the gym is able to text the consumer a prompt to transfer money into their account in time for their next payment and avoid a late payment fee.

Consumer protections

The Data Minimisation Principle (rule 1.8) in the CDR Rules prohibits an accredited person from collecting or using a CDR consumer's data beyond what is reasonably needed to provide the goods and services the consumer requested. This requirement applies when an insight disclosure consent is sought and when the CDR insight is disclosed. As a result, ADRs are required to limit CDR insights to the minimum information necessary to meet the consumer's request.

Under rule 7.5A(5), even if an insight disclosure consent is given, the accredited person is not permitted to disclose the CDR insight if it includes or reveals ***sensitive information*** within the meaning of the *Privacy Act 1988*.

Rule 7.5A(4) provides that disclosure of CDR data under an insight disclosure consent is not a permitted use or disclosure until the earlier of a date to be determined in the rules or when the Data Standards Chair makes consumer experience data standards for disclosure of CDR insights. The specified date is expected to be three months after the commencement of the rules.

Rule 4.11(3)(ca) requires an accredited person to give an explanation of the CDR insight to the CDR consumer when seeking the insight disclosure consent that will

make it clear what the CDR insight would reveal or describe. The CDR Rules do not require a CDR insight to be shown to a consumer prior to it being disclosed. However, where practical, this step could be taken to assist the consumer's understanding of what the CDR insight would reveal or describe and help meet the accredited person's obligation under rule 4.11.

Rule 8.11(1)(c)(v) contains new requirements for data standards to be made about disclosure and security of CDR data that is disclosed in a CDR insight, and the processes by which insight disclosure consents are obtained, including ensuring the consumer understands their data will leave the CDR system and explaining the CDR insight in accordance with rule 4.11 (rule 8.11(1A).

Rule 1.14(3)(ea) provides that after an ADR discloses a CDR insight, it must update the consumer's dashboard as soon as is practicable with a description of the CDR insight and to whom it was disclosed.

Record keeping and reporting

Rule 9.3(2)(ed) requires accredited data recipients to keep records of CDR insights, including a copy of each insight itself and when and to whom it was disclosed. Though these records are not required to be included on the ADR's consumer dashboard (in light of such detailed information potentially crowding dashboards and making them overly difficult to engage with), the dashboards must notify consumers that they are entitled to request further records and information about how to make such a request under rule 9.5 (rule 1.14(3A)).

Rule 9.4(2)(f)(viii) requires an accredited data recipient to report to the ACCC and the Office of the Australian Information Commissioner on the number of insight disclosure consents it received during a reporting period.

Schedule 4 - Joint accounts

Background

The CDR Rules only apply to CDR data held in consumers' joint accounts in the banking sector and require all joint account holders to set data sharing preferences before a joint account holder can provide consent and authorisation to share data on the joint account.

In April 2021, Treasury and the Data Standards Body released a rules and standards design paper (**design paper**) seeking informal feedback on switching the joint account data sharing to a single consent model by default. This was proposed to address concerns that the current approach involves high levels of friction that may lead to poor consumer outcomes. The development of the approach to data sharing for joint accounts in the Rules was informed by the design paper consultation process.

Schedule 4 to the Rules establishes new economy-wide rules that set out the approach for data sharing where there are two or more account holders who are individuals with equivalent ownership of the account (commonly understood to be a 'joint account').

Where the concept of a joint account is not relevant to a sector, the joint account rules would accordingly not be relevant. For example, in the energy sector it is anticipated

that where accounts are set up with a primary account holder, the existing secondary user rules would be used to expand data sharing access to additional persons on the account.

CDR data that relates to a joint account can be disclosed under the Rules only in accordance with the disclosure option that applies to the account. Division 4A.2A sets out:

- the three disclosure options, with the default option being the pre-approval option;
- an obligation for data holders to provide a disclosure option management service (DOMS)[2] for all joint accounts through which joint account holders can change the disclosure option that applies to the account, or propose a change to the other account holders;
- when one joint account holder proposes to change the disclosure option—a process by which the other joint account holders can either agree with or reject the proposal; and
- some associated notification requirements.

The Rules move the joint account rules from Schedule 3 (the banking sector Schedule) to the main body of the CDR Rules.

Disclosure options

Rule 4A.4 sets out the disclosure options that can apply to a joint account. These disclosure options are relevant when an accredited person makes a consumer data request on behalf of one joint account holder or a secondary user under Part 4.

The default is the pre-approval option (rule 4A.4(1)(a)). This automatically allows an individual joint account holder to independently share data on the joint account by consenting to an accredited person collecting and using the data from a joint account, and authorising the disclosure of that data with a data holder.

Another option is the non-disclosure option (rule 4A.4(1)(c)). If this option applies, CDR data relating to the joint account cannot be disclosed under the CDR Rules.

