CONSUMER DATA RIGHT – EXPOSURE DRAFT LEGISLATION TO ENABLE ACTION INITIATION

SUBMISSION TO THE TREASURY

October 2022

PUBLIC

INTRODUCTION

1. ANZ thanks the Treasury (**Treasury**) for the opportunity to comment on the exposure draft *Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation* (**Draft Bill**).

2. The Government's *Inquiry into Future Directions for the Consumer Data Right* final report in October 2020 (**Future Directions**) highlights the potential of action initiation to reduce barriers to switching products, promote competition and to provide more cost effective and convenient products and services for consumers. It also acknowledges the increased risk of cyber-attack, fraud and other harms associated with action initiation that must be addressed so consumers trust and use the CDR regime.

3. We support a CDR regime that appropriately protects consumers and provides clear guard rails for developing innovative CDR products and services.

4. With these general principles in mind, we recommend that Treasury makes some revisions to the Draft Bill and undertakes certain analysis before legislation to enable action initiation is settled, introduced or used. This analysis should inform any adaptation of the existing regime. We consider this to be the most efficient path to delivering effective, fit for purpose and risk-focussed regulation.

5. To assist Treasury to achieve its policy objectives, we have made some observations below on the Draft Bill. These comments are made within the context of our overall support for an effective CDR regime which enables consumers to safely, efficiently and conveniently use their information to access better products and services. These comments are organised into:

   - First, our key points regarding the Draft Bill; and
   - Second, discrete comments on some provisions within the Draft Bill.

6. Our key points for Treasury's consideration are summarised below.

   - **Complete a cyber security review before introducing action initiation**

     Consumer trust in the CDR regime is essential to its success. The introduction of action initiation could increase the risk to consumers of fraud and scams. Future Directions recommends that an information security assessment be undertaken before legislation enabling action initiation is settled. The Government's *Statutory Review of the Consumer Data Right* (**CDR Review**) recommends that the Government consider undertaking a 'whole of ecosystem cyber security assessment to ensure the CDR cyber security architecture' is fit for purpose into the future. In light of recent significant data

breaches in Australia, we recommend that these reviews are undertaken before legislation enabling action initiation is introduced.

- **Define the perimeter between the instruction and action layers and avoid regulating the action layer**

  The Draft Bill intends to regulate action *instructions* only, leaving the regulation of *actions* unaffected. As such, the regulatory perimeter between the instruction and action layers must be clearly defined to establish the scope of the CDR regime. We suggest the Draft Bill define 'the action layer' to capture any action the action service provider (**ASP**) takes after receiving a valid action instruction that an authenticated consumer has authorised. The Draft Bill should not include obligations, and should prevent Rules being made, that apply at 'the action layer' as defined. This includes privacy safeguard (**PS**) 3 and PS 4.

- **The non-discrimination principle should not restrict ASPs from taking fraud protection measures and complying with action layer obligations**

  ASPs remain liable for complying with regulatory obligations governing actions. Despite this, the Draft Bill *requires* ASPs to comply with a valid CDR action instruction if, having regard to the criteria in the consumer data rules (**Rules**), the ASP would ordinarily perform actions of that type in the course of their business.[1] The non-discrimination principle should not constrain an ASP's discretion to take measures it considers appropriate to protect against cyber-attack, fraud and scams, and to comply with regulatory and other obligations in the action layer in line with its risk appetite.

- **Minimise regulatory duplication and consider Privacy Act review outcomes before introducing legislation**

  There is, by design, significant overlap between the *Privacy Act 1988* (**Privacy Act**) Australian Privacy Principles (**APPs**) and the CDR regime privacy safeguards. The Draft Bill proposes to apply PS 3 and PS 4 to ASPs in place of corresponding APPs 3 and 4. The Privacy Act, including the APPs, is under review with a final report on proposed amendments to strengthen the Act anticipated this year. Amendments to the Privacy Act are also expected to be introduced this year following recent significant data breaches. Regulatory duplication creates complexity, risks non-compliance and is inefficient. To maximise regulatory efficiency, we recommend that the outcome of the

[1] Draft Bill, s56BZC

Privacy Act review and other proposed amendments to the Privacy Act are considered before settling revisions to the privacy safeguards in the Draft Bill.

- **Align payment initiation with payments system developments**

  If not already contemplated, we suggest it would be prudent to address the implications of CDR payment initiation in the Government's strategic plan for the payments system, the single, tiered payments licensing framework and the associated review of the ePayments Code.[2] This would help to ensure efficient and consistent implementation of payments reform.

