CONSUMER DATA RIGHT

DRAFT LEGISLATION

SUBMISSION TO THE TREASURY

September 2018

Public

EXECUTIVE SUMMARY

1. ANZ thanks Treasury for the opportunity to comment on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (**Bill**). Terms used but not defined in this submission have the meaning given to them in the Bill.

2. ANZ supports economy-wide open data in the form contemplated by the Productivity Commission in its 2017 *Data Availability and Use* report (**PC Report**) and the Treasury's 2018 *Review into Open Banking* report (**Open Banking Report**). In response to the Government's 9 May 2018 announcement that it would implement a consumer data right (**CDR**) with banking the initial designated sector, ANZ has commenced the preparatory work to implement data access and transfer arrangements for its customers.

Key points

3. While the Bill is an important step in implementing a CDR in Australia, it would benefit from further reflection and refinement before its introduction into Parliament as the CDR's facilitative framework. The key issues that would benefit from additional work largely concern the breadth of the Bill's potential scope of application and its interaction with the existing law. Through an understandable desire to establish a comprehensive and flexible framework, the Bill would create an overbroad set of powers and duties that could undermine privacy, incentives to compete and commercial practices that benefit consumers.

4. In particular, amendments could be usefully made to:

    a) Tighten the nexus between a CDR consumer and CDR data so that corporations and individuals with only tenuous connections to CDR data do not have rights in respect of it

    b) Remove 'derived data' from CDR data so the regime does not deter innovation through data in opposition to the CDR regime's declared policy intent – the potential for competitors to acquire confidential information and other intellectual property from one another under the CDR framework seems incongruent with supporting incentives for innovation – the PC Report and the Open Banking Report both recommended against the inclusion of such data

    c) Reconsider how the privacy safeguards interact with the Australian Privacy Principles (**APP**s), existing commercial uses and other legal obligations – at present the Bill applies the privacy safeguards on top of the APPs while also prohibiting uses that have been approved under the APPs and that are

required in order to comply with foreign and Australian law – the safeguards also need to be improved so that, for example, they do not require notification of all CDR consumers upon transfer (which would include any person or company merely identifiable in the data)

d) Adopt better procedural safeguards for designating sectors and CDR data and preparing the consumer data rules and, in any event, follow the full consultative process with respect to the designation of authorised deposit-taking institutions (**ADI**s), particularly if Treasury continues with the inclusion of derived data in the definition of CDR data – while much antecedent work has been done on open banking, it has not sufficiently addressed the considerations set down by the Bill for sector designation

COMMENTS ON SPECIFIC CLAUSES

CLAUSE 56AA

1. The reference to 'certain sectors' in clause 56AA(a) may understate the ambit of Part IVD. The Part itself applies to all sectors of the economy: There are no limits on which sector the Minister can designate. Thus, 'certain' should be replaced with 'any designated'. Conversely, the reference in clause 56AA(b) to 'any information' is perhaps also incorrect as the designation process would define the available information for which there are no CDR consumers. Again, 'any designated' may be more apt than 'any' alone. Obviously, the same comments apply to clause 56AB, which contains similar language to that in clause 56AA.

CLAUSE 56AD

2. Because of the importance of designation, we would suggest that clause 56AD be recast as a set of outcomes that the Minister must be satisfied that designation will achieve. Thus, for example, designation should only occur when the Minister is satisfied that it will generate positive outcomes for consumers, their privacy and the economy.

3. One reason for reframing clause 56AD in this way is to better embed the purpose of the Part articulated in clause 56AA in the framework which the Part establishes. This could help give the broad powers contained in the Part some guardrails.

4. As an extreme example to highlight the utility of such guardrails, the broad and permissive grants of power in clauses 56AC and 56BA and the decisional processes that surround them would appear, on their face, to allow a Ministerial designation and a consumer data rule that compelled data holders to expose personal information to unaccredited entities on the basis of a consumer's 'defaulted' consent or 'deemed' request (even though the consultation with the Information Commission would likely highlight the privacy implications of this type of arrangement). Privacy safeguard 3 (clause 56EF) would not stop these kinds of disclosure as it only concerns *collection* by an *accredited data recipient* (not *disclosure* to the *others*) and a 'valid' request could be defined by the consumer data rules. We note that there is no statutory requirement that recipients of CDR data be accredited data recipients (although paragraph (a) of clause 56AB suggests that they need to be). At best, an aggrieved CDR consumer would need to challenge the decision on the grounds that it was ultra vires due to the purpose of the Part as expressed in clause 56AA and the description of the Part in clause 56AB.