The third option is the co-approval option (rule 4A.4(1)(b)). If this option applies, CDR data relating to the joint account can be disclosed only with the approval of all the account holders.

Data holders must offer the pre-approval option and non-disclosure option on joint accounts, and may offer the co-approval option on an optional basis (rules 4A.4(2) and (3)).

The Rules seek to strike the right balance between providing consumers with control over data sharing and providing convenience to consumers so they can benefit from the CDR. The Rules reflect current data sharing capabilities on joint accounts for PDF and CSV files.

[2] The disclosure option management service (DOMS) is equivalent to, and replaces, the joint account management service (JAMS) within the current CDR Rules.

Currently joint account holders may independently share their joint account data in CSV or PDF format, or via screen scraping, without consent from or notification to the other account holders.

Under the Rules, joint account holders will be able to:

- change the default sharing setting to the non-disclosure option, including ahead of joint account data being in-scope and available for sharing. Choosing this setting would ensure no future data sharing from the joint account via the CDR is possible and any on-going data sharing arrangements are ceased;
- stop data sharing arrangements with a specific accredited person, whether this was initiated by themselves or another joint account holder. This will allow consumers to have granular control of data sharing arrangements.

The Rules treat CDR data sharing as a new authority, rather than as an authority that is analogous to current transaction or payment authorities on joint accounts. This means all joint accounts, will be treated in the same manner under the CDR, irrespective of how authorities to transact have been set for the account. The intention is that this will reduce implementation complexity, and aid consumer understanding in using the CDR.

Example: Joint account holder initiates data sharing on a joint account under the single consent model for data sharing

Bob and Erin have a joint account with Peanuts Bank. The default pre-approval disclosure option applies to the joint account which means that the joint account is available for sharing.

Erin wishes to share data from the joint account with Penny Savers, an accredited person. She gives her consent to Penny Savers to collect data on the joint account and provides her authorisation to Peanuts Bank to disclose the data. Peanuts Bank discloses the data to Penny Savers. Peanuts Bank sends a notification to Bob that Erin has authorised the disclosure of data on the joint account to Penny Savers. Peanuts Bank also updates Bob and Erin's consumer dashboard to reflect details of the sharing arrangement.

Example: Joint account holder turns sharing setting 'off' on a joint account

Bob decides to set his data sharing preference to 'off' and stop data sharing on the joint account. Via the DOMS he selects the non-disclosure option.

Peanuts Bank stops sharing data from the joint account with Penny Savers. Peanuts Bank contacts Erin using its ordinary means for contacting her to notify her that Bob selected the non-disclosure option, and consequently that disclosure option now applies to their joint account. Peanuts Bank also updates both Bob and Erin's consumer dashboard and DOMS to show that the non-disclosure option applies to their joint account.

Oversight and changing disclosure options

Rule 4A.5 provides that a data holder must offer joint account holders a DOMS that can be used to select and manage disclosure options.

Data holders would still be required to provide a consumer dashboard. Currently, the CDR Rules only require data holders to provide a consumer dashboard if a disclosure

option applies or has applied to the joint account. However, the Rules require data holders to provide a dashboard to all joint account holders at the outset.

Rule 4A.7 provides that:

- any joint account holder can choose that the non-disclosure option will apply;
- a change from the non-disclosure option to another option requires the agreement of all the joint account holders.

Rule 4A.7 also provides that if the co-approval option is offered by the data holder:

- if the pre-approval option applies to a joint account, any joint account holder can choose that the co-approval option will apply; and
- a change from the co-approval option to the pre-approval option requires the agreement of all the joint account holders.

Rule 4A.8 provides that if a joint account holder wants to change the disclosure option on the joint account from non-disclosure to either pre-approval or co-approval (if offered), that account holder may propose the change using the DOMS. If co-approval is offered by the data holder and the joint account holder wants to change the disclosure option from co-approval to pre-approval, that account holder may likewise propose the change using the DOMS. In both cases, the data holder must notify the other joint account holders of specified matters concerning the proposed change and invite them to either agree or reject the proposal.

If the data holder considers it necessary, in order to prevent financial or physical harm or abuse, to avoid seeking the other joint account holders' agreement to change the disclosure option , the data holder need not seek that agreement (rule 4A.14(4)). This would also apply if co-approval is in place.

Consumer data requests that relate to joint accounts

Rule 4A.11 provides that when a data holder receives a consumer data request that includes CDR data relating to one or more joint accounts, the request must be processed as follows:

- if the pre-approval disclosure option applies to the joint account—the data holder must respond to the request;
- if the co-approval option is offered by the data holder and applies to the joint account—the data holder must ask the requesting account holder to authorise the disclosure of the requested data, seek the other account holders' approval for the disclosure, then disclose the data in accordance with the request;
- if the non-disclosure option applies—the data holder must refuse to disclose the requested CDR data.

