CONSUMER DATA RIGHT

DRAFT RULES

SUBMISSION TO THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION

May 2019

PUBLIC

EXECUTIVE SUMMARY

1. ANZ thanks the Australian Competition and Consumer Commission (**Commission**) for the opportunity to comment on its draft Consumer Data Right Rules (**Draft Rules**). Terms used but not defined in this submission have the meaning given in the Draft Rules and the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (**Bill**).

Key points

2. The Draft Rules are a well-considered set of precepts to govern the implementation of open data in Australia. We have made some comments on the drafting for the Commission's consideration that are set out in full below. We would draw the Commission's attention to the following four key points.

3. **First**, we note that the Commission has not yet proposed a mechanism for addressing reciprocal data exposure obligations. We continue to believe that an economy-wide approach to open data is appropriate to allow potential consumer welfare benefits in all markets on an equal competitive basis. One consequence of the absence of a reciprocity mechanism is that when consumers transfer data to accredited data recipients, they will have no right to access the data. This is because accredited data recipients will hold the data in accordance with the privacy safeguards and not the Australian Privacy Principles (**APP**). The privacy safeguards do not contain any equivalent of APP 12, which gives individuals the right to access information relating to them. If the consumer data rules do not impose any obligation on accredited data recipients to comply with data access requests from consumers, then consumers will have no legal entitlement to access information held under the privacy safeguards. We would ask that the Commission consider a reciprocity mechanism in the interests of both economic welfare and individual privacy.

4. **Second**, and related to the preceding point, the Explanatory Memorandum at paragraph 1.86 contemplates that an accredited data recipient will be able to hold data as a data holder if it meets the conditions set out in the consumer data rules. This will allow an accredited data recipient to hold received CDR data subject to the APPs and not the privacy safeguards. The Draft Rules do not set out the conditions on which this could occur. We would ask that the Commission consider providing these conditions.

5. **Third**, as we have noted below, the Draft Rules could benefit from further clarity on when credit products provided to businesses will become subject to the consumer data right. This is because the Draft Rules contemplate that certain

business credit products will be caught in the three phases of staging when they are offered to the general public. The idea that business products are offered to the general public appears slightly contradictory and we would appreciate further clarity from the Commission on the treatment of business credit products.

6. **Fourth**, we support the intent of the data correction mechanism in privacy safeguard 11 and reflected in proposed rule 7.7. We wondered whether the currently proposed obligation for updating data could be improved by considering what the appropriate timeframes might be and what actual mechanisms for data correction should be implemented. We have made some comments on proposed rule 7.7 below.

COMMENTS ON SPECIFIC PROVISIONS

RULE 1.7 – DEFINITIONS

1. The definition of 'data minimisation principle' contemplates that the data which is collected is no more than necessary to provide goods or services under a CDR contract. We wondered whether the Commission contemplates that this principle would allow data to be used to improve products and services. If so, it may be useful to expand the drafting to accommodate this. We assume that the Commission would understand the principle as permitting assessments of eligibility to receive the provision of the good or service.

2. The definition of 'associated person' is capable of including third party data processing and infrastructure providers to accredited data recipients. While this could be intended, the Commission may like to consider whether such providers are intended to be part of 'senior management' as defined in Schedule 1.

RULE 1.8 – MEANING OF CDR CONTRACT

3. The definition of a 'CDR contract' contemplates that the contract will be about the collection and use of the data. From the drafting it does not appear necessary that the CDR contract be about the good or service that is actually provided. Thus, a CDR contract could conceivably contemplate that data will be collected and used for various services or goods that will actually be provided under distinct contracts.

4. We would suggest that the drafting could be clearer on whether the contract concerns the collection and use of the CDR data or the subsequent provision of the goods and service or both. As discussed below, this issue arises in relation to rule 4.3 which contemplates that the CDR contract must be terminated as a whole in order to stop an authorisation being 'valid'.

5. We also query whether there would be benefit in extending the scope of rule 1.8(1)(c) to any clause that is inconsistent with any of the instruments specified in rule 1.5(2).

RULE 1.12 – CONSUMER DATA REQUEST SERVICE

6. Rule 1.12(4) provides that data provided under the direct request service be in human-readable form. Much of the 'customer data', 'account data', 'transaction data' and 'product specific' data that could be required to be made available for the banking sector is already made available to customers in human readable form through bank statements and disclosure documents. It may be worthwhile considering what existing information formats could be used to satisfy the direct request service requirements.

