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

I, Jane Hume, Minister for Superannuation, Financial Services and the Digital Economy, make the following rules.

Dated 30 September 2021

Jane Hume
Minister for Superannuation, Financial Services and the Digital Economy

41589883

……..

Contents

1 Name 2
2 Commencement 2
3 Authority 2
4 Schedules 2

Schedule 1—Amendments relating to sponsored accreditation 3

Schedule 2—Amendments relating to CDR representatives 11

Schedule 3—Amendments relating to trusted advisers and insights 25

Schedule 4—Amendments relating to joint accounts 29

Schedule 5—Amendments relating to staged implementation 41

Schedule 6—Consequential and minor amendments 43

Schedule 7—Transitional 54

41589883

Authorised Version F2021L01392 registered 05/10/2021

1 Name

This instrument is the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 4, and anything in this instrument not elsewhere covered by this table	The day after this instrument is registered	
2. Schedule 1	1 February 2022	
3. Schedule 2	The day 14 days after this instrument is registered	
4. Schedules 3, 4 and 5	The day after this instrument is registered	
5. Items 1,2,3,15,18, and 19 of Schedule 6	The day 14 days after this instrument is registered	
6. The remainder of Schedule 6	The day after this instrument is registered	
7. Schedule 7	The day after this instrument is registered	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 56BA of the *Competition and Consumer Act 2010*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments relating to sponsored accreditation

Note: This Schedule commences on 1 February 2022

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.6 (11)

Omit "persons accredited at the "unrestricted" level", substitute "accredited persons".

2 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

affiliate has the meaning given by rule 1.10D.

level, in relation to accreditation, has the meaning given by rule 5.1A.

sponsor has the meaning given by rule 1.10D.

sponsored accreditation means accreditation at the sponsored level mentioned in rule 5.1A.

Note: See also rules 1.10D and 5.1B.

sponsorship arrangement has the meaning given by rule 1.10D.

unrestricted accreditation means accreditation at the unrestricted level mentioned in rule 5.1A.

3 Before the heading to Division 1.4, in Division 1.3

Insert:

1.10D Meaning of *sponsorship arrangement*, *sponsor* and *affiliate*

(1) A ***sponsorship arrangement*** is a written contract between a person with unrestricted accreditation (the ***sponsor***) and another person (the ***affiliate***), under which:

(a) the sponsor agrees to disclose to the affiliate, in response to a consumer data request made by the affiliate in accordance with rule 5.1B(2), CDR data that it holds as an accredited data recipient; and

(b) the affiliate undertakes to provide the sponsor with such information and access to its operations as is needed for the sponsor to fulfil its obligations as a sponsor.

Note: A person does not need to have sponsored accreditation to enter into a sponsorship arrangement as an affiliate, but will need it to make the consumer data requests mentioned in paragraph (a)

(2) A sponsorship arrangement may also provide for the sponsor to:

(a) make consumer data requests at the request of the affiliate; or

41589883

Authorised Version F2021L01392 registered 05/10/2021

(b) use or disclose CDR data at the request of the affiliate.

4 After paragraph 1.14(3)(h)

Insert:

(ha) if the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request:

(i) the sponsor's name; and

(ii) the sponsor's accreditation number;

5 Before subrule 4.3(3)

Insert:

(2B) If the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request:

(a) the request for a collection consent must specify that fact; and

(b) a consent for the affiliate to collect the CDR data is taken to be consent for the sponsor to so collect it.

6 Subrule 4.11(3)

At the end, add:

;

(i) if the accredited person is an affiliate and the CDR data will be collected by a sponsor at its request;

(i) a statement of that fact; and

(ii) the sponsor's name; and

(iii) the sponsor's accreditation number; and

(iv) a link to the sponsor's CDR policy; and

(v) a statement that the CDR consumer can obtain further information about such collections or disclosures from the sponsor's CDR policy if desired.

7 After rule 4.20

Insert:

4.20A Application of Subdivision to sponsor and affiliate

Where this Subdivision would, if not for this rule, require both an affiliate and the affiliate's sponsor to give a notice to a CDR consumer, the sponsor and the affiliate may choose which will give the notice.

8 Before subdivision 5.2.1

Insert:

41589883

Authorised Version F2021L01392 registered 05/10/2021

Subdivision 5.2.1A—Levels of accreditation

5.1A Levels of accreditation

Accreditation may be at either of the following ***levels***:

(a) unrestricted;

(b) sponsored.

5.1B Sponsored accreditation

(1) This rule applies in relation to a person with sponsored accreditation.

(2) The person must not make a consumer data request under these rules unless it has a registered sponsor.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) The person must not make a consumer data request under these rules otherwise than:

(a) to an accredited data recipient under rule 4.7A; or

(b) through a registered sponsor acting at its request under the sponsorship arrangement.

Note: This subrule is a civil penalty provision (see rule 9.8).

(4) The person must not engage a provider in a CDR outsourcing arrangement to collect CDR data from a CDR participant on its behalf.

Note: This subrule is a civil penalty provision (see rule 9.8).

(5) The person must not have a CDR representative.

Note: This subrule is a civil penalty provision (see rule 9.8).

(6) If the person ceases to have any registered sponsor, then, for subrule 4.14(1)(f):

(a) any collection consents for the person expire; however

(b) any use consents and disclosure consents continue in effect.

Note: It is also possible for the accreditation to be suspended or revoked under item 11 of subrule 5.17(1).

(7) If the person has not had a registered sponsor for a period of 120 days, the accreditation is taken to have been surrendered.

Note: See subrule 4.14(2) and rule 5.23 for the effect of surrender of accreditation.

(8) For this rule, a sponsor of the person is a ***registered sponsor*** if:

(a) the sponsor has notified the Data Recipient Accreditor in accordance with subrule 5.14(2); and

(b) the Registrar has recorded on the Register of Accredited Persons that the person is an affiliate of the sponsor.

Note: If the sponsorship arrangement terminates, the sponsor is no longer a registered sponsor for subrules (2) and (3), even if the Register has not yet been updated to reflect this.

41589883

9 Rule 5.2, note after heading

Repeal.

10 After paragraph 5.2(2)(a)

Insert:

(aa) indicate the level of accreditation that is sought; and

11 Rule 5.5, heading

Omit "—unrestricted level".

12 Rule 5.5, note after heading

Omit " This rule specifies those criteria for the "unrestricted" level of accreditation.".

13 Rule 5.5

Omit "at the "unrestricted" level".

14 Rule 5.12, heading

Omit "at the "unrestricted" level".

15 Subrule 5.12(1)

Omit "A person who is accredited at the "unrestricted" level", substitute "An accredited person".

16 Subrule 5.12(2)

Omit "A person who is accredited at the "unrestricted" level", substitute "An accredited person".

17 Rule 5.14

(a) At the beginning, insert:

General

(1)

(b) After subrule (1), as numbered by paragraph (a), insert:

Sponsors

(2) An accredited person must notify the Data Recipient Accreditor as soon as practicable, but no later than 5 business days after either of the following occurs:
  (a) the person becomes a sponsor of an affiliate;
  (b) where the accredited person is a sponsor of an affiliate—the sponsorship arrangement is suspended, expires, or is terminated.

18 Table in subrule 5.17(1)

Add at the end:

41589883

Authorised Version F2021L01392 registered 05/10/2021

11	for a person with sponsored accreditation: (a) a sponsorship arrangement expires or terminates; or (b) the accreditation of a sponsor is suspended or revoked; or (a) the person has had a sponsor but now has none;	may, in writing: (a) suspend; or (b) revoke; the person's accreditation, as appropriate.

19 Paragraph 5.18(1)(a)

After "accredited person" insert "and any associate".

20 Paragraph 5.18(1)(b)

After "accredited person" insert "and any associate".

21 Subrule 5.18(2)

After "notify the person" insert "and any associate".

22 After subrule 5.18(2)

Insert:

(3) For this rule, each of the following is an ***associate*** of the accredited person:
(a) any sponsor;
(b) any affiliate.

23 After paragraph 5.24(b)

Insert:

(ba) for a person with sponsored accreditation—any sponsor;
(bb) for a sponsor—each affiliate;

24 Rule 5.24, Note 2

Repeal.

25 After paragraph 7.2(4)(a)

Insert:

(aa) include a list of the accredited persons with whom the accredited data recipient has a sponsorship arrangement; and
(ab) for each such arrangement—include the nature of the services one party provides to the other party; and

26 Rule 7.4

Substitute:

41589883

Authorised Version F2021L01392 registered 05/10/2021

7.4 Rule relating to privacy safeguard 5—notifying of the collection of CDR data

(1) For section 56EH of the Act, and subject to subrule (2), an accredited data recipient that collected the CDR data in accordance with section 56EF of the Act as a result of a collection consent must update the person's consumer dashboard as soon as practicable to indicate:

(a) what CDR data was collected; and

(b) when the CDR data was collected; and

(c) the CDR participant for the CDR data from which the CDR data was collected.

(2) Where the CDR data was collected by a sponsor on behalf of an affiliate:

(a) the sponsor and the affiliate may choose which of them will be responsible for updating the consumer's dashboard in accordance with subrule (1); and

(b) the dashboard must also indicate that the CDR data was collected by the sponsor on behalf of the affiliate.