5. A similar point could be made concerning highly sensitive commercial information, such as trade secrets. Such information could be designated by the Minister for exposure to the public under clause 56AC(2), with the only constraint being the operation of section 51(xxxi) of the Constitution (as recognised by clause 56GG). This scenario would be contingent on the data holder not also being recognised as a CDR consumer (which is currently possible due to the definition of CDR consumer, as discussed below). However hypothetical, these types of outcomes suggests that an outcomes-based framing of clause 56AD provides stronger safeguards than a list of matters for consideration.

6. The list of relevant matters or outcomes prescribed by this clause should also be expanded to include:

   a) Whether the designated information or any possible derivations from it are or could be 'property' that would be 'acquired' if made available for the purposes of section 51(xxxi) of the Constitution. This is a critical consideration as it will help inform the Commission's setting of any fees for the transfer of the information and place CDR participants on notice that receipt of the information could expose them to a claim from the transferring CDR participant for 'just terms' compensation.

   b) The likely effect of the instrument on Australian economic activity (if framed as an outcome, that the instrument will positively benefit the Australian economy). Because wholly offshore entities can be accredited data recipients, the designation may have an impact on the location of data-orientated economic activities. Thus, it would be relevant to consider issues such as whether Australian competitors in the relevant sector have opportunities in other jurisdictions equivalent to those which designation would give foreign companies either in Australia or with respect to Australian consumers. Such a consideration should not create unnecessary barriers to cross-border trade.

   c) The need for effective reciprocal data sharing in respect of the CDR data as contemplated by the Government's 9 May 2018 publication *Consumer Data Right*. At present, there is no requirement in the Bill that there will be a '…mechanism that will provide that those who wish to become accredited and receive designated data at a consumer's request must be willing to share

equivalent data, in response to a consumer's request.'[1] This concept should be enshrined in law. Clause 56AD could include a requirement that the Minister is satisfied that entities which receive CDR data will be under an equivalent obligation to expose CDR data at consumer request. This would involve consideration of whether it is possible for the Commission to establish a reciprocity mechanism in respect of the information and sector that are proposed to be designated.

7. We would suggest also that it would be helpful if the primary regulator for a designated sector is consulted before the designation occurs. Thus, while the Commission must consult with the primary regulator for a designated sector before making consumer data rules under clause 56BO(1)(c), it is arguable that the primary regulator's input would be equally relevant at the point of designation. This is because designation is the main mechanism by which the operation of a sector could be affected.

CLAUSES 56AD/56AE

8. Both Ministerial designations and the Commission's decision processes should be subject to some form of review mechanism. This is because designation would have a significant impact on consumers and an industry, including the competitive dynamics within it. It would be beneficial if any decision concerning CDR data were subject to review, possibly by the Australian Competition Tribunal. This would help ensure that the consumer data rules are well-adapted to specific policy objectives.

CLAUSE 56AE

9. We would ask Treasury to reconsider clause 56AE(6). The consultative process prescribed by clause 56AE is an essential safeguard to good policy making in respect of the consumer data right. Clause 56AE(6) would allow the designation of a sector for the CDR without those safeguards being adhered to. Rather than the current formulation of clause 56AE(6), which permits an avoidance of the consultative process without consequence, Treasury should consider how it can achieve a situation where a minor technical failure in the consultative process does not void a designation instrument but the obligation to consult remains firm.

10. More mundanely, we note that while the Commission *must* publish its report on its website under clause 56AE(1), the Information Commissioner only *may* publish its

[1] The Australian Government the Treasury *Consumer Data Right* (9 May 2018), 4.

equivalent report under clause 56AE(2). We thought that the Information Commissioner should be under an obligation equivalent to the Commission's.

CLAUSE 56AF(1) & (2)

11. Clauses 56AF(1) and (2) set up a two part definition of CDR data:

    a) Any information designated under clause 56AC(2); and

    b) Any information derived from (a), including through successive derivations.