RULE 1.13 – CONSUMER DASHBOARD – ACCREDITED PERSON

7. Rule 1.13(a) could be clarified by making clear that the relevant consents are those that have been given to the accredited person providing the dashboard. The current drafting just refers to consents given by the CDR consumer. CDR consumers may have given consents to multiple accredited persons.

8. Rule 1.13 does not stipulate how long the dashboard or the information it presents must be available to a CDR consumer. The Commission may wish to consider prescribing a timeframe for maintenance beyond expiry of the consent request.

RULE 1.14 – CONSUMER DATA REQUEST SERVICE

9. Rule 1.14 requires data holders to provide a consumer dashboard from receipt of a consumer data request regardless of whether the request is rejected or valid. Given the obligations imposed on data holders in relation to the consumer dashboards, the Commission may wish to consider whether a consumer dashboard might better be required at some point later than receipt of requests such as issuance of consumer authorisation to the data holder.

10. As with rule 1.13, rule 1.14 is silent on the duration for which the dashboard and the information it presents must be available in the dashboard.

RULE 2.6 – USE OF DATA DISCLOSED PURSUANT TO PRODUCT DATA REQUESTS

11. We understand the rationale behind proposed rule 2.6 prohibiting data holders from attempting to control how persons use CDR data disclosed in response to a product data request. We would, however, ask the Commission to consider whether the rule as drafted:

    a) Could expose consumers to risk if persons receiving the data reorganise it in such a way that it no longer accurately describes the product it relates to, or otherwise omits critical features; and

    b) Operates in an overbroad fashion to potentially deprive the data holder of intellectual property. For example, it is conceivable that the data could be the data holder's copyright. If so, the proposed rule would purport to deny the data holder the ability to control how it is replicated. This is relevant given that the rule is intended to operate for any product data that is designated by the Minister (not just the initial banking industry data).

RULE 3.5 – REFUSAL TO DISCLOSE IN RESPONSE TO CONSUMER DATA REQUEST

12. Proposed rule 3.5 allows a data holder to refuse a request to disclose CDR data when it could harm an individual or the ICT system used to expose the CDR data. An equivalent right of refusal is proposed under rule 4.7 in relation to requests by an accredited person. The Commission may like to consider whether this right should extend to situations of potential harm to:

    a) A CDR consumer that is a business;

    b) The data holder due to fraud or other illegal financial activity; and

    c) The ICT system of the data holder in general, not merely those that are used to expose the CDR data. The exposure ICT systems will unlikely be the most critical system that data holders run. It could be an odd result if the proposed rules allowed the protection of the CDR-related systems and not systems that were more important to the data holder's business continuity.

13. It may also be appropriate that data holders have the right to refuse a request when responding to it may be unlawful or facilitate unlawful activity (such as money laundering).

14. The Commission may like to consider whether the time period for notification of the Commission following a refusal should be specified in business days (ie one or two business days). If the report is to be made within 24 hours, then an appropriate reporting portal would need to be established that could receive reports outside of business hours. We note that there could be a high level of reporting to the Commission if all refusals are reported. The Commission may like to consider whether the reporting is limited to refusals which have a systemic basis or thematic similarity.

15. It could further be helpful if the Commission were to clarify that data holders have no obligation to assess for risks of harm before complying with a data request. Data holders will not always be able to usefully assess the risk of harm arising from a request.

RULE 3.6 – USE OF DATA DISCLOSED PURSUANT TO CONSUMER DATA REQUEST MADE UNDER THIS PART

16. The Commission may like to consider whether rule 3.6 is drafted in overbroad terms and is actually needed.

17. As drafted, the rule purports to authorise any use of the data by the CDR consumer. There will obviously be legal limits on what the CDR consumer can use the data for. A more appropriate framing may be that the data holder may not impose contractual restrictions on the use of the data.

18. Further, as the Bill does not purport to limit what use CDR consumers can put CDR data to (unlike privacy safeguard 6 which limits the use of CDR data by accredited data recipients), rule 3.6 may be otiose.

RULE 4.1 – SIMPLIFIED OUTLINE OF THIS PART

19. We wondered whether rule 4.1 can assert that a fee cannot be charged for the disclosure of CDR data under Part 4 of the Draft Rules. Whether a fee is chargeable for CDR data is determined by the Ministerial designation under proposed section 56AC(2)(d) of the Bill. It is thus conceivable that Part 4 of the Draft Rules could function with respect to chargeable data.