Note 1: See paragraph 1.14(3)(h).

Note 2: See rule 1.16 for how this rule applies in the case of a CDR outsourcing arrangement in which a provider collects CDR data on behalf of a principal.

27 Paragraph 7.5(1)(d)

After "outsourcing arrangement" insert ", or to the other party in a sponsorship arrangement".

28 After subrule 7.6(2)

Insert:

(3) For this rule, any CDR data collected by an accredited person at the request of an affiliate is taken also to have been collected by the affiliate.

29 Paragraph 9.3(2)(i)

Substitute:

(i) if applicable:

(i) any sponsorship arrangement or CDR outsourcing arrangement to which the accredited data recipient is a party;

(ii) the use and management by the other party to each such arrangement of CDR data collected by it or provided to it under the arrangement;

30 Subparagraph 9.4(2)(f)(i)

Substitute:

(i) the number of consumer data requests made by the accredited data recipient during the reporting period, distinguishing

(A) in the case of a sponsor—between requests made on its own behalf and those made on behalf of affiliates; and

(B) in the case of an affiliate—between those made to its sponsors and those made to other accredited persons;

41589883

Authorised Version F2021L01392 registered 05/10/2021

31 Subparagraph 9.4(2)(f)(iii)

Substitute:

(iii) the number of consumer data requests the accredited data recipient received from an accredited person on behalf of a CDR consumer during the reporting period, distinguishing, in the case of a sponsor, between requests from affiliates and those from other accredited persons;

32 Paragraph 9.4(2)(f)

At the end, add:

;

(ix) in the case of a sponsor or an affiliate—the number of sponsorship arrangements to which it was a party during the period.

33 Schedule 1, subclause 2.1(1), definitions of *assurance report* and *attestation statement*

Substitute:

assurance report means:

(a) for a person with unrestricted accreditation—a report that is made in accordance with:

(i) ASAE 3150; or

(ii) an approved standard, report or framework; and

Note: See the *CDR Accreditation Guidelines*, which could in 2020 be downloaded from the Commission's website (https://www.accc.gov.au).

ASAE 3150 could in 2020 be downloaded from the Auditing and Assurance Standards Board's website (https://www.auasb.gov.au/admin/file/content102/c3/Jan15_ASAE_3150_Assurance_Engagements_on_Controls.pdf).

(b) for a person with sponsored accreditation—an assessment of its capacity to comply with Schedule 2 that is made in accordance with any approved requirements;

that does not include the information that must be provided in an attestation statement.

attestation statement means:

(a) for a person with unrestricted accreditation—a statement in the form of a responsible party's statement on controls and system description that is made in accordance with ASAE 3150; and

(b) for a person with sponsored accreditation—a statement about its compliance with Schedule 2 that is made in accordance with any approved requirements.

34 Schedule 1, After clause 2.1

Insert:

41589883

Authorised Version F2021L01392 registered 05/10/2021

2.2 Conditions on sponsors and potential sponsors

(1) An accredited person that proposes to become the sponsor of a person that has, or proposes to apply for, sponsored accreditation must:

(a) have in place a defined third-party management framework that:

(i) will ensure that the person maintains appropriate information security capabilities as an affiliate; and

(ii) includes requirements and activities relating to the following matters as they relate to information security:

(A) due diligence prior to establishing new relationships or contracts; and

(B) annual review and assurance activities; and

(C) reporting requirements; and

(b) provide the person with any appropriate assistance or training in technical and compliance matters relating to Schedule 2.

(2) The sponsor of an affiliate must:

(a) maintain the management framework and manage its relationship with the affiliate in accordance with it;

(b) continue to provide any appropriate assistance or training in such technical and compliance matters; and

(c) take reasonable steps to ensure that the affiliate, as an accredited person, complies with its obligations under Schedule 2.

35 Schedule 2, paragraph 1.5(1)(a)

After “complies with the”, insert “applicable”.

41589883

Authorised Version F2021L01392 registered 05/10/2021

Schedule 2—Amendments relating to CDR representatives

Note: This Schedule commences on the day 14 days after this instrument is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

CDR representative has the meaning given by rule 1.10AA.

CDR representative arrangement has the meaning given by rule 1.10AA.

CDR principal has the meaning given by rule 1.10AA.

2 Subrule 1.7 (1), definition of "CDR consumer complaint"

Substitute:

CDR consumer complaint means any expression of dissatisfaction made by a CDR consumer to or about a CDR participant, or a CDR representative of a CDR participant:

(a) that relates to:

(i) that person's obligations under or compliance with:

(A) Part IVD of the Act; or

(B) these rules; or

(C) binding data standards; or

(ii) the provision to the CDR consumer, by that person, of the goods or services in respect of which the consumer granted consent under Part 4; and

(b) for which a response or resolution could reasonably be expected.

Note: Complaints of a kind referred to in sub-subparagraph (a)(i)(B) include a complaint relating to the participant's obligations under, or compliance with, rules dealing with the handling of CDR consumer complaints.

3 Subrule 1.7 (1), definition of "service data"

Substitute:

service data:

(a) in relation to a CDR outsourcing arrangement—has the meaning given by rule 1.10; and

(b) in relation to a CDR representative arrangement— has the meaning given by rule 1.10AA.

41589883

Authorised Version F2021L01392 registered 05/10/2021

4 After rule 1.10

Insert:

1.10AA Meaning of *CDR representative* and related terms

Note: From the point of view of a CDR consumer who is the customer of a CDR representative, the consumer deals with the CDR representative~~,~~ as if it were an accredited person, and may not deal with the principal at all. The consumer requests the goods or services from the CDR representative; the CDR representative identifies the CDR data that it needs in order to provide the goods and services; the consumer gives their consent to the CDR representative for the collection and use of the CDR data. The consumer is informed that the CDR principal will do the actual collecting, but as a background detail.

(1) For these rules, where two persons are the principal and the representative in a CDR representative arrangement, the representative is a ***CDR representative*** of the principal.

(2) For these rules, a ***CDR representative arrangement*** is a written contract between a person with unrestricted accreditation (the ***principal***) and a person without accreditation (the ***representative***) under which:

(a) where the representative has obtained the consent of a CDR consumer to the collection and use of CDR data in accordance with rule 4.3A:

(i) the principal will:

(A) make any appropriate consumer data request; and

(B) disclose the relevant CDR data to the representative; and

(ii) the representative will use the CDR data to provide the relevant goods or services to the CDR consumer; and

(iii) the representative may disclose the CDR data in accordance with a disclosure consent; and

(b) the representative must not enter into another CDR representative arrangement; and

(c) the representative must not engage a person as the provider in a CDR outsourcing arrangement; and

(d) the representative is required to comply with the following requirements in relation to any service data:

(i) in holding, using or disclosing the service data, the representative must comply with:

(A) section 52EE of the Act (privacy safeguard 2);

(B) section 52EG of the Act (privacy safeguard 4);

(C) subsection 56EN(2) of the Act (privacy safeguard 11);

(D) section 56EO of the Act (privacy safeguard 12); and

(E) subsection 56EP(2) of the Act (privacy safeguard 13);

as if it were the principal;

(ii) the representative must take the steps in Schedule 2 to protect the service data as if it were the principal; and

(iii) the representative must not use or disclose the service data other than in accordance with a contract with the principal;

41589883

Authorised Version F2021L01392 registered 05/10/2021

(iv) the representative must, when so directed by the principal, do any of the following:

(A) delete any service data that it holds in accordance with the CDR data deletion process;

(B) provide, to the principal, records of any deletion that are required to be made under the CDR data deletion process; and

(e) the representative is required to adopt and comply with the principal's CDR policy in relation to the service data; and

(f) the representative is required to comply with sections 56EK and 56EL of the Act (Privacy safeguards 8 and 9) as if it were an accredited data recipient; and

(g) the provisions of the arrangement for the purposes of paragraph (a) do not operate unless the details of the representative have been entered on the Register of Accredited Persons.

Note: See rule 1.18 for the definition of "CDR data deletion process".

(3) For these rules, the ***service data*** in relation to a CDR representative arrangement consists of any CDR data that:

(a) was disclosed to the CDR representative for the purposes of the arrangement; or

(b) directly or indirectly derives from such CDR data.

5 Rule 1.10A

Add at the end:

Consents in relation to CDR representatives

(4) For an accredited person with a CDR representative, a consent given by a CDR consumer under these rules to the CDR representative for the accredited person to collect particular CDR data from a CDR participant for that CDR data and disclose it to the CDR representative is also a ***collection consent***.

(5) In this rule, a reference to an accredited data recipient of particular CDR data includes a reference to a CDR representative that holds the CDR data as service data.

6 Rule 1.14

At the end. add:

Dashboard in relation to CDR representative

(5) Where a CDR principal makes a consumer data request at the request of a CDR representative, it may arrange for the CDR representative to provide the consumer dashboard on its behalf.

7 After rule 1.16

Insert:

41589883

Authorised Version F2021L01392 registered 05/10/2021

1.16A Obligations relating to CDR representative arrangements

(1) If an accredited person is the principal in a CDR representative arrangement, it must ensure that the CDR representative complies with its requirements under the arrangement.