Division 4A.3 also deals with how requests are processed when the accredited person makes a consumer data request on behalf of a secondary user of the joint account (if there is a secondary user instruction in place on the account).

Notification requirements

Rule 4A.6 requires data holders to notify joint account holders of the following matters in relation to the account (for new accounts, when the account is opened, or for existing accounts, at least 7 days prior to joint accounts being in scope for sharing under the Rules):

- the default setting for data sharing being set to 'pre-approval' so that the joint account is available for data sharing by all joint account holders;
- how joint account holders can change the default sharing setting on their joint account;
- the disclosure options that are available in relation to the joint account;
- the effect of each disclosure option and how it operates, including, if there is a secondary user for the joint account, how it operates in relation to the secondary user;
- that they can at any time, either change the disclosure option on the account to non-disclosure, or propose to the other joint account holders to change to either pre-approval or co-approval (where co-approval is offered by the data holder);
- how they can make such a choice or proposal and how to respond when they receive a change proposal; and
- that when CDR data relating to the joint account is disclosed under the CDR Rules, the data holder will ordinarily provide each joint account holder with a consumer dashboard through which they will be able to see information about disclosures relating to the account.

This notification must be made, in accordance with any data standards and via the ordinary method for contacting each joint account holder.

Rule 4A.16 requires data holders to allow joint account holders to set certain notification preferences. If data standards are in place, this must be done in line with those standards. This would allow consumers to set preferences such that they would not receive certain notifications that data holders would otherwise be required to provide. The ability to set preferences does not affect dashboard requirements or the requirement for data holders to obtain agreement from joint account holders to change the disclosure option or approve a disclosure of CDR data.

Secondary users of joint accounts

The CDR Rules include principles-based provisions relating to 'secondary users' of joint accounts. The Rules maintain these settings. That is, in order for a secondary user to be able to share data on a joint account, a secondary user instruction must be provided by an account holder.

The secondary user rules generally operate such that:

- if a pre-approval disclosure option applies to the joint account, secondary users can independently authorise data sharing on the account (if there is a secondary user instruction in place on the account);

- if a co-approval option applies to the joint account, secondary users can authorise data sharing on the joint account, however, the data holder must obtain the approval of all joint account holders before data on the joint account can be shared; and
- if a non-disclosure option applies to the joint account, secondary users cannot authorise data sharing on the joint account.

Other matters

Existing provisions in the CDR Rules relating to protections for vulnerable consumers, including exemptions from data holder obligations to prevent physical or financial harm or abuse are maintained (see rule 4A.14(4)). This includes the ability for data holders, in situations where they consider it necessary in order to prevent physical or financial harm or abuse (by applying their existing practices and procedures), to:

- treat a joint account as an individually held account so that a person who may be in an abusive relationship can share data on a joint account without the other account holder knowing; and
- refuse to share data on a joint account.

The Rules also repeal the existing provision in the CDR Rules requiring data holders to invite joint account holders to set up their joint account data sharing preferences during the authorisation process (known as the 'in-flow' election). This function is unnecessary if a single consent model for data sharing on joint accounts is adopted.

Implementation timeline

On 30 April 2021, Treasury announced that requirements for banks to implement the joint account requirements that would have applied from November 2021 would be deferred, with new compliance dates to be set following consultation.

The Rules amend the commencement table in rule 6.6 of Schedule 3 to the CDR Rules and set 1 April 2022 as the new compliance date for joint account data sharing in the banking sector. This date seeks to balance the benefits of having joint accounts data sharing in the CDR and the need for sufficient time for data holders to meet technical requirements.

The Rules also include transitional provisions that:

- require relevant data holders to continue to comply with the former joint account transitional provisions until 1 April 2022, when they must begin to comply with Part 4A of the CDR Rules;
- require data holders to notify consumers with joint accounts of the change to the default setting to share at least a week before the commencement date; and
- provide that joint accounts that are currently set to the 'no disclosure option' are not switched to the pre-approval option on the commencement date.

Schedule 5 - Other amendments

Direct to consumer request service

Background

Under Part 3 of the CDR Rules, data holders are required to implement an online service that allows consumers to directly request their CDR data in a human readable form and in accordance with the data standards. For data holders in the banking sector, this requirement must be complied with by 1 November 2021 (CDR Rules, Schedule 3, clause 6.6).

Deferral of Part 3 obligations

In order to allow further consultation about the way in which direct to consumer obligations should be provided for and in machine-readable form via APIs (and the way in which the data standards should provide for this), the Rules amend clause 6.6 of Schedule 3 to remove the compliance date for the Part 3 obligations in the banking sector.