12. Because the derivation limb of the concept of CDR data operates by virtue of law, rather than by virtue of Ministerial designation or Commission rule, it has a scope of operation that is impossible to know in advance. Whenever someone derives information from designated data, that information will become, by virtue of law, CDR data. This means that the Minister can never know what information will ultimately be subject to the CDR through designation.

13. Another consequence of this is that the consultative processes in clause 56AE will always be incomplete assessments of the impact of the designation: Understanding the impact of the designation on ex ante basis will be an epistemological impossibility because of the construction of clause 56AF(1).

14. Moreover, it also means that data holders could be under an uncertain obligation to make CDR data available. The degree of this uncertainty would, of course, be contingent upon the CDR rules made under clauses 56BC(a) and 56BD(a). These allow CDR rules requiring that '…all or part of…' the CDR data is to be made available. Thus, the Commission would be able to limit the operation of the derivation limb of clause 56AF(1). However, it is under no obligation to do so. We note that this potential constraint on the impact of the definition of CDR data does not mitigate our concerns about the consultative process. This is because designation is the enabling action which occurs prior to the promulgation of the CDR rules.

15. However, the derivation limb of 'CDR data' also has implications for how derived data is treated, irrespective of whether the Commission intends to bring such data within the scope of the consumer data rules (ie to make such data available for transfer). Some of the privacy safeguards apply to 'CDR data' (ie the statutory concept) regardless of whether it has been dealt with under Part IVD or even had consumer data rules written in respect of it. Thus, those safeguards would apply data immediately upon its derivation from CDR data. As discussed below, our

reading of the Bill is that the consumer data rules could not carve out this data from the privacy safeguards (although regulations could).

16. At a broader policy level, the inclusion of derived data within the scope of the CDR represents a departure from the Government's prior work on data. This includes both the PC Report and the Treasury's own Open Banking Report. Both reports recommended against including derived data within mandated data availability.

17. The PC Report stated:

> *Data that is solely imputed by a data holder to be about a consumer may only be included with industry-negotiated agreement. Data that is collected for security purposes or is subject to intellectual property rights would be excluded from consumer data.*[2]

18. The Open Banking Report recommended that:

> *data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.*[3]

19. This recommendation was caveated in respect of 'know-your-customer' assessments. The reason for the recommendation was that:

> *its value has largely been generated by the actions of the data holder, or has been externally augmented by authorised data recipients (such as credit bureaux). As such, imposing an obligation to share that data may amount to a breach of intellectual property rights, or interfere with existing commercial arrangements. At the very least it would represent a transfer of value from the data holder to the customer.*[4]

20. The reasons for adopting a policy in opposition to these recommendations are not clear.

21. The implications of including derived data within the scope of the CDR are significant. This significance can be demonstrated by exploring what data could be caught by a designation of bank transaction account statement data. If the Minister

---

[2] Productivity Commission *Data Availability and Use* (May 2017), 36.
[3] The Australian Government the Treasury *Review into Open Banking* (December 2017), 38 (recommendation 3.3).
[4] Ibid, 37.

were to designate this data, then the derivation limb of clause 56AF(1) would capture the following data sets at least. Of course, a consumer data rule could operate only with respect to part of this universe of data, although some of the privacy safeguards would operate in respect of all of it. Thus, data derived from transaction account statement data could include any:

a) Credit scores that a bank created from the designated data

b) Customer preference insights and strategic business plans based on them

c) Material generated for the purposes of resolving a dispute with the customer

d) Reports generated for regulators in relation to anti-money laundering, counter-terrorism and sanctions laws

e) Financial record of the bank (as information concerning the financial performance of the bank is ultimately derived from the transactions it conducts with its customers)

The customer would be identifiable through some of this data, while other information would not identify a customer, such as records of the bank's aggregate financial performance. Of course, those financial records would identify the bank, and due to the breadth of the definition of CDR data, that CDR data would still be data through which a person could be identified.

22. This information would include material that is:

a) Critical to the bank's competitive position;

b) Intellectual property of the data holder and/or a third party service provider that would otherwise be protected by law (including through actions for breach of confidence);

c) Subject to legal professional privilege;

d) Legally unable to be exposed to the customer (eg some reports to AUSTRAC);

e) Subject to regulatory constraints on its disclosure; and/or

f) Market sensitive.