RULE 4.3 – REQUEST FOR ACCREDITED PERSON TO SEEK TO COLLECT CDR DATA

20. It is not clear from the drafting of rule 4.3 whether the consents to collect and use data are divisible concepts or a single concept. While the concepts are broken out in paragraphs 4.3(1) and 4.3(2), paragraph 4.3(3) states that '[i]n giving the consents, the consumer gives the accredited person a ***valid*** request to seek to collect that CDR data from a data holder' (underline added). This drafting implies that the consents are a single concept. If the concepts are divisible, the drafting of paragraph 4.3(3) suggests that consent to 'use' is sufficient to give an accredited person a valid request to 'collect' data. If so, the utility of the separate consent to collect is questionable.

21. We note that the draft CX guidelines contemplate that the two consents are a single concept.

22. We also note that rule 4.3(4) provides that a request ceases to be valid if the CDR contract is terminated. This means that the request continues to be valid until the consumer terminates not only the consent to collect the data but also the consent to use it and any service covered by the CDR contract. We wondered if this is the right outcome as a consumer may wish to continue to use a data-based service even if the consumer wants the data collection to stop.

RULE 4.4 – CONSUMER DATA REQUESTS BY ACCREDITED PERSON

23. Rule 4.4 contemplates that once a CDR consumer has given an accredited person a valid request to seek to collect CDR data from a data holder, the accredited person

may then request the data holder to disclose some or all of the CDR data that is subject of the consent and it is able to collect in accordance with the data minimisation principle.

24. We note that under the permission granted by rule 4.4, the accredited person can choose what CDR data from within the universe of CDR data it has consent to collect it ultimately seeks from data holder. Thus, the accredited person may collect less data than the CDR consumer anticipates. While this may be reasonable, it does raise the question of whether the data minimisation principle should apply to the CDR data that an accredited data recipient seeks to collect rather than simply use.

25. The Commission may also like to consider whether this rule could be used to oblige the accredited person to inform the data holder of the information that the data holder will need to comply with rule 4.22(2). This latter rule obliges the data holder to inform the CDR consumer of certain parameters around the data authorisation. The accredited person will need to inform the data holder of these parameters. If the data holder is not informed of these parameters, then it would be difficult for the data holder to comply with rule 4.22. The Commission may like to consider what would happen if the data holder does not have the information that it is required to disclose under rule 4.22.

26. We also wondered whether the term 'consumer data request' as used in rule 4.4 may be more clearly expressed as 'consumer authorisation request'.

RULE 4.8 – USE AND DISCLOSURE OF DATA COLLECTED PURSUANT TO CONSUMER DATA REQUESTS UNDER THIS PART

27. Rule 4.8(2) provides that an accredited data recipient must not use or disclose collected data for a prohibited use or disclosure. We wondered whether this provision is perhaps overbroad in that it seems to close off disclosures that are required or authorised by law or court/tribunal order. In this sense, rule 4.8(2) appears more narrowly drawn than proposed section 56EI(1) (privacy safeguard 6) as set out in the Bill.

RULE 4.10 – ASKING CDR CONSUMER TO GIVE CONSENT TO COLLECT DATA

28. We note that paragraph 4.10(4) contemplates that consent could be given for 'a single collection of CDR data'. This is also reflected in subparagraphs 4.12(1)(d) and 4.25(1)(d). The Commission may like to consider what a 'single collection' means, particularly where there are several APIs as part of the authorised data scopes (ie does the 'single collection' apply to each consented API?). It may be

simpler if instead of 'single collection, the rules simply contemplated access being granted for a very short period of time from first access (eg 10 minutes).

RULE 4.11 – WITHDRAWAL OF CONSENT TO COLLECT CDR DATA AND NOTIFICATION

29. It would be useful if the point at which the withdrawal becomes effective is specified (eg when received by the accredited person, rather than when sent).

RULE 4.12 – DURATION OF CONSENT TO COLLECT CDR DATA

30. Rule 4.12(1d) states that a one-off consent will expire upon data collection but there is no provision for any data which has not been collected. We wonder if this provision should be extended to include unfulfilled consents and whether a time-out reference is appropriate (with specific detail to be set out in the standards).

31. When Rule 4.12(2) operates, we wonder by what mechanism the data holder is to be informed of the revocation or surrender.

