Australian Government

Office of the Australian Information Commissioner

Consumer Data Right (CDR) Action Initiation Exposure Draft Legislation

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

24 October 2022

OAIC

Contents

Part 1: Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the exposure draft of the Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation (the Bill) and the exposure draft explanatory materials to the Bill (explanatory materials).

The explanatory materials indicate that a key goal of expanding the consumer data right (CDR) system to action initiation is to *'empower… consumers to authorise, manage and facilitate actions securely in the digital economy'*.[1] The Bill would expand the CDR from a system that facilitates data sharing to a system that would also enable consumers to instruct an entity to initiate actions on their behalf, for example making a payment or opening and closing an account.[2] The OAIC generally supports the expansion of the CDR to action initiation to achieve this goal, provided a robust framework for privacy and confidentiality is built to protect consumers and their associates, and safeguard the integrity of the CDR system.

The OAIC sees consumer trust as central to the success of the CDR, and strong privacy and security safeguards as the fundamental pillars for building and maintaining that trust. The existing CDR framework has been designed with the aim of ensuring that consumers who participate in the CDR system can have confidence that CDR entities will handle their information appropriately, and that they will be able to access redress mechanisms if this does not occur. As the government continues to expand the CDR system, it is critical to its success that consumers can have trust and confidence, whether they engage with CDR data sharing or action initiation.

CDR action initiation will introduce new entities into the CDR ecosystem,[3] and create new roles for certain existing CDR entities.[4] It will create new information flows between participating entities (potentially including banks, telecommunications providers, fintechs and energy providers), and facilitate CDR information moving outside the CDR system in new ways (especially during the 'action layer').[5] In addition to these new entities and data flows, CDR action initiation may also increase motivation for third parties to target CDR entities' systems. For example, if action initiation facilitates payments or changes to a consumer's financial information, this may increase motivation for unauthorised actors to attempt to use the CDR system to commit fraud in order to initiate such a payment or change.[6] It is therefore critical that a complete, consistent and clear legislative framework for privacy and confidentiality is created for CDR action initiation. This should build on, and be consistent with, the strong privacy and information security protections that are already a fundamental part of the CDR data sharing system.

---

[1] Explanatory materials, paragraph 1.7.

[2] Ibid.

[3] For example, it appears that voluntary action service providers may not otherwise be CDR entities.

[4] For example, data holders who become action service providers, and accredited persons who become accredited action initiators.

[5] The proposed amendments aim to create a clear delineation between the instruction layer (which is regulated by the CDR) and the action layer (which is regulated by existing law). The 'action layer' refers to the process through which the action service provider carries out an action for a consumer, for example making a payment, opening an account, updating details or preferences: see explanatory materials.

[6] Although financial information is not sensitive information within the meaning of the Privacy Act, people often expect that their financial information will be given a high level of protection (see OAIC guide to securing personal information).

The OAIC's starting point for this submission is that the privacy framework for CDR action initiation should be complete, meaning no CDR consumers are left without privacy protection when they participate in action initiation, and no CDR action initiation entities are able to handle personal information in an unregulated way, without oversight or accountability (see Parts 6 and 7). The framework should also be clear, in the sense that consumers and participants can understand the boundaries of the CDR system and its intersection with other regulation (see Parts 5 and 8). Finally, the framework should be consistent, so that consumers can have confidence that they will have the same privacy rights, regardless of which action initiation entity they choose to engage with (see Parts 5, 6 and 7). This will also help participants to understand and comply with their privacy obligations.

The OAIC considers that further work is needed to build a complete, clear and consistent CDR action initiation system in the primary legislation. As currently drafted, we consider the Bill has the potential to leave gaps in privacy protection for CDR consumers in some circumstances, and to result in regulatory overlap in others. We are also concerned that the core privacy framework for action initiation is not clearly articulated in the Bill and the explanatory materials.

In this submission, the OAIC makes several recommendations which we consider would improve the clarity, consistency, and completeness of the action initiation framework. That said, we recognise that there may be other ways to address the matters identified. In light of this, the OAIC seeks to remain engaged with Treasury in relation to the Bill, including as any changes to the privacy framework are considered as a result of this consultation. The OAIC notes that this submission is by necessity focused on highly technical and complex matters of construction and welcomes the opportunity generally to work issues through to find solutions.