23. The ramifications of exposing this type of material through the CDR are difficult to predict in advance. At the very least, if the CDR transfers intellectual property and competitive advantages from one competitor to another then it may undermine the

market system. Even if fees are chargeable for this information, it still allows competitors to acquire, under compulsion of law, information that would never have been available through normal market mechanisms. As competitors would be able to benefit from any derivation of data, there would be little incentive to innovate.

24. We would strongly encourage Treasury to redraft clauses 56AF(1) and (2) to remove derived data from the definition of CDR data.

CLAUSE 56AF(4)

25. Clause 56AF(4) defines 'CDR consumer' to mean any person (natural and legal) to whom the CDR data relates if the person is identifiable or reasonably identifiable through the data. This is a very broad definition that has a number of implications for the operation of the framework established by the Bill.

26. First, the expansive conceptualisation of who should be entitled to access and transfer data means that individuals and companies with only loose connections to the contract and activities that created the data could become entitled to it. For example, a retailer could be a CDR consumer in relation to transaction account data held by a bank when the retailer is the payee in a transaction record. This would theoretically give the retailer the right to ask for transaction records held by the bank that identify the retailer even if the retailer is not a customer of the bank.

27. Second, the definition of CDR consumer has interesting knock-on effects through the rest of the Bill. For example, clause 56EH requires a person who collects CDR data to notify each CDR consumer about that collection. For a data recipient receiving bank transaction data, this could mean informing every payer and payee identified in the data.

28. Similarly, clause 56EI would mean that if one CDR consumer requested their CDR data, then data holders would be unable to deal with that data any further except through the consumer data rules or as required or authorised under Australian law (other than the APPs). Thus, if a retailer were to request all CDR data that a bank holds on it, would this mean that the bank is precluded from exposing that data to the actual account holder, including in accordance with the APPs?

29. Third, the definition means that if Treasury intends to designate data relating to products (so-called product attribute data), then that data will be data for which there is a CDR consumer (the issuer or manufacturer of the product). Ironically, this means that data which is currently publicly available would become subject to

the privacy safeguards in the Bill. Because of this, we wondered what operation clause 56BD would have.

30. Fourth, the concept of 'reasonably identifiable' is problematic as it invites questions of what threshold applies to data that is capable, through varying degrees of effort, of being re-identified to a consumer. Whether data is capable of re-identification is an empirical question, the answer to which is contingent on motivation, technology, availability of related data and degree of data security. The precise ambit of CDR data for which there is a CDR consumer would change over time as these factors changed.

31. Fifth, we wondered whether such a broad definition of CDR consumer could be implemented feasibly. It requires suppliers to both have an omniscient understanding of which individuals and corporations can be identified through their data holdings and an ability to construct an entitlement and data extraction mechanism that is tailored to the data that identifies the person.

32. These observations suggest that a fundamental component of the CDR – the nexus between consumer and data – would benefit from further work. The Bill appears to adopt a privacy-oriented nexus between consumer and data (ie based on identifiability). The original drivers for the consumer data right concerned allowing consumers to place greater competitive pressure on suppliers through using data relating to the relationship with the supplier to assess other offers and move to better suppliers. These drivers suggest a competition-oriented nexus between consumer and data. This should be based on the consumer's contractual relationship with the supplier. Such a nexus would more tightly link the consumer to the relevant data and avoid the negative implications listed above. In operation, it may better protect the privacy of individuals than the current formulation.

CLAUSE 56AH

33. Clause 56AH extends the consumer data right to data generated offshore and could cause significant additional complexity for data holders with international businesses including through possible conflict of laws. It is not clear, for example, that the CDR will constitute a lawful basis for data export from the European Economic Area under the European Union General Data Protection Regulation.[5]

[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

34. We also note that because of how CDR consumer is defined, clause 52AH(2) may have a very broad scope of operation. This is because entities that generate data will likely be identifiable through the data (thus rendering them CDR consumers in respect of that data).

CLAUSE 56BA

35. As we noted above, there are no limits on what kinds of consumer data rules can be written. It may be useful if the Bill were to limit the rule making power to those rules which support a clear, statutorily-defined policy purpose.

36. Clause 56BA allows the Commission to make rules that differ across different designated sectors, different classes of CDR data and different classes of persons (both data holder and recipients). It may also be useful to insert an obligation on the Commission to prefer rules that allow data to be shared across designated sectors. This would allow innovation to occur across sectors at the lowest cost.