(2) The accredited person breaches this subrule if the CDR representative fails to comply with a required provision of the CDR representative arrangement.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) For this rule, a provision of a CDR representative arrangement is a ***required provision*** if the arrangement would cease to be a CDR arrangement under subrule 1.10AA(2) if the provision were removed.

8 Rule 4.1 (second boxed paragraph)

After "must have first asked the accredited person", insert ", or a CDR representative of the accredited person,".

9 After subrule 4.3(2)

Insert:

(2A) If a CDR consumer has given a collection consent requested under subrule (2) in relation to CDR data, and whether or not the CDR data has yet been collected, the accredited person may also ask the consumer to give a disclosure consent in relation to the CDR data.

10 After rule 4.3

Insert:

4.3A Request for CDR principal to seek to collect CDR data on behalf of CDR representative

(1) This rule applies if:
  (a) a CDR consumer requests a CDR representative to provide goods or services to the CDR consumer or to another person; and
  (b) the CDR representative needs to:
    (i) request its CDR principal to collect the CDR consumer's CDR data from a CDR participant under these rules; and
    (ii) use it in order to provide those goods or services.

(2) The CDR representative may, in accordance with Division 4.3, ask the CDR consumer to give:
  (a) a collection consent for the CDR principal to collect their CDR data from the CDR participant; and
  (b) a use consent for:
    (i) the CDR principal to disclose that data to the CDR representative; and

41589883

Authorised Version F2021L01392 registered 05/10/2021

(ii) for the CDR representative to use it in order to provide those goods or services.

Note 1: In order to provide goods or services in accordance with the CDR consumer's request, it might be necessary for the accredited person to request CDR data from more than 1 CDR participant.

Note 2: The CDR data may be collected and used only in accordance with the data minimisation principle: see rule 1.8.

(3) If a CDR consumer has given a collection consent requested under subrule (2) in relation to CDR data, and whether or not the CDR data has yet been collected, the CDR representative may also ask the consumer to give a disclosure consent in relation to the CDR data.

Note 1: In order to provide goods or services in accordance with the CDR consumer's request, it might be necessary for the accredited person to request CDR data from more than 1 CDR participant.

Note 2: The CDR data may be collected and used only in accordance with the data minimisation principle: see rule 1.8.

(4) In giving the consents, the CDR consumer gives the CDR principal a ***valid*** request to seek to collect that CDR data from the CDR participant.

Note: If an accredited person seeks to collect CDR data under this Part without a valid request, it will contravene privacy safeguard 3 (a civil penalty provision under the Act): see section 56EF of the Act.

(5) The request ceases to be ***valid*** if the collection consent is withdrawn.

Note: So long as the use consent is not also withdrawn, the CDR principal could continue to disclose CDR data it had already collected to the CDR representative, and the CDR representative could use it in order to provide the requested goods or services. However, the notification requirement of rule 4.18A would apply.

4.3B Consumer data requests by accredited persons to CDR representatives

Note: Subrule (1) allows an accredited person to make a consumer data request to a CDR representative as if the latter were also an accredited person.

Subrule (2) allows a CDR representative that receives such a consumer data request to obtain a disclosure consent from the customer. Under paragraphs 7.5(1)(g) and (h), the CDR representative is then able to disclose the requested data.

Application of rule 4.7A to CDR representative holding service data

(1) Rule 4.7A applies in relation to a CDR representative that holds service data as if:

(a) a reference to CDR data were a reference to CDR data included in the service data; and

(b) a reference to an accredited data recipient were a reference to the CDR representative.

41589883

Authorised Version F2021L01392 registered 05/10/2021

Application of rule 4.7B to CDR representative receiving request for service data

(2) Rule 4.7B applies in relation to a CDR representative that receives, or reasonably anticipates receiving, a consumer data request under rule 4.7A as applied by subrule (1), as if:

(i) a reference to an accredited data recipient were a reference to the CDR participant; and

(ii) a reference to Division 4.3 were a reference to Division 4.3 as modified by rule 4.3C.

4.3C Modifications of Division 4.3 in relation to CDR representative

(1) The CDR principal must ensure that, when the CDR representative asks for the CDR consumer's consents, it does so in accordance with Division 4.3, applied with the following modifications:

(a) replace references to the accredited person with references to the CDR representative, except in the following (the ***exceptional provisions***):

(i) Subdivision 4.3.2B; and

(ii) Subdivision 4.3.5, other than paragraph 4.18(2)(c); and

(iii) subrule 4.14(1A); and

(b) in the exceptional provisions, replace references to the accredited person with references to the CDR principal;

(c) replace references to the goods and services provided by the accredited person with references to the goods or services provided by the CDR representative;

(d) replace references to the consumer dashboard provided by the accredited person with references to the consumer dashboard provided by the CDR principal;

Note: The consumer dashboard may in practice be provided by the CDR representative on the CDR principal's behalf—see subrule 1.14(5).

(e) replace references to the accredited person's CDR policy with references to the CDR principal's CDR policy;

(f) replace references to an outsourced service provider of the accredited person with references to an outsourced service provider of the CDR principal;

(g) replace subrule 4.11(1A) with the following:

"(1A) A CDR representative must not ask a CDR consumer to give a disclosure consent for disclosure of CDR data by the CDR representative unless the consumer has already given the collection and use consents required for the data to be collected by the CDR principal and disclosed to and used by CDR representative.";

(h) omit paragraph 4.11(3)(b);

(i) replace paragraph 4.11(3)(i) with the following:

"(i) the fact that the person is a CDR representative and that the CDR data will be collected by its CDR principal at its request;

41589883

Authorised Version F2021L01392 registered 05/10/2021

(j) if the CDR representative is not located in Australia—the country in which it is located;

(k) the CDR principal's name; and

(l) the CDR principal's accreditation number; and

(m) a link to the principal's CDR policy; and

(n) a statement that the CDR consumer can obtain further information about such collections or disclosures from the CDR principal's CDR policy if desired.";

(ia) omit subrule 4.14(1B);

(j) replace subrules 4.14(1C) and (2) with the following:

"(1C) If a CDR principal becomes a data holder, rather than an accredited data recipient, of particular CDR data as a result of subsection 56AJ(4) of the Act, all of the CDR representative's consents given under these rules that relate to that CDR data expire.

"(2) If a CDR principal's accreditation is revoked or surrendered in accordance with rule 5.17, all of the consents of any CDR representative expire when the revocation or surrender takes effect.";

(k) replace subrule 4.16(2) with the following:

"(2) The CDR consumer may make the election:

(a) by communicating it to the CDR principal or CDR representative in writing; or

(b) by using the CDR principal's consumer dashboard.";

(l) add the following rule to Subdivision 4.3.5:

"***4.20B Application of Subdivision to CDR principal and CDR representative***

Where an accredited person who is a CDR principal is required under this Subdivision to give a notice to a CDR consumer in relation to a consumer data request made at the request of a CDR representative, the notice may be given through the CDR representative.".

(2) The accredited person breaches this subrule if the CDR representative fails to comply with a provision of Division 4.3 as modified by subrule (1).

Note: This subrule is a civil penalty provision (see rule 9.8).

11 Paragraph 4.4(1)(a)

After "rule 4.3", insert "or 4.3A".

12 Paragraph 4.7A(1)(a)

After "rule 4.3", insert "or 4.3A".

13 Subrule 4.11(1A)

Repeal.

14 Rule 5.14

At the end, add:

CDR Principals

(3) An accredited person that enters into a CDR representative arrangement as the principal must notify the Data Recipient Accreditor that they have done so as soon as practicable, but no later than 5 business days after the event.

(4) The notification must include the following:
- (a) the date the arrangement was entered into;
- (b) the name and address of the CDR representative;
- (c) the ABN of the CDR representative or, if it is a foreign entity, another unique business identifier;
- (d) the names and contact details of the directors or any persons responsible for the CDR representative;
- (e) the nature of any goods and services to be provided by CDR representative using CDR data.

(5) An accredited person that is the principal in a CDR representative arrangement must notify the Data Recipient Accreditor if the arrangement terminates or otherwise ends as soon as practicable, but no later than 5 business days after the event.

15 Before paragraph 5.24(c)

Insert:

(bc) the name, ABN and business address of any CDR representative;

16 Before paragraph 7.2(4)(b)

Insert:

(ac) include a list of the CDR representatives of the accredited data recipient; and

(ad) for each CDR representative—include the nature of the goods and services that the CDR representative provides to customers using CDR data;

17 Subrule 7.2(8)

After "by means of which the CDR participant", insert ", or a CDR representative of the CDR participant,".

18 Rule 7.3

At the beginning, insert "(1)", at the end add:

(2) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EE of the Act in relation to service data of a CDR consumer as if it were an accredited person.

41589883

Authorised Version F2021L01392 registered 05/10/2021

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(3) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

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

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EG of the Act in relation to service data of a CDR consumer as if;

(a) it were an accredited person; and

(b) it had collected the service data.

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

19 Subrule 7.5(1)

At the end, add:

;

(h) where the accredited data recipient is a CDR principal—disclosing the CDR data to a CDR representative for the purposes of a use or disclosure by the CDR representative that would be a permitted use or disclosure under paragraphs (a) to (ca) or paragraph (e) if the CDR representative were an accredited data recipient that had collected the CDR data under the consumer data request.