Part 2: About the OAIC and our role in the CDR system

The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

The OAIC co-regulates the CDR system with the Australian Competition and Consumer Commission (ACCC). The OAIC enforces the Privacy Safeguards[7] (and related *Competition and Consumer (Consumer Data Right) Rules 2020* (consumer data rules)) and advises on the privacy implications of consumer data rules and data standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

The OAIC's goal in regulating the privacy aspects of the CDR system is to ensure that the system has a robust data protection and privacy framework, and effective accountability mechanisms to ensure consumers' privacy and confidentiality is protected.

[7] For the Privacy Safeguards, see Competition and Consumer Act, sections 56ED - 56EP.

Part 3: About this submission

This submission reflects the time and information available to the OAIC in considering the changes to the CDR system proposed by the Bill.

In preparing this submission, the OAIC has considered the Bill, the summary of proposed changes,[8] the draft explanatory materials,[9] and the privacy impact assessment (PIA) which accompanies consultation on the Bill.[10] The OAIC supports Treasury's decision to conduct a PIA before the Bill is finalised to inform its drafting. So that the legislative design process can benefit from and be informed by the PIA process, we recommend that Treasury have regard to the recommendations in that PIA when finalising the Bill.[11]

This consultation focuses on amendments to the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act) for CDR action initiation. In the existing CDR system, privacy and information security protections are located across several instruments, including the Competition and Consumer Act, the consumer data rules, designation instruments and consumer data standards. It appears a similar approach is proposed for action initiation. While it is appropriate to focus on the Competition and Consumer Act in this consultation, the multi-instrument framework means that subsequent updates to the consumer data rules, the data standards, and other relevant instruments, have the potential to alter or adapt the policy settings in a way stakeholders cannot currently predict. The comments the OAIC is able to provide on this consultation are therefore limited to the information available at this time.

Further, action initiation represents a significant change to the CDR system. As addressed in this submission, action initiation will create new information lifecycles and new CDR entities. This means that the potential privacy and confidentiality implications of CDR action initiation are also significant and complex. In the time available, the OAIC has focused our attention on matters that relate to the structural elements of the Bill and the overall approach to expanding CDR to action initiation. Consequently, this submission generally does not address specific drafting matters raised by the Bill. We seek to remain engaged with Treasury on these matters moving forward.

---

[8] Treasury, Summary of proposed changes - Exposure draft legislation to enable action initiation in the Consumer Data Right (treasury.gov.au), accessed 21 October 2022.

[9] Treasury, Exposure Draft Explanatory Memorandum: Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right - Implementing action initiation, accessed 21 October 2022.

[10] Treasury, PIA on the introduction of Action Initiation in the Consumer Data Right (treasury.gov.au),accessed 21 October 2022.

[11] See the OAIC's Guide to undertaking privacy impact assessments - Home (oaic.gov.au). See also the Inquiry into Future Directions for the Consumer Data Right - Final Report (treasury.gov.au) ('Future Directions Report'), recommendation 7.11, which recommended that '*the privacy impact assessment and information security assessment should consider appropriate protections, proportionate to the risks involved for action initiation authorisation, consent and instruction data and, if warranted, identify protections that need to be put in place… The assessments should occur before the legislation is settled to determine what should be captured in the primary legislation, the Rules or Standards*'.

Part 4: Summary of recommendations

Recommendation 1

The Bill and/or explanatory materials make clear what the intended boundaries of the CDR privacy framework are, which data flows are intended to be covered by the Privacy Safeguards, how the Privacy Safeguards interact with the APPs, and if/when the Privacy Safeguards are intended to be replaced by the APPs for action initiation data.

Recommendation 2

Treasury revisit the concept of CDR data in the context of action initiation and consider whether it is possible to amend the definition of CDR data or to use any other drafting mechanism, together with declaration and designation instruments, to ensure that only CDR data moves through the CDR system.

Recommendation 3

Treasury revisit the drafting of the Bill to ensure that the Privacy Safeguards apply to accredited action initiators when they collect, use or disclose CDR data (for which there is one or more CDR consumer) in the CDR action initiation system. This should be clear on the face of the legislation.