CLAUSE 56BB

37. We note that the matters that the consumer data rules may deal with do not include the consent that needs to be obtained from CDR consumers. While consent may be covered by the matter of 'disclosure', because of its centrality to success of the CDR regime, it would be worthwhile explicitly identifying this as a matter for consumer data rules.

CLAUSE 56DA

38. In recognising external dispute resolution schemes, it may be useful if the Commission were directed to have consideration to schemes which already operate in a sector. This would avoid industry participants needing to be members of multiple schemes.

CLAUSE 56CK

39. It would be helpful if this clause contained a statement to the effect that CDR participants can rely on the Register of Accredited Data Recipients as conclusive evidence of whether a person has been accredited under clause 56CE(1). This would give CDR participants comfort concerning who they can trust as being accredited.

40. Further, the Register of Accredited Data Recipients should not only be maintained by electronic means, but available for public inquiry by electronic means in a form that can be easily interrogated by external systems. A publicly available PDF list of

accredited data recipients would not be sufficient; it should be accessible through an application programming interface.

DIVISION 5

41. Division 5 would introduce a new privacy regime into Australian law that appears intended to operate in coordination with the existing privacy regime of the *Privacy Act 1988* (Cth) (**Privacy Act**), which includes the APPs. This new regime is ostensibly needed, in the most part, because the existing privacy regime would not (a) protect all CDR consumers, which can be corporations or (b) regulate all CDR participants, which can be foreign entities holding accreditation or businesses with a turnover of less than $3 million.

42. Introducing a new privacy regime into Australian law is a significant undertaking and requires consideration of how the protections it grants interact with existing Australian and foreign laws and commercial practices that are currently legal. The current draft of Division 5 raises issues that would benefit from further reflection and refinement. These issues are raised below in context of each clause introducing the safeguards.

43. Besides the existing draft clauses, we do not believe that the Bill yet contains a mechanism that deals with the delineation between when CDR data is subject to the privacy safeguards and when it is subject to the APPs. Example 1.14 from the Explanatory Materials suggests that received CDR Data can stop being treated in accordance with the privacy safeguards and start being treated in accordance with the APP. The Explanatory Materials suggest this could occur in accordance with the consumer data rules.

44. However, our interpretation of Division 5 is that the privacy safeguards can apply to CDR data from the moment of its designation under clause 56AC(2) and capture any derivations from it. This is because several of the safeguards apply to 'CDR data', a concept that is defined in clause 56AF(1). The consumer data rules could not limit the operation of the privacy safeguards as suggested by Example 1.14, nor could they restrict the operation of clause 56AF(1). This is because of clause 56EC which provides that if there is an inconsistency between the safeguards and the rules, the safeguards will prevail. We note, however, that a regulation made under clause 56GE may be able to do this in respect of specified persons. This means that CDR data would always be subject to the privacy safeguards: There is no mechanism that allows data to move from one privacy regime to the other (or back again). We would suggest this issue would benefit from further work. Any

solution to this issue would best be reflected in legislation, rather than consumer data rules.

45. One option may be to use the APPs as a nearly sufficient set of protections for the CDR instead of introducing a novel set of privacy safeguards that operate in addition to the APPs. To do this, the Bill could bind all accredited data recipients to the APPs. This would mean that CDR consumers that are corporations would not benefit from the privacy safeguards (as the Bill currently proposes) but it would mean a simpler implementation. Some additional safeguards concerning use of CDR data could be added as a constraint on CDR participants but this could occur through a supplementation to the APPs rather than through a parallel regime.

CLAUSE 56ED

46. Privacy safeguard 1 requires that CDR participants must have a policy concerning their management of CDR data. We would ask that CDR participants be able to use their existing privacy policies, appropriately amended, to satisfy this obligation. CDR participants should not need to maintain a privacy policy and a separate CDR data policy.

47. Clauses 56ED(5)(e) and (f) require a CDR participant to have policies that contain information on whether they are likely to disclose CDR data to accredited recipients who are based overseas and which countries they will be located in. We wondered how a CDR participant would know in advance that they are likely to disclose data in this way. The identity and location of the CDR participant that receives data will be driven by the CDR consumer, not the CDR participant drafting the policy.