20 Subrule 7.5(3)

At the end, add:

;

(d) where the accredited data recipient is a CDR principal—disclosing the CDR data to a CDR representative for the purposes of a use or disclosure by the CDR representative that would be a permitted use or disclosure under paragraph (a) or (b) if the CDR representative were an accredited data recipient that had collected the CDR data under the consumer data request.

21 Subrule 7.6(2), note

Substitute:

Note: See rule 1.10AA for the definition of "service data" in relation to a CDR outsourcing arrangement.

41589883

Authorised Version F2021L01392 registered 05/10/2021

22 Rule 7.6

At the end, add:

(4) For this rule:

(a) any use or disclosure of service data by a CDR representative is taken to have been by the CDR principal; and

(b) it is irrelevant whether the use or disclosure is in accordance with the CDR representative arrangement.

Note: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

23 After rule 7.8

Insert:

7.8A Rule relating to privacy safeguards 8 and 9—failure by CDR representative to comply with safeguards

Privacy safeguard 8—overseas disclosure

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EK of the Act in relation to service data of a CDR consumer as if it were an accredited data recipient of the service data.

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

Privacy safeguard 9—government related identifiers

(2) A CDR principal breaches this subrule if its CDR representative fails to comply with section 56EL of the Act in relation to service data of a CDR consumer as if it were an accredited data recipient of the service data.

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

24 Rule 7.9

At the end, add:

(5) For this rule, where an accredited data recipient is a CDR principal, a disclosure of service data by a CDR representative is taken to be a disclosure by the CDR principal.

25 After rule 7.10

Insert:

41589883

Authorised Version F2021L01392 registered 05/10/2021

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

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with subsection 56EN(2) of the Act in relation to service data of a CDR consumer as if it were an accredited person.

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

26 Rule 7.11

At the beginning, insert "(1)", at the end add:

(2) For this rule, where an accredited data recipient is a CDR principal, a failure by a CDR representative to comply with Schedule 2 in relation to service data is taken to be a failure by the CDR principal.

27 Paragraph 7.12(2)(b)

After "outsourced service provider", insert "or CDR representative":

28 Rule 7.12

At the end, add:

(3) For this rule, where an accredited data recipient is a CDR principal, a failure by a CDR representative to comply with subsection 56EO(2) of the Act in relation to service data as if it were a CDR entity is taken to be a failure by the CDR principal.

29 After rule 7.15

Insert:

7.16 Rule relating to privacy safeguard 13—correction of data—CDR representative

(1) A CDR principal breaches this subrule if its CDR representative fails to comply with subsection 56EP(2) of the Act in relation to service data of a CDR consumer as if it were an accredited person.

Note 1: See rule 1.10AA for the definition of "service data" in relation to a CDR representative arrangement.

Note 2: This subrule is a civil penalty provision (see rule 9.8).

41589883

Authorised Version F2021L01392 registered 05/10/2021

(2) For subrule (2), it is irrelevant whether the action of the CDR representative in relation to the service data is in accordance with the CDR representative arrangement.

30 After subrule 9.3(2)

Insert:

Records to be kept and maintained—CDR principal

(2A) An accredited data recipient that is a CDR principal must keep and maintain records that record and explain the following in relation to each CDR representative:

(a) the CDR representative arrangement;

(b) the management of data by the CDR representative;

(c) steps taken to ensure that the CDR representative complies with their requirements under the arrangement;

(d) all consents obtained by the CDR representative, including, if applicable, the uses of the CDR data that the CDR consumer has consented to under any use consents;

(e) amendments to or withdrawals of consents by CDR consumers;

(f) notifications of withdrawals of authorisations received from data holders;

(g) CDR complaint data;

(h) collections of CDR data under these rules;

(i) elections to delete and withdrawals of those elections;

(j) the use of CDR data by the CDR representative;

(k) the processes by which the CDR representative asks CDR consumers for their consent and for an amendment to their consent, including a video of each process;

(l) if CDR data was de-identified in accordance with a consent referred to in paragraph 4.11(3)(e):

(i) how the data was de-identified; and

(ii) how the CDR representative used the de-identified data; and

(iii) if the CDR representative disclosed (by sale or otherwise) the de-identified data to another person as referred to in paragraph 4.15(b):

(A) to whom the data was so disclosed; and

(B) why the data was so disclosed;

(iv) if the use is for general research—records of any additional benefit to be provided to the CDR consumer for consenting to the use;

(m) records that are required to be made for the purposes of the CDR data de-identification process when applied as part of privacy safeguard 12;

(n) records of any matters that are required to be retained under Schedule 2 to these rules;

41589883

Authorised Version F2021L01392 registered 05/10/2021

(o) any terms and conditions on which the CDR representative offers goods or services where the CDR representative collects or uses, or discloses to an accredited person, CDR data in order to provide the good or service.

Note: For paragraph (k), see section 56EO of the Act and rule 7.12.

Civil penalty:

(a) for an individual—$50,000; and

(b) for a body corporate—$250,000.

31 After subrule 9.4(2)

Insert:

Reports that must be prepared—CDR principal

(2A) An accredited data recipient that is a CDR principal must prepare a report for each reporting period that is in the form approved by the Commission for the purposes of this rule and, in relation to each CDR representative:

(a) summarises the CDR complaint data that relates to that reporting period; and

(b) describes any goods or services that the CDR representative offers to CDR consumers using CDR data that were not:

(i) described in the relevant application to be a CDR representative; or

(ii) previously included in a report prepared under this rule; and

(c) in relation to any good or service that is required to be described under paragraph (b):

(i) describes the CDR data that is needed in order to offer the good or service to CDR consumers; and

(ii) explains why that data is needed in order to offer the good or service to CDR consumers; and

(d) describes any material changes that have been made to any goods or services offered by the CDR representative since the previous reporting period, including any changes to the matters referred to in paragraph (b); and

(e) sets out the following:

(i) the number of consumer data requests made by the accredited data recipient on behalf of the CDR representative during the reporting period;

(ii) the number of consumer data requests made by the CDR representative to the CDR principal during the reporting period;

(iii) the proportion of CDR consumers who, at the date of the report, had exercised the election to delete, by reference to each brand of the CDR representative;

(iv) the total number of CDR consumers the CDR representative provided goods or services to using CDR data during the reporting period.

Civil penalty:

(a) for an individual—$50,000; and
(b) for a body corporate—$250,000.

32 Paragraph 9.4(4)(b)

After "subrule (2)", insert "or 2A".

41589883

Schedule 3—Amendments relating to trusted advisers and insights

Note: This Schedule commences on the day after this instrument is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

CDR insight, in relation to an insight disclosure consent, means the CDR data subject to the consent.

insight disclosure consent has the meaning given by rule 1.10A.

TA disclosure consent has the meaning given by rule 1.10A.

trusted adviser has the meaning given by rule 1.10C.

2 Paragraph 1.10A(1)(c)(ii)

Omit "; and", substitute:

; or

(iii) to a trusted adviser of the CDR consumer (a ***TA disclosure consent***); or

(iv) to a specified person in accordance with an insight disclosure consent; and

3 Subrule 1.10A(2)

At the end, add:

;

(f) TA disclosure consents;

(g) insight disclosure consents.

4 After subrule 1.10A(2)

Insert:

(3) For these rules, an ***insight disclosure consent*** in relation to particular CDR data of a CDR consumer held by an accredited data recipient is a consent given by the CDR consumer under these rules that:

(a) authorises the accredited data recipient to disclose the CDR data to a specified person for one or more of the following purposes:

(i) verifying the consumer's identity;

(ii) verifying the consumer's account balance;

(iii) verifying the details of credits to or debits from the consumer's accounts; but

41589883

(b) where the CDR data relates to more than one transaction—does not authorise the accredited data recipient to disclose an amount or date in relation to any individual transaction.

5 After rule 1.10A

Insert:

1.10C Trusted advisers

(1) An accredited person may invite a CDR consumer to nominate one or more persons as ***trusted advisers*** of the CDR consumer for the purposes of this rule.

(2) A trusted adviser must belong to one of the following classes:
  (a) qualified accountants within the meaning of the *Corporations Act 2001*;
  (b) persons who are admitted to the legal profession (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession;
  (c) registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*;
  (d) financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*;
  (e) relevant providers within the meaning of the *Corporations Act 2001* other than:
    (i) provisional relevant providers under section 910A of that Act; and
    (ii) limited-service time-sharing advisers under section 910A of that Act;
  (f) mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

(3) Where the accredited person has taken reasonable steps to confirm that a person nominated as a trusted adviser was, and remains, a member of a class mentioned in subrule (2), the person is taken to be a member of that class for the purposes of this rule.

(4) The accredited person must not make:
  (a) the nomination of a trusted adviser; or
  (b) the nomination of a particular person as a trusted adviser; or
  (c) the giving of a TA disclosure consent;

a condition for supply of the goods or services requested by the CDR consumer.

6 Paragraph 1.14(1)(b)

After "subrule (3)", insert "and the information specified in subrule (3A)".

7 After paragraph 1.14(3)(e)

Insert:

(ea) for an insight disclosure consent—a description of the CDR insight and to whom it was disclosed;

41589883

Authorised Version F2021L01392 registered 05/10/2021

8 After subrule 1.14(3)

Insert:

(3A) For paragraph (1)(b), the other information is:

(a) a statement that the CDR consumer is entitled to request further records in accordance with rule 9.5; and

(b) information about how to make such a request.