7. We look forward to the next steps in Treasury's review and would welcome the opportunity to discuss the points in this submission if this would be useful.

[2] Australian Government, *Transforming Australia's Payments System*, December 2021 (**Payments Review**).

KEY POINTS

Complete a cyber security review before introducing action initiation

8. The CDR Review notes that cyber security issues are likely to increase as the CDR matures and expands and recommends that the Government considers undertaking a cyber security assessment to ensure the CDR cyber security architecture is fit for purpose into the future.[3] We strongly support this recommendation.

9. Consumer trust is critical to the success of the CDR regime. Recent significant data breaches have highlighted to consumers the risks of sharing their data. This may have a material impact on consumer uptake of the CDR. The 'whole of ecosystem cyber security assessment' recommended by the CDR Review would ensure the appropriate settings are in place and support consumer confidence in the regime.

10. The new cyber security challenges associated with the introduction of action initiation should also be considered. For example, accredited action initiators (**AAIs**) and ASPs, with the ability to instruct and make payments, will likely be attractive targets for malicious actors.[4] Future Directions acknowledges the need to address the increased risk of cyber-attack, fraud and other harms associated with action initiation and payment initiation.[5] It recommends that an information security assessment be undertaken to consider appropriate protections for action initiation instructions and notes that this assessment should occur *before* the legislation is settled to determine what should be captured in the primary legislation, the Rules or Standards.[6]

11. We support undertaking the security assessment before the Draft Bill is settled because it may result in changes to the legislative framework. For example, an assessment of the information security architecture for CDR payment initiation may identify a particular instruction architecture for initiating payment instructions that would better protect against cyber-attacks, fraud and scams. This might include leveraging other secure payment system

---

[3] See CDR Review at page 43. While the CDR Review also acknowledges that the Review didn't hear many concerns from stakeholders regarding cyber security, consumer uptake of the CDR is still relatively low so cyber security settings may still be, to some extent, untested.

[4] At page 4 of its submission to the Future Directions inquiry, the OAIC noted "*…the expansion to write access may also raise new privacy and security implications, which will need to be appropriately addressed. In particular, as write access would allow third parties to modify a consumer's financial information, it may increase the motivation for unauthorised actors to target an accredited data recipient's information system.*"

[5] Future Directions, p. 97

[6] See Recommendation 7.11, Future Directions, p. 179. We note that in June 2022 the Data Standards Body (**DSB**) obtained an independent assessment of the information security profile of CDR data standards against relevant security benchmarks. While the DSB notes on github that this assessment is timely with action initiation and payment initiation on the horizon, the assessment doesn't appear to expressly "…consider appropriate protections, proportionate to the risks involved for action initiation authorisation, consent and instruction data…" in line with Future Directions recommendation 7.11.

developments that offer similar third party payment initiation functionality like PayTo. PayTo includes its own third party instruction layer potentially requiring a particular payment initiation use case design that commences in the CDR regime and connects to PayTo. This may result in a different legislative framework for payment initiation with consent, authentication and authorisation occurring outside of the CDR regime.

12. We recommend that this information security assessment includes a review of worked action initiation use cases considered in the light of existing regulatory requirements governing actions, the Draft Bill and proposed information security architecture. This would highlight any issues in the security architecture and inform the proposed legislative framework, including confirming the appropriate regulatory perimeter between the instruction and action layer and the scope of the non-discrimination principle (see commentary below).

13. While undertaking this assessment may delay the introduction of legislation enabling CDR action initiation, it will provide time for the system to 'mature and capitalise on lessons learnt' in line with the findings of the CDR Review.[7] This will allow patterns of consumer use and objectives to emerge more clearly enabling the regime to respond to the demands of consumers. Consumer demand should inform the development of CDR functionality to ensure the utility of the regime.

Define the perimeter between the instruction and action layers and avoid regulating the action layer

14. The Exposure Draft Explanatory Materials for the *Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation* (**Explanatory Materials**) state that the Draft Bill regulates the instruction layer and intends to leave laws governing the action layer unchanged. As such, a clear perimeter between the instruction and action layer is critical to determine the scope of application of the CDR regime (for example, the Rules must not apply at the action layer) and the intersection with other regulatory regimes that govern the action layer.[8] We're concerned that the regulatory perimeter between the instruction and action layers is unclear and the Draft Bill interferes in the action layer.[9]

15. Below we describe why the regulatory perimeter is unclear; an example of how the Draft Bill regulates the action layer; why this is problematic; and how this might be addressed.