CLAUSE 56EF

48. Privacy safeguard 3 provides that a person who holds accreditation under clause 56CE(1) must not collect CDR data by soliciting it except through the CDR framework or as otherwise required or authorised by Australian law. This safeguard purports to apply to all 'CDR data' regardless of whether it has been subject to a request by a CDR consumer.

49. In this context, CDR data would appear to take its statutory meaning and not any more limited meaning given by a consumer data rule. As discussed above, this is because the consumer data rules do not appear capable of limiting the application of the safeguards to particular classes of CDR data.

50. Because of this broad definition of CDR data, and because privacy safeguard 3 covers collection by solicitation for any purpose, its prohibition appears overbroad.

It would prohibit the collection by solicitation of any data covered by the definition in clause 56AF outside of the mechanisms of Part IVD except where directly required by Australian law.

51. Thus:

    a) If no consumer data rule had been made by the Commission facilitating the collection of the CDR data (eg the Commission made rules in respect of a subset only of the CDR data designated by the Minister), clause 56EF would, on its face, categorically prohibit the collection by solicitation of the CDR data (unless otherwise authorised or permitted by Australian law, other than the APPs);

    b) Where an Australian statute required the use of information but did not specifically require or authorise its collection, it is questionable whether soliciting information for that use would fall within the exception in clause 56EF(b);

    c) The collection of CDR data that is explicitly required by, or in order to comply with, foreign laws would be prohibited (clause 56GC would not provide immunity from any violation of foreign laws that is caused by adherence to the CDR framework); and

    d) Where CDR data is currently collected pursuant to APP 3, or in situations where the APPs do not apply (such as the collection of information from corporations), the safeguard would now prohibit that collection by solicitation.

52. These outcomes appear to place undue fetters on the collection of CDR data. The operation of privacy safeguard 3, together with privacy safeguard 6, appears to prevent data collection and availability other than through the CDR mechanisms. This seems contrary to the Open Banking Report. Recommendation 1.1 of that report stated:

    Open Banking should not be mandated as the only way that banking data may be shared. Allowing competing approaches will provide an important test of the design quality of Open Banking and the Consumer Data Right.[6]

53. We would ask Treasury to reconsider privacy safeguard 3 both to allow adherence to laws and to encourage alternative forms of data collection and access.

[6] Ibid, xii.

CLAUSE 56EG

54. Privacy safeguard 4 requires that persons who hold accreditation under clause 56CE(1) must destroy any unsolicited CDR data that they receive. Like privacy safeguard 3, this safeguard operates in an overbroad manner:

    a) It applies to receipt of CDR data outside of the transfer mechanisms of Part IVD, including when those mechanisms have not been created by the Commission through consumer data rules; and

    b) It does not recognise requirements to retain CDR data as a result of foreign laws.

55. The obligation should also be subject to a reasonable steps test because, for example, the person may be unaware that they have received unsolicited data if the data sender transmits, amongst a large volume of solicited data, small amounts of unsolicited data (eg a slightly larger date range).

CLAUSE 56EH

56. Privacy safeguard 5 requires the notification of each CDR consumer for the CDR data of the collection. As noted above, there could be many CDR consumers for collected CDR data (ie all payees and payers identified in transaction data). As such, this obligation could become extremely onerous on the collector of the CDR data and, perhaps, annoying for CDR consumers who are frequently identifiable through data (such as utility and telephone companies which would be identifiable in the bank statements of almost all Australians).

57. We also note that the obligation in this safeguard should be subject to any Australian or foreign law requirements that would prohibit the notification.

CLAUSE 56EI

58. Privacy safeguard 6 prohibits the disclosure of CDR data for which a request has been made except through the consumer data rules, or where authorised or required by law. This means that once a CDR consumer has made a request under the consumer data rules for their data, the data holder would be precluded from showing that CDR consumer or any other CDR consumer the relevant data, including through the normal means by which the consumers access their data.

59. For banks, if a customer had requested that their account balance be disclosed under the consumer data rules, we could be precluded from showing that balance to that customer (or any joint account holder) through means that are not legally

mandated. This may include, for example, answering an inquiry from the customer about that account balance or displaying account data through internet or mobile banking.