9 After paragraph 4.11(3)(c)

Insert:

(ca) in the case of an insight disclosure consent—an explanation of the CDR insight that will make clear to the CDR consumer what the CDR insight would reveal or describe;

10 Rule 7.5A

At the beginning, insert "(1)", at the end add:

(2) Despite paragraph 7.5(1)(ca), disclosure of CDR data to a trusted adviser under a TA disclosure consent is not a ***permitted use or disclosure*** until the earlier of the following:

(a) 1 February 2022;

(b) the day the Data Standards Chair makes the data standard about the matter referred to in subparagraph 8.11(1)(c)(iv).

(3) Despite paragraph 7.5(1)(ca), disclosure of a CDR insight under an insight disclosure consent is not a ***permitted use or disclosure*** until the earlier of the following:

(a) 1 February 2022;

(b) the day the Data Standards Chair makes the data standard about the matters referred to in subrule 8.11(1A).

(4) Despite paragraph 7.5(1)(ca), disclosure of a CDR insight under an insight disclosure consent is not a ***permitted use or disclosure*** if the CDR insight includes or reveals sensitive information within the meaning of the *Privacy Act 1988*.

11 After rule 7.9(2)

Insert:

(3) For subsection 56EM(2) of the Act, an accredited data recipient that discloses CDR data to a trusted adviser must, as soon as practicable, update each consumer dashboard that relates to the request to indicate:

(a) what CDR data was disclosed; and

(b) when the CDR data was disclosed; and

(c) the trusted adviser.

41589883

Authorised Version F2021L01392 registered 05/10/2021

(4) For subsection 56EM(2) of the Act, an accredited data recipient that discloses a CDR insight must, as soon as practicable, update each consumer dashboard that relates to the request to indicate:
  (a) what CDR data was disclosed; and
  (b) when the CDR data was disclosed; and
  (c) the person to whom it was disclosed.

12 After paragraph 8.11(1)(c)(iii)

Insert:

and

(iv) consumer experience data standards for disclosure of CDR data to trusted advisers;

(v) consumer experience data standards for disclosure of CDR insights;

13 After subrule 8.11(1)

Insert:

(1A) The standards for the purposes of paragraph (1)(a)(ii) that relate to obtaining insight disclosure consents must include provisions that cover the following:
  (a) how the accredited person can meet the requirement to explain a CDR insight in accordance with paragraph 4.11(3)(ca);
  (b) ensuring that the CDR consumer is made aware that their data will leave the CDR system when it is disclosed.

14 After paragraph 9.3(2)(ea)

Insert:

(eb) disclosures of CDR data to trusted advisers, and trusted advisers to whom CDR data was disclosed;

(ec) any steps taken for the purposes of subrule 1.10C(3) to confirm that a trusted adviser is a member of a class of trusted advisers;

(ed) disclosures of CDR insights, including a copy of each CDR insight disclosed, to whom it was disclosed and when;

15 Paragraph 9.4(2)(f)

At the end, add:

;

(vi) the number of consents received from CDR consumers during the reporting period to disclose CDR data to trusted advisers;

(vii) for each class of trusted advisers—the number of trusted advisers to whom CDR data was disclosed during the reporting period;

(viii) the number of insight disclosure consents received from CDR consumers during the reporting period.

Schedule 4—Amendments relating to joint accounts

Note: This Schedule commences on the day after this instrument is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.7 (1)

Insert in the appropriate alphabetical position:

co-approval option has the meaning given by rule 4A.5.

disclosure option has the meaning given by rule 4A.5.

disclosure option management service has the meaning given by rule 4A.6.

joint account:

(a) means a joint account with a data holder for which there are 2 or more joint account holders, each of which is an individual who:

(i) so far as the data holder is aware, is acting in their own capacity and not on behalf of another person; and

(ii) is eligible in relation to the data holder; but

(b) does not include a partnership account with a data holder.

non-disclosure option has the meaning given by rule 4A.5.

ordinary means of contacting an account holder by a data holder means:

(a) if the data holder has agreed with the account holder on a particular means of contacting the account holder for the purposes of the relevant provision—that means; and

(b) otherwise—the default means by which the data holder contacts the account holder in relation to the account.

pre-approval option has the meaning given by rule 4A.5.

2 Subrule 1.7 (1)—definition of *consumer dashboard*

Omit "rule 1.15", substitute "rules 1.15 and 4A.13".

3 Subrule 1.14(1)

Omit all words up to and including "that:", substitute:

Subject to subrule (5), an accredited person must provide each eligible CDR consumer on whose behalf the accredited person makes a consumer data request with an online service that:

4 Paragraph 1.14(1)(a)

Substitute:

(a) can be used by the CDR consumer to manage:

(i) such requests; and

41589883

Authorised Version F2021L01392 registered 05/10/2021

(ii) associated consents; and

5 Subparagraph 1.14(1)(c)(i)

Omit "a CDR consumer", substitute "the CDR consumer".

6 Subrule 1.15(2), note

Substitute:

Note: If the consumer data request relates to a joint account, there may be an obligation to provide all joint account holders with consumer dashboards: see rule 4A.13.

7 Rule 3.1 (second last boxed paragraph)

Substitute:

> Special rules apply to joint accounts with 2 or more individual joint account holders. These are set out in Part 4A.

8 Subrule 3.4(3), note 2

Substitute:

Note 2: For a request that relates to a joint account, see rules 4A.10 and 4A.15 for additional circumstances in which data relating to the joint account might not be disclosed under these rules.

9 Paragraph 3.5(1)(a)

After "prevent physical", insert ", psychological".

10 Rule 4.1 (second last boxed paragraph)

Substitute:

> Special rules apply to joint accounts with 2 or more individual joint account holders. These are set out in Part 4A.

11 Subrule 4.6(2), note 2

Substitute:

Note 2: For requests that relate to joint accounts, additional requirements need to be met in order for the data holder to be authorised to disclose requested CDR data that relates to the joint account: see Part 4A.

12 Subrule 4.6(4), note 2

Substitute:

Note 2: For requests that relate to joint accounts, additional requirements need to be met in order for the data holder to be authorised to disclose requested CDR data that relates to the joint account: see Part 4A.

41589883

Authorised Version F2021L01392 registered 05/10/2021

13 Paragraph 4.7(1)(a)

After "prevent physical", insert ", psychological".

14 After Part 4

Insert:

Part 4A—Joint accounts

Note: When this Part commences, it will be subject to transitional provisions that operate until July 2022.

Division 4A.1—Preliminary

4A.1 Purpose of Part

Special rules apply in relation to consumer data requests under Part 4 under which there is a request for disclosure of CDR data that relates to one or more joint accounts. This Part sets out those rules.

4A.2 Simplified outline of this Part

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

- the three disclosure options, with the default option being the pre-approval option; and
- an obligation for data holders to provide a service (a disclosure option management service) for all joint accounts to which this Part applies through which joint account holders can change the disclosure option that applies to the account, or propose a change to the other account holders; and
- 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.

Any joint account holder can choose that the non-disclosure option will apply.

If the pre-approval option applies, any joint account holder can choose that the co-approval option will apply.

A change from the non-disclosure option to another option, or a change from the co-approval option to the pre-approval option, requires the agreement of all the joint account holders.

When an accredited person makes a consumer data request under Part 4 on behalf of a CDR consumer, and the request includes CDR data relating to one or

41589883

Authorised Version F2021L01392 registered 05/10/2021

more joint accounts of which the CDR consumer is a joint account holder, Division 4A.3 deals with how the request is processed.

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.

4A.3 Interpretation

For this Part, in relation to a consumer data request to a data holder under Part 4 where the CDR data requested includes CDR data that relates to a joint account:

(a) the ***requester*** is the person on whose behalf the consumer data request was made; and

(b) the ***relevant account holders*** are:

(i) if the requester is a secondary user—all joint account holders; and

(ii) if the requester is a joint account holder—the other joint account holders; and

(c) the ***joint account data*** is the CDR data relating to the joint account that was the subject of the request.

Note: The CDR data that can be requested on behalf a CDR consumer is governed by the relevant general provisions in the sector Schedules, so that, for example, customer data that relates to another joint account holder cannot be covered by a consumer data request (see paragraphs 3.2(3)(b) of Schedule 3 and 3.2(3)(b) of Schedule 4).

Division 4A.2— Disclosure options

4A.4 Simplified outline of this Division

This Division 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 option is the pre-approval option. If this option applies, when the data holder receives a consumer data request, the other account holders are treated as having approved disclosing the data relating to the joint account in response to that request. However, the other account holders can withdraw this presumed approval in relation to that request at any time.

Another option is the non-disclosure option. If this option applies, joint account data cannot be disclosed under these rules.

The third option is the co-approval option. If this option applies, joint account data can be disclosed under these rules 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.

The process for changing the disclosure option is set out in this Division.

For each joint account, a data holder must offer a disclosure option management service that can be used by joint account holders to select and manage these disclosure options.

However, the data holder will not be liable for a failure to comply with this Part if it considered that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse to any person.