32. The Commission may like to consider whether rule 4.12(2) should also provide clarity on what happens when an accredited person's accreditation is suspended. The rule currently only deals with situations of revocation or surrender. Will, for example, any authorisations automatically re-enliven when the suspension ends?

RULE 4.22 – ASKING CDR CONSUMER TO AUTHORISE DISCLOSURE OF CDR DATA

33. The reference to 'consent process' in rule 4.22(1)(a) could possibly be better expressed as 'authorisation process'.

RULE 4.24 – WITHDRAWAL OF AUTHORISATION

34. If consumers are able to withdraw their authorisation in writing, the Commission may like to consider specifying when the withdrawal becomes effective. We would suggest two business days within receipt by the data holder. This timeframe is to allow processing of mailed withdrawal notices.

RULE 5.9 – CONDITIONS ON ACCREDITATION

35. The Commission may like to consider whether it would be appropriate for any conditions imposed on accredited persons to be communicated to CDR consumers.

RULE 5.21 – CONSEQUENCES OF SURRENDER, SUSPENSION OR REVOCATION OF ACCREDITATION

36. We note the actions that flow from the revocation of accreditation under this rule. Perhaps an additional step would be to notify all data holders who have received a

request from the disaccredited person. It may be appropriate for this notification to be made by the Accreditation Registrar.

RULE 7.2 – RULES RELATING TO PRIVACY SAFEGUARD 1

37. We note the obligation to provide a list of outsourced service providers. We wondered whether the providers that need to be included on this list should be confined to those providers that receive CDR data. We don't believe the definition of 'outsourced service providers' in rule 4.8 is constrained to this group of entities. If the definition is not so confined, then the disclosure obligation could be significant.

RULE 7.7 – RULES RELATING TO PRIVACY SAFEGUARD 11

38. Rule 7.7 obligates data holders to inform CDR consumers no later than 24 hours after discovering that data is inaccurate, out of date or incomplete of that fact and then give the CDR consumer the option of directing the data holder to transfer the corrected data to the accredited data recipient.

39. While we support the policy intent of this rule, we would like the Commission to consider three points in relation to it:

    a) First, the need to advise the CDR consumer within 24 hours of the discovery of the erroneous data could be challenging to implement if corporate knowledge of the discovery is deemed to arise when a staff member first identifies the issue. For example, if a customer advises a branch staff member on a Friday afternoon of the need to correct a data entry, the rules would require that data holders run their notification processes through the evening and into Saturday. It may be more feasible if the obligation to advise the customer applies as soon as reasonably practicable.

    b) Second, we note that the obligation to correct is only enlivened when the data holder is 'aware' of the erroneous nature of the data at the point of disclosure. This makes the disclosure obligation contingent upon the corporate knowledge of the reason for data correction. Thus, the obligation would be enlivened if the data holder was told that an address needs to be changed because it was incorrect when disclosed but not if the address needs to be changed because the customer has moved properties subsequent to a disclosure. This will require data holders to keep records of, and act upon, the reason for data corrections (not merely the correction alone). This is understandable but the Commission may to consider the feasibility of all data holders having such systems.

c) Third, it is not clear how the updating mechanism contemplated by rule 7.7 aligns with the data transfer mechanism in Part 4. Is the disclosure contemplated by subparagraph 7.7(1)(d)(ii) subject to the same consent and authorisation flows as a Part 4 disclosure? If not, does this mean that the request contemplated by 7.7(1)(d)(i) constitutes both consent to the accredited data recipient to collect and use the corrected data and an authorisation to disclose it? We note that if the disclosure contemplated by subparagraph 7.7(1)(d)(ii) is to be separate from the mechanism contemplated by Part 4, then additional data standards will be needed to make clear how the disclosure is to occur.

40. We also wondered whether rule 7.7 should extend to accredited data recipients as well. This is because proposed section 56EN applies to both data holders and accredited data recipients.

RULE 9.3 – RECORDS TO BE KEPT

41. We would ask the Commission to clarify whether paragraph 9.3(1)(f) requires data holders to keep a copy of the CDR data that was disclosed or merely a description of it. We anticipate that the correct interpretation of the provision is that it only requires a description of the disclosed CDR data to be kept but it would be helpful if the rule were clear on this. We note that the same issue arises with paragraph 9.3(2)(c).