---

[7] CDR Review, p. 42
[8] Draft Bill, s 56BGA(4)
[9] *Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation* (**Explanatory Materials**), p. 8

16. The Draft Bill provides that Part IVD of the *Competition and Consumer Act 2010* regulates 'the instruction layer associated with instructions for the performance of actions' and 'contains little regulation of the action layer (that is, regulating how service providers perform actions they are instructed to do)'.[10] Section 56BGA specifies that the Rules:

    - Cannot include rules requiring an ASP to perform (or not perform) a CDR action in a particular way;[11] and
    - May include requirements on an ASP relating to how it processes a valid instruction.[12]

    This appears to define the instruction and action layers by relying on a distinction between 'processing an instruction' and 'processing an action'. It's unclear where 'processing an instruction' ends and 'processing an action' begins.

17. An example of how the Draft Bill regulates the action layer concerns the information that ASPs can collect to process a valid action instruction. The Draft Bill potentially regulates the action layer by applying PS 3 and PS 4 to ASPs. PS 3 prevents ASPs from collecting CDR data unless they meet all requirements in the Rules.[13] PS 4 requires ASPs to destroy unsolicited CDR data it receives under the CDR regime in the action layer. The Rules could specify *what* data is permitted to be shared with an ASP for different action types.[14] If this occurs, the Draft Bill and Rules will require an ASP to perform an action in a particular way (by restricting the information an ASP can collect to perform the action).

18. For example, a consumer instructs an AAI that they wish to switch from their existing bank X credit product to new bank Y credit product. Bank Y (as ASP) receives an instruction from the AAI to commence processing an application. Bank Y (*as ASP*) actions this instruction by requesting further consumer CDR data from the AAI. Bank Y receives relevant solicited and unsolicited data in response. The request for information is part of the action layer and, as such, should not be regulated by the privacy safeguards.[15] Bank Y must retain discretion to obtain information it considers necessary to assess the credit card application in compliance

---

[10] Draft Bill, s 56AB

[11] Draft Bill, s 56BGA(4)

[12] Draft Bill, s 56BGA(1)(d)

[13] Draft Bill, s 56EF Privacy safeguard 3 – soliciting CDR data from participants under the consumer data rules

[14] See *Exposure draft legislation to enable action initiation in the Consumer Data Right – Summary of proposed changes* September 2022, p. 9. The *Privacy Impact Assessment on the introduction of Action Initiation in the Consumer Data Right* (**PIA**), at page 25, explains that the Rules would apply where an ASP requests additional data to complete an action, such as a bank requiring additional details from a consumer to consider an application.

[15] To avoid doubt, if the ASP elects to collect CDR data *in its capacity as an ADR* the privacy safeguards already apply. If the ASP collects consumer data in the action layer in its capacity as an ASP only, the data should be managed under existing regulation governing the action layer ie the Privacy Act (including APPs 3 and 4) and other sectoral regulation.

with its policies, prudential regulation and responsible lending legislation.[16] Information required to comply with these requirements can differ from consumer to consumer.

19. It is vital that ASPs retain 'action layer' discretion regarding how to process actions because ASPs continue to be subject to regulation governing the performance of actions. This includes retaining the ability to determine what data is necessary to satisfy their obligations and comply with their policies.

20. To clarify the regulatory perimeter between the instruction and action layers, Treasury might consider expressly defining 'action layer' in Part IVD, Division 1, Subdivision C (Meanings of key terms) of the Draft Bill to include any action an ASP takes after it receives a valid action instruction that has been authorised by an authenticated consumer. PS 3 and PS 4 should not apply to CDR data collected by ASPs in the 'action layer'. Section 56BGA(4) could also be revised to prevent the Rules regulating ASPs in the 'action layer' as defined.

The non-discrimination principle should not restrict ASPs from taking fraud protection measures and complying with action layer obligations

21. As observed, the CDR regime should not constrain how ASPs perform actions because ASPs remain liable for complying with obligations governing the performance of actions. The Draft Bill requires ASPs to uphold the non-discrimination principle. This requires ASPs to comply with a valid CDR action instruction if, having regard to the criteria in the Rules, the ASP would ordinarily perform actions of that type in the course of their business.[17] The scope of this requirement is unclear and may constrain *how* ASPs perform actions including how ASPs protect against fraudulent transactions.