4A.5 Disclosure options for joint accounts

Disclosure options

(1) Disclosure of joint account data may be authorised only as permitted by the ***disclosure option*** that applies to the joint account. This may be any of the following:
   (a) the ***pre-approval option***, under which joint account data may be disclosed in response to a valid consumer data request on the authorisation of the requester without the approval of the relevant account holders;
   (b) the ***co-approval option***, under which joint account data may be disclosed in response to a valid consumer data request only after:
      (i) the requester has authorised the disclosure; and
      (ii) each of the relevant joint account holders has approved the disclosure;
   (c) the ***non-disclosure option***, under which joint account data may not be disclosed even in response to a valid consumer data request.

(2) The data holder must provide for the pre-approval and non-disclosure options to be available for a joint account.

(3) The data holder may provide for the co-approval option to be available for a joint account.

(4) For the purposes of rule 4A.12, where the pre-approval option applies to a joint account and the requester authorises the disclosure of joint account data in response to a valid consumer data request:
   (a) each relevant account holder is taken to have approved the disclosure; and
   (b) if an approval is withdrawn, the joint account data may not be disclosed despite the authorisation.

Default option

(5) Unless a sector Schedule provides otherwise, the pre-approval option applies to a joint account by default.

(6) The disclosure option that applies to a joint account may be changed in accordance with rule 4A.7 or 4A.8.

4A.6 Obligation to provide disclosure option management service

Obligation to provide disclosure option management service

(1) For each joint account to which this Part applies, the data holder must provide a service to each joint account holder that allows the joint account holder to:
   (a) change the disclosure option that applies to the account in accordance with rule 4A.7; and
   (b) propose a change in the disclosure option to the other joint account holders in accordance with rule 4A.8; and
   (c) respond to a proposal by another joint account holder to change the disclosure option.

Note: This subrule is a civil penalty provision (see rule 9.8).

(2) Such a service is a ***disclosure option management service***.

Requirements for disclosure option management service

(3) The service must be provided online and, if there is a data holder's consumer dashboard for a joint account holder, may be included in the dashboard.

(4) The service may, but need not, also be provided other than online.

(5) The service must give effect to a change in the disclosure option as soon as practicable.

(6) The service must not do any of the following in relation to the processes that it provides for changing or proposing to change the disclosure option that applies to the joint account, or responding to such a proposal (the ***processes***):
   (a) add any requirements to the processes beyond those specified in the data standards and these rules;
   (b) offer additional or alternative services as part of the processes;
   (c) include or refer to other documents, or provide any other information, so as to reduce comprehensibility;
   (d) offer any pre-selected options.

(7) The service must indicate to the joint account holder which disclosure option currently applies.

(8) The service must be in accordance with the data standards.

4A.7 Changing to a more restrictive disclosure option

(1) A joint account holder may at any time choose that the non-disclosure option will apply to the joint account, using the disclosure option management service.

41589883

Authorised Version F2021L01392 registered 05/10/2021

(2) If the pre-approval option applies to a joint account, a joint account holder may at any time choose that the co-approval option will apply to the joint account, using the disclosure option management service.

(3) If a joint account holder (***account holder A***) changes the disclosure option that applies to the account in accordance with this rule, the data holder must, as soon as practicable through its ordinary means of contacting the other joint account holders:

(a) explain to each of them what the consumer data right is; and

(b) inform them which disclosure option previously applied to the account; and

(c) inform them that account holder A has changed the disclosure option, and of the disclosure option that now applies; and

(d) explain to them the mechanisms for changing the disclosure option again.

Note: This subrule is a civil penalty provision (see rule 9.8).

4A.8 Obtaining agreement on change to a less restrictive disclosure option

Application of rule

(1) This rule applies in relation to a particular joint account if:

(a) the non-disclosure option applies to the account, and a joint account holder (***account holder A***) proposes, using the disclosure option management service, to change to the co-approval or pre-approval disclosure option; or

(b) the co-approval option applies to the account, and a joint account holder (***account holder A***) proposes, using the disclosure option management service, to change to the pre-approval option.

Inviting other account holders to respond to proposal

(2) The data holder must, as soon as practicable through its ordinary means of contacting the other joint account holders:

(a) explain to each of them what the consumer data right is; and

(b) inform them which disclosure option currently applies to the account; and

(c) inform them that account holder A has proposed that the co-approval or pre-approval option apply to the account, as the case may be; and

(d) explain to them that this change requires the agreement of all account holders; and

(e) explain to them any alternative options for change that are available and how they can be made; and

(f) invite them to either agree to or reject the proposal within a specified period.

Note: This subrule is a civil penalty provision (see rule 9.8).

(3) At the end of the specified period, the data holder must, as soon as practicable through its ordinary means of contacting the joint account holders, inform them whether:

41589883

(a) all the joint account holders have approved the change, and as a result the new disclosure option applies to the joint account; or

(b) not all the joint account holders have approved the change, and as a result the disclosure option is unchanged.

Note: This subrule is a civil penalty provision (see rule 9.8).

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

Subdivision 4A.3.1—Preliminary

4A.9 Application of Division

(1) This Division applies in relation to a consumer data request to a data holder under Part 4 where the CDR data requested includes joint account data.

(2) If the CDR data requested includes joint account data in relation to more than one joint account, this Division applies separately in relation to each such joint account.

(3) In this Division a reference to a consumer data request is a reference to the consumer data request only to the extent that it relates to a particular joint account.

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

4A.10 How data holder is to deal with a consumer data request

(1) This rule applies when the data holder receives a consumer data request to which this Division applies.

Note: Under rule 4A.5, data holders are required to offer the pre-approval disclosure option, which applies by default. Data holders may, but are not required to, offer the co-approval option.

Pre-approval option

(2) If the pre-approval option applies to the joint account, rules 4.5 to 4.7 apply subject to subrule (3).

(3) If a relevant account holder has withdrawn their approval using their consumer dashboard, the data holder must not disclose any, or any further, requested CDR data.

Co-approval option

(4) If the co-approval option applies to the joint account, the data holder must, subject to subrule (5):

(a) ask the requester for authorisation in accordance with rule 4.5 and Division 4.4; and

41589883

Authorised Version F2021L01392 registered 05/10/2021

(b) if the authorisation is given, invite the approval of the relevant account holders in accordance with rule 4A.11; and

(c) if all the relevant account holders give their approval, or are taken to have given their approval, comply with rules 4.6 to 4.7.

Note: The data holder must provide each relevant account holder with a consumer dashboard in accordance with rule 4A.13.

(5) If a relevant account holder who approved the disclosure in accordance with rule 4A.11 within the time specified has withdrawn the approval using their consumer dashboard, the data holder must not disclose any, or any further, requested CDR data.

Non-disclosure option

(6) If the non-disclosure option applies to the joint account, the data holder must refuse to disclose the requested CDR data.

4A.11 Asking relevant account holders for approval to disclose joint account data

For the purposes of paragraph 4A.10(4)(b), the data holder must, through its ordinary means of contacting each relevant account holder:

(a) indicate that an accredited person has requested disclosure of CDR data that relates to the joint account on behalf of the requester; and

(b) indicate that:

(i) the requester has authorised, under Division 4.4, the disclosure of the joint account data; and

(ii) a co-approval option applies to the joint account; and

(c) indicate the matters referred to in paragraphs 4.23(1)(a), (b), (c), (d) and (e) so far as they relate to the request; and

(d) ask the relevant account holder to approve or not approve disclosure of the joint account data; and

(e) specify the time by which the data holder needs to receive any approval, and inform them that if an approval is not received by that time, the joint account data will not be disclosed; and

(f) inform them that any relevant account holder may, at any time, withdraw the approval using their consumer dashboard; and

(g) indicate what the effect of removing the approval would be.

Note: For removal of an approval, see rule 4A.12.

4A.12 Continuation and removal of approvals

(1) If a relevant account holder:

(a) approves of the disclosure of joint account data in accordance with this Division; or

(b) is taken to have approved of the disclosure under the pre-approval option;

41589883

the approval is taken to apply while the authorisation referred to in paragraph 4A.10(4)(b) is current, unless withdrawn sooner in accordance with this Division.

(2) Any relevant account holder may withdraw an approval given under this Division at any time, using their consumer dashboard.

4A.13 Consumer dashboard for joint account holders

Note: Where this Division applies, the data holder must provide a consumer dashboard for the requester under rule 1.15. Under this rule, in some circumstances, the data holder must also provide a consumer dashboard for each relevant account holder and the dashboards must have additional functionality.

Obligation for data holder to provide relevant account holders with consumer dashboard

(1) Where:

(a) this Division applies in relation to a consumer data request; and

(b) either the co-approval option or the pre-approval option applies, or has applied, to the joint account;

the data holder must provide each relevant account holder with an online service that:

(c) contains the details referred to in paragraph 1.15(1)(b) that relate to the joint account data; and

(d) has a functionality that:

(i) can be used by the relevant account holder to manage approvals in relation to each authorisation to disclose joint account data made by a requester; and

(ii) allows for withdrawal, at any time, of such an approval; and

(iii) is simple and straightforward to use; and

(iv) is prominently displayed; and

(v) as part of the withdrawal process, displays a message relating to the consequences of the withdrawal in accordance with the data standards.

Note: This subrule is a civil penalty provision (see rule 9.8).

(2) Where the data holder already provides a consumer dashboard for the relevant account holder under rule 1.15, the service under subrule (1) must be included in the consumer dashboard.