SCHEDULE 1, CLAUSE 2.2, CONTROL REQUIREMENT 3

42. We note the proposed obligation to prevent data leaving the CDR data environment. There is a possible interpretation of this obligation that it would extend to bank's internet and mobile banking portals (as those portals relate to the management of CDR data). This would mean that banks would, for example, be required to prevent screen scraping of internet banking. The Commission may like to consider whether this was the intended operation of the requirement.

SCHEDULE 2, CLAUSE 1.2 – DEFINITION OF 'JOINT ACCOUNT'

43. The definition of 'joint account' is limited to accounts with two joint account holders. We note that there are joint accounts with more than two joint account holders and wondered whether the Commission is intentionally not including those accounts within the initial roll out of the consumer data right.

SCHEDULE 2, CLAUSE 1.3 – ITEM 2 (ACCOUNT DATA)

44. We wondered whether item (d)(i) actually belongs under the heading of 'transaction data' as it concerns the amount and date of specific transactions. It may be appropriate if this item instead refer to the 'last' amount that was debited.

SCHEDULE 2, CLAUSE 2.1/2.2 – REQUIRED PRODUCT/CONSUMER DATA

45. Clauses 2.1 and 2.2 of Schedule 2 set out what is required product and consumer data respectively. The Commission may like to consider how the 'earliest holding day' limitation imposed by proposed section 56AC(2)(c) is reflected in these provisions. Specifically, section 56AC(2)(c) means that no entity can be a data holder in respect of data it began holding before the earliest date included in the designation instrument (see paragraph 1.79 of the Explanatory Memorandum).

46. We note that clause 2.2(1)(b)(ii) will mean that secondary credit card holders will not be able to access any account data in relation to them. This is because they are not an account holder.

47. The Commission may like to consider whether the drafting of clause 2.2(1)(d) could be clearer as consumers may be able to 'access' products of the data holder online without being authorised to transact on their accounts through a digital channel. For example, all consumers may be able to apply for a credit card through a website. This could be construed as an ability to 'access' a product but likely falls short of meaning the consumer is digitally active.

48. We also wonder whether in the situation of a joint account if both account holders need to satisfy subparagraph 2.2(1)(d).

49. Note 4 (misstated as Note 3) implies that if a consumer has an account that satisfies clause 2.2(1)(e), then they can make a data request in respect of all accounts even if they don't satisfy clause 2.2(1)(e). It is not clear if this means that that the consumer can access accounts that were closed before 1 January 2017. The concept of 'earliest holding day' would seem to prevent this (see above).

SCHEDULE 2, PART 3, CLAUSE 3.3 – REFUSAL TO DISCLOSE

50. We wondered whether some additional language is needed in paragraph 3.3(2) to the effect of 'when this clause applies and despite subrule 3.4(1)…'.

SCHEDULE 2, PART 3, CLAUSE 3.4 – CONSUMER DASHBOARD FOR JOINT ACCOUNTS

51. Could the Commission possibly clarify what information is to be provided to the joint account holder via the dashboard? We assume the dashboard only needs to concern the joint accounts.

SCHEDULE 2, PART 4

52. It is not clear how the drafting in Part 4 of Schedule 2 actually controls the requests that may be made under rules 2.3, 3.3 and 4.3. The scope of the requests made under these rules is constrained to 'required product data' and 'required consumer data'. In Part 2 of Schedule 2, these concepts are defined by reference to various parameters. However, these parameters do not incorporate the staging parameters set out in Part 4 of Schedule 2. It is not clear by which drafting mechanism those staging parameters influence what data can be requested when. The parameters are just asserted to have effect without being incorporated into the actual request mechanisms.

SCHEDULE 2, PART 4, CLAUSE 4.3

53. The table set out under this clause contemplates that credit card accounts, business finance, lines of credit (business) and overdrafts (business) will be in one of the three phases. It is not clear, however, whether these credit products would be offered to 'the general public'. By definition, these accounts are limited to customers that are engaged in business and thus are not offered to the general public. The *National Consumer Credit Protection Act 2010* (Cth) draws a distinction between credit provided to 'consumers' for 'personal, domestic or household purposes' and other credit. 'Consumers' is defined to mean individuals or strata corporations.

54. We would suggest that only credit that is provided for personal, domestic or household purposes is truly offered to the general public. This statutory distinction may be useful to giving clarity about what products are caught by the initial version of the consumer data rules.

55. We are also not clear how the concept of 'complex accounts' is dealt with by the Draft Rules.

ENDS