Recommendation 4

Treasury engage with the Attorney-General's Department about applying the Privacy Act to action service providers, regardless of their status. We ask that Treasury consult with and involve the OAIC as part of this engagement.

Recommendation 5

Treasury consider whether the existing language in subsection 6E(1D) of the Privacy Act would adequately protect all personal information handled by small business operators who are accredited persons in CDR action initiation. We recommend that Treasury engage with the Attorney-General's Department about this matter, and involve the OAIC in this engagement.

Recommendation 6

The Bill be amended so that significant elements of the CDR action initiation privacy and security framework, including the framework for consent, authorisation and authentication, are included in the Competition and Consumer Act.

Recommendation 7

If key elements of the CDR privacy framework will be dealt with the consumer data rules, this should be stated and explained in the explanatory materials.

Part 5: Clarity about the privacy framework for CDR action initiation

It is important that CDR consumers who would like to understand how their privacy is protected in the CDR action initiation system are able to do so. While many consumers will not be able to navigate the privacy provisions in CDR legislation and other instruments (and should not be expected to do so), the general privacy framework for action initiation should be comprehensible to consumers at a high level.[12] This will help consumers to have trust in the CDR system, and to understand how they can seek redress in relation to the handling of their information through CDR action initiation if needed.

It is also important that action initiation entities can understand and implement their privacy obligations in relation to CDR action initiation. This includes so that action initiation entities understand and do not unintentionally breach their obligations, and so that they can clearly communicate with consumers about their privacy practices (including through notices, their CDR policy and privacy policy).

The OAIC considers the privacy framework presented in the Bill is complex and lacks clarity. As outlined in Part 6, there appear to be circumstances in which the Privacy Safeguards will not apply to information handled through CDR action initiation processes. As explained in Part 7, it appears that the Privacy Act and Australian Privacy Principles (APPs) may apply in some of these cases, but not others. If the Bill were passed as drafted, we consider it would be extremely difficult for consumers and CDR participants to navigate and understand the complex relationship between these different privacy protections. While there is a role for guidance in providing clear and accessible explanations of regulatory frameworks, the OAIC considers the complexity in this particular framework creates a challenge to developing sufficiently accessible guidance to provide participants and consumers with the necessary clarity.

Further, while the explanatory materials indicate the CDR system will generally regulate the 'instruction layer' of an action,[13] this concept is not clearly defined in a technical sense. This means the intended boundaries of the CDR system are not clear. For example, if an accredited action initiator collected information through usual business practices unconnected with the CDR, and a consumer later consents to the accredited action initiator using that information to prepare an instruction, it is not clear whether and when CDR is intended to regulate that information.

If the boundaries of the CDR action initiation framework, and its intersection with other privacy regulation, are not clear this creates risk in the CDR system; for consumers to understand when and how their data is protected, and participants to understand their compliance obligations. We recommend the Bill and/or explanatory materials make clear what the intended boundaries of the CDR privacy framework are, which data flows are intended to be covered by the Privacy Safeguards, how the Privacy Safeguards interact with the APPs, and if/when the Privacy Safeguards are intended to be replaced by the APPs for action initiation data.

---

[12] See also Future Directions Report page 179, which indicated that '*consumers will interact with the CDR as one holistic regime and should not be expected, nor need, to understand how certain functions or data sets within the CDR are protected in different ways. However, being able to clearly understand that protections and safeguards do apply to their data, and where to seek redress, will be paramount.*'

[13] Explanatory materials, paragraph 1.12.

Recommendation 1: The Bill and/or explanatory materials make clear what the intended boundaries of the CDR privacy framework are, which data flows are intended to be covered by the Privacy Safeguards, how the Privacy Safeguards interact with the APPs, and if/when the Privacy Safeguards are intended to be replaced by the APPs for action initiation data.