(3) Where the data holder does not already provide a consumer dashboard for that relevant account holder under rule 1.15, the service under subrule (1) is the data holder's ***consumer dashboard*** for the relevant account holder.

(4) A data holder does not contravene subrule (1) in relation to subparagraphs (1)(d)(iii) and (iv) so long as it takes reasonable steps to ensure that the functionality complies with those subparagraphs.

41589883

Authorised Version F2021L01392 registered 05/10/2021

Common information on consumer dashboard

(5) For paragraph 1.15(1)(d), if a relevant account holder's consumer dashboard contains details of approvals under this Division, the dashboards of the other joint account holders must contain those details.

4A.14 Notification requirements for consumer data requests on joint accounts

(1) For this rule, an ***approval notification*** is a notice given by the data holder:
   (a) to a relevant account holder, to inform them that the requester has given, amended or withdrawn an authorisation, or that the authorisation has expired; or
   (b) to the requester, to inform them that:
      (i) one or more of the relevant account holders has not given their approval for disclosure within the time frame referred to in paragraph 4A.11(e); or
      (ii) a relevant account holder has withdrawn an approval previously given;

   in accordance with the data standards.

(2) The data holder must make the appropriate approval notification to a joint account holder in relation to an event mentioned in subrule (1):
   (a) as soon as practicable after the event occurs, unless the joint account holder has selected an alternative schedule of notifications; and
   (b) through its ordinary means of contacting the joint account holders.

   Note: This subrule is a civil penalty provision (see rule 9.8).

(3) The data holder must, in accordance with any relevant data standards:
   (a) provide for alternative notification schedules (including reducing the frequency of notifications or not receiving notifications); and
   (b) give each joint account holder a means of selecting such an alternative, and of changing a selection.

   Note: This subrule is a civil penalty provision (see rule 9.8).

4A.15 Avoidance of harm

A data holder is not liable under these rules for a failure to comply with this Part if it considered that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse to any person.

15 Subrule 7.9(1), Note 2

Substitute:

Note 2: If a consumer data request is made that relates to a joint account, the other joint account holder's consumer dashboard may not be required to be similarly updated. See clause 4A.13.

41589883

Authorised Version F2021L01392 registered 05/10/2021

16 Schedule 3, clause 1.1, fifth boxed paragraph

Repeal.

17 Schedule 3, clause 1.2, definitions of *joint account* and *joint account management service*

Repeal.

18 Schedule 3, Part 4

Repeal.

41589883

Schedule 5—Amendments relating to staged implementation

Note: This Schedule commences on the day after this instrument is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

1 Schedule 3, subclause 6.4(3)

Substitute:

(3) Where a table cell includes the term ***JAE*** (for "joint accounts excepted"), despite these rules, the data holder is not required to disclose required consumer data about a product that relates to joint accounts.

(4) Where a table cell includes the term ***CODE*** (for "certain other data excepted"), despite these rules, the data holder is not required to disclose required consumer data about a phase 1 product that:

(a) relates to any of the following:

(i) closed accounts;

(ii) direct debits;

(iii) scheduled payments;

(iv) payees; or

(b) is "get account detail" or "get customer detail" data within the meaning of the data standards.

2 Schedule 3, clause 6.6

Substitute:

41589883

6.6 Commencement table

(1) For this Part, the ***commencement table*** is:

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

Schedule 6—Consequential and minor amendments

Note: Items 1,2,3,15,18, and 19 of tis Schedule commences on the day 14 days after this instrument is registered. The other items commence on the day after it is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

1 Paragraph 1.10(2)(a)

Substitute:

(a) the provider will do one or both of the following:

(i) collect CDR data from a CDR participant in accordance with these rules on behalf of the principal;

(ii) provide goods or services to the principal using CDR data that it has collected on behalf of the principal or that has been disclosed to it by the principal; and

2 Subparagraph 1.10(2)(b)(iv)

Repeal.

3 Subrule 1.10(2), note

Substitute:

Note 1: See rule 1.18 for the definition of "CDR data deletion process".

Note 2: For collection of CDR data under subparagraph (2)(a)(i), the principal must be the accredited person on whose behalf the CDR data may be collected under these rules—that is, the provider cannot further outsource collection.

However, the provision of goods and services using the CDR data under subparagraph (2)(a)(ii) can be further outsourced by the provider using another CDR outsourcing arrangement.

4 Subrule 1.15(1)

Omit "the CDR consumer has", substitute "it provides the CDR consumer with".

5 Paragraph 1.15(1)(a)

Omit "the request", substitute "consumer data requests".

6 Paragraph 1.15(1)(d)

Substitute:

(d) contains any other details, and has any other functionality, required by a provision of these rules.

7 Subrule 1.15(1), note 2

Repeal.

8 Subrule 1.15(3)

After "the information is the following", insert "for each authorisation".

41589883

Authorised Version F2021L01392 registered 05/10/2021

9 Subrule 1.16(1), note

Omit "rule", insert "subrule".

10 After subrule 1.17(5)

After "Office of the" insert "Australian".

11 Subrule 4.10(1)(a)(ia)

Repeal.

12 Subparagraph 4.10(2)

Repeal.

13 Subrule 4.16(3)

Substitute:

(3) This rule does not apply if the accredited person:

(i) has a general policy of deleting redundant data; and

(ii) when seeking the consent, informs the CDR consumer that their CDR data will be deleted when it becomes redundant data.

Note: See paragraph 4.17(1)(a).

14 Subparagraph 5.15(a)(vi)

Substitute:

(vi) a notification under paragraph 5.14(1)(c), or subrule 5.14(2), (3) or (5); and

15 Subparagraph 7.2(4)(c)(ii)

After "disclosed to it", insert "or collected by it".

16 Subrule 7.5(2)

Substitute:

(2) However:

(a) a disclosure is not a ***permitted use or disclosure*** unless it is done in accordance with the data standards; and

(b) none of the uses or disclosures of CDR data referred to in subrule 4.12(3) is a ***permitted use or disclosure***.

17 Subrule 7.5(3)

After "CDR consumer's data", insert "by an accredited data recipient".

18 Paragraph 7.6(2)(a)

Omit "provider under", substitute "provider in".

41589883

Authorised Version F2021L01392 registered 05/10/2021

19 Rule 7.6

At the end, add:

(5) For this rule:

(a) any collection of service data by the provider in a CDR outsourcing arrangement is taken to have been by the principal under the arrangement; and

(b) it is irrelevant whether the collection is in accordance with the arrangement.

Note: See rule 1.10AA for the definition of "service data" in relation to a CDR outsourcing arrangement.

20 Subrule 9.5(2)

Substitute:

(2) A CDR consumer may request an accredited data recipient for copies of records relating to the information referred to in:

(a) paragraphs 9.3(2)(a), (b), (c), (d), (e), (ea), (eb), (ec), (ed), (f) and (m); and

(b) paragraphs 9.3(2A)(d), (e), (f), (g), (h), (i) and (o);

that relates to the CDR consumer.

21 Rule 9.8

Substitute:

9.8 Civil penalty provisions

For section 56BL of the Act, the following provisions of these rules are civil penalty provisions (within the meaning of the Regulatory Powers Act):

(a) subrule 1.12(1);
(b) subrule 1.13(1);
(c) subrule 1.14(1);
(d) subrule 1.15(1);
(e) subrule 1.15(5)
(f) subrule 1.15(7)
(g) subrule 1.16(1);
(h) subrule 1.16A(2);
(i) subrule 2.4(2A);
(j) subrule 2.4(3);
(k) rule 2.6;
(l) subrule 3.4(3);
(m) subrule 4.3(5);
(n) subrule 4.3C(2):

41589883

Authorised Version F2021L01392 registered 05/10/2021

(o) subrule 4.4(3);
(p) subrule 4.5(2);
(q) subrule 4.5(3);
(r) subrule 4.6(3);
(s) subrule 4.6(4);
(t) subrule 4.7B(3)
(u) subrule 4.13(2);
(v) subrule 4.18(1);
(w) subrule 4.18A(2);
(x) subrule 4.18B(2);
(y) subrule 4.18B(3);
(z) subrule 4.18C(2);
(aa) rule 4.19;
(bb) subrule 4.20(2);
(cc) subrule 4.22A(1)
(dd) subrule 4.25(2);
(ee) rule 4.27;
(ff) subrule 4.28(2);
(gg) subrule 4A.6(1);
(hh) subrule 4A.7(3);
(ii) subrule 4A.8(2);
(jj) subrule 4A.8(3);
(kk) subrule 4A.13(1);
(ll) subrule 4A.14(2);
(mm) subrule 4A.14(3);
(nn) subrule 5.1B(2);
(oo) subrule 5.1B(3);
(pp) subrule 5.1B(4);
(qq) subrule 5.1B(5);
(rr) subrule 5.12(1);
(ss) rule 5.13;
(tt) subrule 5.14(1);
(uu) subrule 5.23(2);
(vv) subrule 5.23(3);
(ww) subrule 5.23(4);
(xx) subrule 5.31(2);
(yy) rule 6.1;
(zz) rule 6.2;
(aaa) subrule 7.2(4);
(bbb) subrule 7.2(6);
(ccc) subrule 7.2(7);

41589883

(ddd) subrule 7.2(8);
(eee) subrule 7.2(9);
(fff) subrule 7.3(2);
(ggg) subrule 7.3A(1);
(hhh) subrule 7.6(1);
(iii) subrule 7.8A(1);
(jjj) subrule 7.8A(2);
(kkk) subrule 7.10A(1);
(lll) subrule 7.14(1);
(mmm) subrule 7.14(2);
(nnn) subrule 7.16(1);
(ooo) subrule 9.6(4);
(ppp) subrule 9.7(3).