60. This privacy safeguard has significant implications when considering disclosure of data in respect of legal persons who are not covered by the APPs (ie businesses).

61. As noted above in relation to privacy safeguard 3, privacy safeguard 6 seems to preclude alternative forms of data access in contradiction to the Open Banking Report's recommendation and, potentially, in frustration of established commercial activities that benefit consumers.

CLAUSE 56EJ

62. Clause 56EJ prohibits the use of collected CDR data for the use of direct marketing unless valid consent is received. We wondered how this provision added to the prohibition already set down in clause 56EI(2); it seems to be a use-specific version of that broader prohibition.

CLAUSE 56EK

63. Again, it is not clear how clause 56EK (concerning disclosures to off-shore persons) adds anything to the prohibition set out in clause 56EI (prohibition on disclosure except in accordance with the consumer data rules).

64. It does, however, highlight how the safeguards can frustrate current commercial practice. For example, we may be required to disclose CDR data to process payments with offshore financial institutions. These institutions may not be accredited to receive CDR data. As drafted, this safeguard would preclude us from processing those payments.

CLAUSE 56EM

65. Privacy safeguard 10 requires that a CDR participant must take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up-to-date and complete when it is disclosed. We appreciate the intent of this clause but would ask that the section explicitly make clear that the purpose for which the data is held does not include its exposure under the CDR. If this amendment is not made, then it is arguable that CDR participants need to take reasonable steps to ensure the data is appropriate for the purposes of exposure, and thus use by the third party data recipient. These uses would be unknowable by

the CDR participant and thus should not be a purpose for which the CDR data is held.

CLAUSE 56EN

66. Clause 56EN(2) requires a person who collects CDR data to destroy that data in accordance with the consumer data rules when the data is no longer needed. We would ask that this obligation be subject to a reasonable steps test due to the possible comingling of needed and unneeded data.

CLAUSE 56ET

67. Clause 56ET(5) protects CDR participants from double jeopardy in respect of contraventions. This protection should also extend to contraventions under the Privacy Act.

CLAUSE 56GC

68. Clause 56GC provides protection from liability that may arise from the legally compliant provision of CDR data. We appreciate the intent of this section but believe it should go further to make clear if and how the new Part IVD and the regulations and consumer data rules made under it may prevail over any inconsistent law.

69. This is important because even though no action may lie against a CDR participant arising out of compliant CDR transfers, the act itself may still be a breach of another law. Thus, for example, a regulatory reporting requirement could arise because of the breach, even though the regulator would not ultimately be able to bring an action in respect of it. Greater clarity is needed for CDR participants in how to understand the interaction of their obligations under the new Part IVD and other laws.

70. We also note that this section would not provide any protection for a data holder that is forced to transfer the intellectual property of a third party due to a consumer data rule (or, indeed, a data recipient that unwittingly receives such intellectual property).

CLAUSE 56GG

71. Clause 56GG provides that if the Part results in the acquisition of property otherwise than on just terms for the purposes of section 51(xxxi) of the Constitution, the person from whom the property is acquired can recover reasonable compensation from the acquirer.

72. As noted above, this issue could be relevant even if a fee is set under the consumer data rules. Transferors of data may assert that such fee does not represent compensation (ie just terms) for the property acquired by the transfer of the data.

73. Receivers of CDR data may need to assess, in advance, whether receipt of the data will constitute an acquisition of constitutional property. Such an assessment may be necessary to form a view whether they could become liable to a suit under clause 56GG for receiving the data. Obviously, it may be difficult to perform this assessment in advance, particularly if it was asserted that the constitutional property that had been acquired was in the form of confidential information (which, by its nature, is not known to others before its disclosure).

74. As noted above, it is not just data holders which may have a claim in respect of the CDR data. Third party service providers may also have intellectual property in respect of CDR data, particularly derived data that is created using such providers' software or other effort.

SECTION 2

75. Section 2 of the Bill removes the requirements for the Minister and the Commission to consult on the designation of, and consumer data rules concerning, banks if those acts occur before 1 July 2019. While the Open Banking Report concerned open data in the context of banks, it cannot be seen as a substitute for consultation on either the designation of banking or the formulation of the consumer data rules. This includes because derived data is now within scope of CDR data and because the Open Banking Report did not resolve many details with how open banking could be implemented.

ENDS