22. Our concern with the non-discrimination principle is illustrated using a payment initiation example. Banks employ a range of fraud prevention measures when instructed to make payments from customer accounts. The specific measures depend on the channel the instruction comes through (eg internet banking, in person). The non-discrimination principle shouldn't limit a bank's ability to apply appropriate measures for the instruction channel.

23. For example, suppose an AAI submits a valid instruction to an ASP bank to make variable recurring payments. The bank must authenticate the consumer and obtain their authorisation to accept the AAI instructions. The bank is a signatory to the ePayments Code requiring it to

[16] For example, Section 131(4) of the *National Consumer Credit Protection Act 2009* includes a prohibition against a credit provider entering an unsuitable credit contract. There may be circumstances in which a credit provider/ASP, complying with responsible lending obligations, reasonably takes a view that it must have regard to certain information in assessing whether a credit contract is unsuitable, even if that information was not solicited.
[17] Draft Bill, s 56BZC

reimburse the consumer for certain unauthorised transactions. This includes transactions where a security breach of the AAI's IT environment results in a payment instruction to the bank that is not in accordance with the consumer's original action initiation instructions.[18] In line with its risk appetite, the bank applies 'step up' authorisation to the recurring transactions instructed by the AAI. 'Step up' authorisation involves contacting the consumer directly to authorise each payment. It's unclear whether this would be permitted under the non-discrimination principle if it does not apply the same 'step up' authorisation to all other third party instructions.

24. The Explanatory Materials state that the non-discrimination principle "…is not intended to prevent an ASP from applying extra security or other checks to CDR action requests on the basis that a third party is involved, *provided it is consistent with existing practices*".[19] [our emphasis]. The meaning of 'consistent with existing practices' is unclear.

25. Fraud detection measures are applied to all third party instructions but the specific measures applied depend on the instruction channel. Fraud detection measures applied to a human third party signatory on an account (such as trusted devices, geolocation and biometric authenticators) cannot be applied to an AAI instruction. ASP banks need to be able to apply fraud detection measures that are effective for specific channels.

26. The non-discrimination principle should clearly support an ASP's discretion to take measures it considers appropriate to protect against cyber-attack, fraud and scams, and to comply with regulatory and other obligations in the action layer in line with its risk appetite. Treasury could consider revising section 56BZC of the Draft Bill to state that ASPs cannot discriminate against action instructions *merely* because they're received through the CDR but it can apply different requirements to address CDR action initiation risks.

Minimise regulatory duplication and consider Privacy Act review outcomes before introducing legislation

27. The CDR Review found that the CDR operates within a complex regulatory regime and that, where possible, the CDR should limit duplication and overlapping regulatory obligations to

[18] Under the ePayments Code, an account holder is not liable for an unauthorised transaction where (among other scenarios) it is clear that a 'user' has not contributed to the loss. An unauthorised transaction is a 'transaction that is not authorised by the user'. A user is an account holder or an *individual* who is authorised to perform transactions. As such, an AAI will not be a 'user' (unless the AAI is an individual) and a payment made a result of a fraud on the AAI will not be authorised by the account holder. While Future Directions suggests an ASP bank should have a direct right of action to recover any compensation the bank pays to the consumer from the AAI where the unauthorised payment is caused by the AAI failing to comply with its CDR security obligations, there are significant challenges with forensic analysis establishing the cause of a data breach and that it caused the loss.

[19] Explanatory Materials, p. 19

simplify compliance.[20] We support this objective. Simplifying compliance results in more reliable and efficient compliance.

28. The Draft Bill proposes to apply PS 3 (regarding collecting CDR data) and PS 4 (regarding dealing with unsolicited CDR data) to ASPs. They are applied to ASPs in place of APPs 3 and 4 which address the same concerns but are less restrictive.[21] Irrespective of the content of the APPs or the privacy safeguards, we believe one privacy regime should apply in the action layer to reduce regulatory complexity.

29. If an ASP receives a valid instruction from an AAI, the ASP may request further information to process the instructed action (ie in the action layer). The ASP may seek this directly from the consumer or from the AAI via the CDR. The ASP should be able to manage all information it receives to process the action in the same way under the Privacy Act and other sectoral legislation. Applying different privacy regimes to data received by ASPs may make it unclear for ASPs and consumers which regulatory framework applies to specific data handled by an ASP at a particular time.[22] It also adds further complexity for participants operationalising compliance.