Note: Subrules 2.5(2), 3.5(2), 4.7(3), 5.25(3), 5.25(5), 5.34(4), 9.3(1), 9.3(2), 9.3(2A), 9.3(5), 9.4(1)), 9.4(2) 9.4(2A), 9.4(3), 9.5(4), 9.5(5) and 9.5(6) are also civil penalty provisions within the meaning of the Regulatory Powers Act.

41589883

22 Schedule 2, table in clause 2.2

Substitute:

	Control requirements		Minimum controls	Description of minimum controls
(1)	An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	(a)	Multi-factor authentication or equivalent control	Multi-factor authentication or equivalent control is required for all access to CDR data. Note: This minimum control does not apply to access to CDR data by CDR consumers.
		(b)	Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.
		(c)	Audit logging and monitoring	Critical events are identified, logged and retained to help ensure traceability and accountability of actions. These logs are reviewed regularly to identify irregularities and deviations from expected processing. Note: In relation to retention, see paragraph 9.3(2)(l) of these rules.
		(d)	Access security	Processes, including automatic processes, are implemented to limit unauthorised access to the CDR data environment. At the minimum these include: (a) provision and timely revocation for users who no longer need access; and

	Control requirements		Minimum controls	Description of minimum controls
				(b) monitoring and review of the appropriateness of user access privileges on at least a quarterly basis.
		(e)	Limit physical access	Physical access to facilities where CDR data is stored, hosted or accessed (including server rooms, communications rooms, and premises of business operation) is restricted to authorised individuals.
		(f)	Role based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principle of least necessary privileges and segregation of duties.
		(g)	Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained. Note: In relation to retention, see paragraph 9.3(2)(l) of these rules.
		(h)	Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.
		(i)	Encryption in transit	Implement robust network security controls to help protect data in transit, including: encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice,

	Control requirements		Minimum controls	Description of minimum controls
				implementing processes to audit data access and use, and implementing processes to verify the identity of communications.
(2)	An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	(a)	Encryption	Encryption methods are utilised to secure CDR data at rest by encrypting file systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed-up and retained. Appropriate user authentication controls (consistent with control requirement 1) are in place for access to encryption solutions and cryptographic keys.
		(b)	Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: (a) restricting all access from untrusted networks; and (b) denying all traffic aside from necessary protocols; and (c) restricting access to configuring firewalls, and review configurations on a regular basis.
		(c)	Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.
		(d)	End-user devices	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.
		(e)	Data Segregation	CDR data that is stored or hosted on behalf of an accredited data recipient or CDR representative is segregated from other CDR data to ensure it is

	Control requirements		Minimum controls	Description of minimum controls
				accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.
(3)	An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle.	(a)	Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: (a) blocking access to unapproved cloud computing services; and (b) logging and monitoring the recipient, file size and frequency of outbound emails; and (c) email filtering and blocking methods that block emails with CDR data in text and attachments; and (d) blocking data write access to portable storage media.
		(b)	CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.
		(c)	Information asset lifecycle (as it relates to CDR data)	The accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention, and, in accordance with rules 7.12 and 7.13, deletion and de-identification.
(4)	An accredited data recipient must implement a formal vulnerability management program to	(a)	Security patching	A formal program is implemented for identifying, assessing the risk of and applying security patches to applications and operating as soon as practicable.

	Control requirements		Minimum controls	Description of minimum controls
	identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	(b)	Secure coding	Changes to the accredited data recipient's systems (including its CDR data environment) are designed and developed consistent with industry accepted secure coding practices, and are appropriately tested prior to release into the production environment.
		(c)	Vulnerability management	A formal vulnerability management program is designed and implemented, which includes regular vulnerability scanning and penetration testing on systems within the CDR data environment.
(5)	An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment.	(a)	Anti-malware anti-virus	Anti-virus and anti-malware solutions are implemented on endpoint devices and on servers to detect and remove malware from the CDR data environment and are updated on a regular basis. End-user systems are updated with the latest virus definitions when they connect to the network. Reports or dashboards highlighting compliance metrics are regularly generated and monitored, and non-compliant items are actioned as soon as practicable.
		(b)	Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.
		(c)	Application whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) is restricted to authorised software only.
(6)	An accredited data recipient must implement	(a)	Security training and awareness	All users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses'

	Control requirements		Minimum controls	Description of minimum controls
	a formal information security training and awareness program for all personnel interacting with CDR data.			provided at least annually.
		(b)	Acceptable use of technology	A policy relating to the CDR data environment is created, implemented, communicated and agreed to by all personnel prior to being able to access the CDR data environment. This policy sets out the responsibilities of these personnel in interacting with the CDR data environment and is regularly made aware to personnel.
		(c)	Human resource security	Background checks are performed on all personnel prior to being able to access the CDR data environment. These may include, but are not limited to, reference checks and police checks.

Schedule 7—Transitional

Note: This Schedule commences on the day after this instrument is registered.

Competition and Consumer (Consumer Data Right) Rules 2020

Note: A set of joint account provisions in relation to the banking sector was included in the principal rules as made (Part 4 of Schedule 3)—this is the "original Part 4".

The *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) (the "earlier amendment rules")* replaced that Part in Schedule 3. That instrument also included the "earlier transitional provision".

This amending instrument repeals the replaced Part 4 in Schedule 3 and inserts new, non-sector-specific joint account provisions in a new Part 4A in the body of the Act—this is the "new Part 4A". Under clause 6.6 of Schedule 3, this will apply to the 4 initial data holders immediately.

However, the earlier transitional provision allowed data holders to continue to apply the original Part 4 for some time. This Schedule allows those data holders that took advantage of that transitional provision (in practice all 4 initial data holders) to continue to use the original Part 4 until 1 July 2022, when they must begin to comply with the new Part 4A.

It also allows other existing data holders to choose to comply with the new Part 4A earlier than they are required to.

1 Definitions

In this Schedule:

amendment date means the day Schedule 4 to these rules commenced.

earlier amendment rules means the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*.

earlier transitional provision means paragraph 105(4)(b) of Schedule 1 to the earlier amendment rules.

new Part 4A means Part 4A of the principal rules as in force on and from the amendment date.

original Part 4 means Part 4 of Schedule 3 to the principal rules as in force immediately before the commencement of Schedule 1 to the earlier amendment rules.

principal rules means the *Competition and Consumer (Consumer Data Right) Rules 2020*.

2 Compliance with original Part 4 instead of new Part 4A for certain existing data holders

(1) This item applies to an initial data holder for Schedule 3 of the principal rules that, immediately before the amendment date, complied with the original Part 4 in order to satisfy the earlier transitional provision.

(2) The data holder may elect, for a period beginning on the amendment date and ending, unless revoked earlier, on 1 July 2022, to continue to comply with the

41589883

Authorised Version F2021L01392 registered 05/10/2021

original Part 4 (as varied to the extent reasonably necessary so that it operates in accordance with the rest of the principal rules as otherwise amended) rather than the new Part 4A in relation to one or more accounts.

(3) If it so elects, such compliance is taken to be compliance with the new Part 4A.

(4) If the data holder revokes an election in relation to an account, it may not make another election in relation to that account.

3 Voluntary compliance with new Part 4A

(1) If a data holder is not required to comply with the new Part 4A because of the operation of clause 6.6 of Schedule 3 of the principal rules (Staged application of rules)., it may nevertheless elect, from a particular day, to comply with the new Part 4A in relation to one or more accounts.

(2) If a data holder makes an election under this item, it is thereafter required to comply with the new Part 4A in relation to those accounts, despite anything in Part 6 of Schedule 3 of the principal rules.

4 Application of new Part 4A to existing account with initial data holder

(1) This item applies in relation to a joint account, with an initial data holder, that is in existence immediately before the Part 4A day.

(2) On and from the Part 4A day, the following disclosure option under the new Part 4A applies to the account:

(a) if a disclosure option applied to the account immediately before the Part 4A day—the equivalent disclosure option under the new Part 4A;

(b) if a disclosure option had previously applied to the account, but no disclosure option applied immediately before the Part 4A day—the non-disclosure option;

(c) if no disclosure option had at any time applied to the account before the Part 4A day—the pre-approval option.

(3) In this item:

Part 4A day means:

(a) if the data holder makes an election under item 2—the earlier of:

(i) the day that the data holder revokes the election; and

(ii) 1 July 2022; and

(b) otherwise—the amendment day; and

5 Application of new Part 4A to existing account with other data holder

(1) This item applies in relation to a joint account, with a data holder other than an initial data holder, that is in existence immediately before the Part 4A day.

(2) On and from the Part 4A day, the pre-approval option applies to the account.

(3) In this item:

41589883

Part 4A day means:

(a) if the data holder makes an election under item 3—the day on which the data holder makes the election; and

(b) otherwise—1 July 2022.