Part 6: Consistency in applying the Privacy Safeguards to CDR action initiation

The Privacy Safeguards are the cornerstone of privacy protection in the CDR system, and it is appropriate that Treasury consider and build on these safeguards when designing the privacy framework for CDR action initiation.[14] However, the safeguards were designed to provide protections to consumers whose data is being collected, used and disclosed in CDR data sharing. The lifecycle of consumer information, and associated risks, in CDR action initiation differ from CDR data sharing in key ways.[15] Importantly, while a main purpose of CDR data sharing is the collection, use and disclosure of consumers' information, the handling and movement of consumer data is only incidental to CDR action initiation (the key purpose of which is to provide instructions to act on consumers' behalf). This creates challenges in adapting the Privacy Safeguards to CDR action initiation.[16]

At a high level, we understand that Treasury intends to apply the Privacy Safeguards to accredited action initiators who are or may become accredited data recipients of CDR data,[17] and a limited number of Privacy Safeguards to action service providers in relation to CDR data.[18] While the Bill proposes various amendments to the Privacy Safeguards to achieve this result, the OAIC considers a more fulsome review is needed to ensure the Privacy Safeguards operate as intended to adequately protect action initiation consumers' privacy.

In particular, the OAIC considers there is a risk that the interaction between existing definitions in the Competition and Consumer Act, proposed definitions in the Bill, and proposed amendments to the Privacy Safeguards could create inconsistent and fragmented privacy protections for CDR consumers, and potentially duplicative obligations for action initiation participants. This section outlines two areas of particular concern, regarding non-CDR data and the status of accredited action initiators.

---

[14] This appears to be the intended approach outlined in the explanatory materials, which indicate that '*CDR action initiation builds on the existing infrastructure, objectives and principles underpinning the current data sharing framework, within sectors that are already designated for data sharing*': explanatory materials, paragraph 1.4.

[15] Diagram 1.1 on page 13 of the explanatory materials demonstrate some of the differences in the action initiation information lifecycle compared with the data sharing lifecycle. Key risks associated with action initiation are summarised in the introduction to this submission. See also Chapter 7 in the Future Directions Report and pages 4–5 of the OAIC's submission to the Inquiry into Future Directions for the Consumer Data Right (treasury.gov.au).

[16] The Future Directions Report also noted that the Privacy Safeguards are crafted to provide protections to data being collected and used in the context of CDR data sharing and this limits the ease with which they can be readily adapted to provide equivalent or tailored protections for action initiation: Future Directions Report, page 177.

[17] Explanatory materials, paragraph 1.127.

[18] Explanatory materials, paragraph 1.129. See also Bill, items 73, 76, 79 and 83, sections 56ED, 56EF, 56EG, 56EM and 56EN.

To address these issues, the OAIC recommends that the Bill is amended to ensure the Privacy Safeguards apply appropriately and consistently to accredited action initiators and action service providers in relation to consumer data handled through CDR action initiation.

Non-CDR data collected, used or disclosed through CDR action initiation

The Bill and explanatory materials suggest that accredited action initiators and action service providers will be able to collect, use and disclose non-CDR data through CDR action initiation processes. Relevantly, the Bill provides that the Minister may make rules relating to information that is not CDR data but relates to a CDR action.[19] The explanatory materials indicate that this is to reflect that accredited action initiators and action service providers may receive non-CDR data related to their functions,[20] and instructions may include non-CDR data.[21]

Various privacy and security-related provisions in the Competition and Consumer Act and CDR instruments, including the Privacy Safeguards, apply only in relation to CDR data.[22] As drafted, the Privacy Safeguards would not apply to non-CDR data collected, used or disclosed in CDR action initiation processes.

The Competition and Consumer Act defines 'CDR data' by reference to information the Minister has specified in sectoral designation instruments.[23] Because the definition of CDR data is tied to designation instruments, certainty about the information that will become CDR data or how much of this information could be handled in CDR action initiation is reliant on future designation instruments. Similarly there is no present certainty about how much non-CDR data could be collected, used or disclosed through CDR action initiation, and whether any of this data will be personal information. Depending on the future designation instruments, this means that personal information (potentially including sensitive information) that moves through the CDR system may not be CDR data, and therefore won't be regulated by the Privacy Safeguards.

The PIA suggests that non-CDR data involved in action initiation could be personal information.[24] For example, based on statements in the PIA,[25] it appears that data an accredited action initiator collects

[19] Bill, item 40, section 56BGA(1)(g).

[20] Explanatory materials, paragraph 1.102.

[21] Explanatory materials, paragraph 1.50.

[22] For the Privacy Safeguards, see Competition and Consumer Act, subsection 56EB(1) and sections 56ED–56EP.