30. In 2020 the Government commenced a comprehensive review of the Privacy Act to examine whether the scope and enforcement mechanisms remain fit for purpose. A final report on proposed amendments is anticipated this year. The review is considering proposals to strengthen requirements for APP entities collecting, using and disclosing personal information under the Privacy Act.[23] The review is also considering a proposal to give individuals a right to erasure of personal information.[24] If adopted, these proposals will strengthen the application of APPs 3 and 4. Other proposed reforms to the Privacy Act may change how entities use individuals' information and may prompt further consideration of the privacy safeguards.

---

[20] CDR Review, p. 9

[21] APP 3 provides that an APP entity must not collect solicited personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities. It also sets out requirements for collecting solicited sensitive information and requirements regarding how information is collected. The Draft Bill proposes that PS 3 state that "CDR data can only be collected if the ASP has validly requested the information under the consumer data rules for the purpose of a valid instruction to be given for the performance of a CDR action of that type."

[22] The PIA, at page 9, identifies this as a key risk of the proposed privacy framework.

[23] The Government's *Privacy Act Review Discussion Paper* at page 11, proposes to introduce a requirement that the collection, use or disclosure of personal information must be fair and reasonable in the circumstances, together with legislated factors to guide this assessment.

[24] The Government's *Privacy Act Review Discussion Paper* at page 13, proposes to introduce a right for individuals to request the erasure of personal information in certain circumstances.

31. We encourage Treasury to consider proposed revisions to the Privacy Act before settling the Draft Bill to minimise regulatory overlap and ensure efficient regulation.

Align payment initiation with payments system developments

32. Payment initiation within the CDR regime should be aligned with payments system developments and reform. Following the payments system review, the Government is developing a strategic plan outlining policy priorities and strategic direction for the payments system.[25] If it's not already contemplated, we suggest that any Ministerial declaration of payment initiation is incorporated into the plan to ensure payment initiation implementation aligns with other payments developments.

33. The Government will also introduce a single, tiered payments licensing framework. The ePayments Code will be revised and mandated for all payments licensees.[26] Before payment initiation is declared, this ePayments Code review should incorporate any adaptations required for CDR payment initiation. For example, Future Directions notes that the ePayments Code should be adapted to ensure it is relevant to payments instructed through CDR. The Code should treat AAIs like others that the consumer properly authorises to give payment instructions on their account.[27]

[25] Payments Review, p. 7
[26] Payments Review, p. 9
[27] Future Directions, p. 91

COMMENTS ON SPECIFIC PROVISIONS

Objects – proposed section 56AA(ba)

34. We suggest that section 56AA(ba) should replicate the language in section 56AA(a) which states that the object of the Part is "…to enable consumers…to require information relating to themselves…to be disclosed *safely, efficiently and conveniently*…" [our emphasis]. Section 56AA(ba) should similarly confirm that the object of the CDR includes enabling consumers to *safely, efficiently and conveniently* request accredited persons to give instructions to service providers in those sectors for the performance of actions. It is vital that the CDR system supports consumers to *safely* instruct actions on their behalf.

Minister's tasks before declaring actions – proposed section 56AD(1)(a)

35. We suggest that section 56AD(1)(a) expressly requires the Minister to consider the security of consumers' information before designating a sector or declaring an action. This would require an information security assessment to be undertaken identifying specific risks and appropriate controls for the proposed action before an action is declared.

36. While section 56AD(1)(a)(iii) requires the Minister to consider the privacy or confidentiality of consumers' information, Future Directions notes this would, in practice, be actioned by undertaking a privacy impact assessment.[28] It would not require a specific information security assessment.

Minister's tasks before declaring actions – proposed section 56AD(1)(b)

37. We recommend section 56AD(1)(b) expressly requires consideration of whether other regulatory changes are appropriate before an action is declared. While the legislation requires the Minister to consider the likely regulatory impact of allowing the Rules to impose requirements relation to actions, it doesn't expressly require consideration of the need for regulatory changes.[29] Future Directions recommends that when conducting sectoral assessments, consideration should be given as to whether regulatory and legal changes are required and appropriate to enable action initiation within a sector.[30] We support this view.

ENDS

[28] Future Directions, p. 179
[29] Draft Bill, s 56AD(b)
[30] Future Directions, Recommendation 4.4, p. 41