[23] Competition and Consumer Act, subsection 56AI(1): 'CDR data' is information within a class specified in a designation instrument (as described subsection 56AC(2)(a)), or information wholly or partly derived from that information (including indirectly derived information). Existing designation instruments specify broad classes of information, including information about customers and users in the sector, and information about those persons' use of relevant products: see Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, sections 6–9; Consumer Data Right (Energy Sector) Designation 2020, sections 7–10; Consumer Data Right (Telecommunications Sector) Designation 2022, sections 6–9.

[24] See PIA, paragraph 5.2.7–5.2.9. Relevantly, those paragraphs indicate '*there would be situations where data that is not designated CDR data is provided by a consumer to an AAI as part of an action initiation request*', '*data may also flow back from the ASP to the AAI through the instruction layer as part of the action initiation process*', and '*it is proposed that any data that the consumer shares with the AAI that is not designated under existing designations or under future action initiation declarations (i.e. CDR data) would not be in scope of the Privacy Safeguards. Instead, any non-CDR data would be subject to the APPs…*'.

[25] See PIA, paragraph 5.2.7–5.2.8.

through screen scraping or directly from a consumer, and uses to prepare and make a valid instruction, may be personal information but not CDR data. It also appears that information an action service provider collects through an instruction, and uses or discloses to notify an accredited action initiator about the outcome of an action, may be personal information that is not CDR data.

If non-CDR data that is personal information is not covered by the Privacy Safeguards, this will create a highly complex privacy framework for CDR action initiation. For example:

- if an accredited action initiator concurrently disclosed CDR data and non-CDR data that is personal information through an instruction, the Privacy Safeguards would apply in relation to the CDR data, but not the non-CDR data
- if the disclosure involved no CDR data, the Privacy Safeguards would not apply at all.

Depending on the entity involved, different information subject to the same CDR action initiation process could be regulated by the Privacy Safeguards, the APPs, and/or by no privacy protections (for application of the Privacy Act, see Part 7). This risks an inconsistent and fragmented privacy framework for CDR consumers and participants. In our view, it would also be inconsistent with consumers' reasonable expectation of robust privacy protection in the CDR system. As explained further below, this approach would also create a complex regulatory and enforcement framework.

The PIA indicates that the proposed approach to non-CDR data '*would be consistent with the current approach to data sharing, where the ADR may offer additional services to CDR data sharing which involve data outside the scope of the CDR*'.[26] The OAIC does not understand that this is the case. While the CDR data sharing system does not regulate accredited persons when they are providing services outside the CDR system using non-CDR data, the consumer information an accredited person collects, uses and discloses through a CDR consumer data request is CDR data, and therefore consistently protected by the Privacy Safeguards. The existing framework has been designed to make clear to consumers when services are provided within or outside of the CDR system, meaning consumers can have confidence that when their information is shared through a consumer data request, it is protected by the Privacy Safeguards. In contrast, it appears that core CDR action initiation services could involve non-CDR data, which may result in fragmented protection of consumers' data within the CDR system. This would not be consistent with the current approach in CDR data sharing.

Conceptually, and for regulatory integrity and consistency with CDR data sharing, we suggest a position that only CDR data should be permitted to move through instructions and outcome notifications in the CDR system. Achieving this policy outcome would ensure the consistent application of the privacy safeguard framework, and the application of regulatory and enforcement oversight across the CDR system. We therefore recommend that Treasury revisit the concept of CDR data in the context of action initiation and consider whether it is possible to amend the definition of CDR data or to use any other drafting mechanism, together with declaration and designation instruments, to achieve this. Doing so would avoid the fragmentation and inconsistency which will arise from having non-CDR data routinely entering the CDR system once action initiation commences.

[26] PIA, paragraph 5.2.8.

Recommendation 2: Treasury revisit the concept of CDR data in the context of action initiation and consider whether it is possible to amend the definition of CDR data or to use any other drafting mechanism, together with declaration and designation instruments, to ensure that only CDR data moves through the CDR system.

Accredited action initiators as accredited data recipients

The explanatory materials indicate that the Privacy Safeguards will apply to an accredited action initiator for a type of CDR action, where that person is or may become an accredited data recipient of CDR data.[27] However, all Privacy Safeguards will not apply to accredited action initiators who 'may become' accredited data recipients for data they handle through CDR action initiation processes. Further, it appears that accredited action initiators may never become accredited data recipients for all relevant CDR data, meaning the Privacy Safeguards would not consistently apply to these entities.

Currently, most Privacy Safeguards (5–13) only apply to accredited persons in their capacity as an accredited data recipient,[28] and the Bill does not propose to alter this approach.[29] There is no mechanism in the existing Competition and Consumer Act or the Bill to apply Privacy Safeguards 5–13 to accredited action initiators who 'may become' accredited data recipients for CDR data, meaning these safeguards would not apply to those entities. If an accredited action initiator is not an accredited data recipient for information it uses to prepare and make an action initiation instruction, there also does not seem to be any mechanism for the Privacy Safeguards to apply.

While the Bill provides that all accredited action initiators must be accredited persons,[30] an accredited person only becomes an accredited data recipient for CDR data if the data was disclosed to the person '*under the consumer data rules*'.[31] Under current consumer data rules, CDR data is generally disclosed to accredited persons by other CDR participants (i.e. data holders and accredited data recipients).[32] Accredited persons who collect data outside the CDR system (e.g. from a third party or directly from consumers) do not usually become accredited data recipients for that data. This reflects that the CDR privacy framework is generally focused on consumer information that has been collected, used or disclosed within the CDR data sharing system.

Unlike CDR data sharing, it appears that CDR action initiation will routinely involve accredited persons using and disclosing CDR data they receive *outside* the CDR data sharing system to prepare and make instructions *within* the CDR action initiation system.[33] It is not clear whether this data will always have

[27] Explanatory materials, paragraph 1.127.

[28] Competition and Consumer Act, sections 56EH–56EP.

[29] Bill, items 77–85.

[30] Bill, item 34, section 56AMC.

[31] Or derived from that data: Competition and Consumer Act, subsection 56AK(c). The Bill proposes a note following this definition, indicating an accredited initiator may become an accredited data recipient where '*CDR data [is] disclosed under the consumer data rules to the person as an accredited action initiator*': Bill, item 32, section 56AK.

[32] See consumer data rules, including Division 4.4 (authorisations to disclose CDR data), Subdivision 4.2 (consumer data requests made by accredited persons to CDR participants), rule 1.10A (types of consents) and rule 7.5 (meaning of permitted use or disclosure and relates to direct marketing).

[33] See explanatory materials, paragraph 1.50, which indicates that a consumer is not required to '*use CDR data sharing before accessing action initiation*' and '*it is possible for a consumer to approach or request an accredited action initiator to instruct for*

been disclosed to the accredited person '*under the consumer data rules*'. It is therefore unclear whether an accredited action initiator will be an accredited data recipient for data it uses and discloses through the CDR action initiation system. Example 1.4 in the explanatory materials outlines a situation where an accredited action initiator makes an instruction through CDR, without taking '*any step in an accredited data recipient*' capacity, which suggests accredited action initiators will not always be accredited data recipients for data they handle through the CDR system.[34] If an accredited action initiator handles consumer information through the CDR action initiation system, otherwise than as an accredited data recipient, Privacy Safeguards 5–13 will not apply. On the current drafting, and subject to the consumer data rules, it is also unclear how Privacy Safeguards 1–4 would apply in these circumstances.

As with non-CDR data, this is likely to cause significant complexity in the CDR privacy framework. It appears that for a single CDR action initiation process, an accredited action initiator could simultaneously be bound by the Privacy Safeguards, the APPs, and/or no privacy regulation, depending on the nature of the data and whether the entity is covered by the Privacy Act for the data. In our view there are significant risks if a CDR action initiation framework results in the Privacy Safeguards applying inconsistently to CDR entities for the same data handling activity.

Even if consumer data rules will be drafted to ensure that an accredited action initiator will become an accredited data recipient for data collected outside, but handled within, the CDR system, there is nothing in the Bill that governs this. The explanatory materials also do not set out these matters. As explained further in Part 8, the OAIC considers that for clarity and certainty, it is essential that the core framework for consumer privacy and confidentiality in the CDR system is clear in the primary legislation.

The OAIC recommends Treasury revisit the drafting of the Bill to ensure that when accredited action initiators are collecting, using or disclosing CDR data for the purposes of preparing or making a CDR action initiation instruction, they are bound by the Privacy Safeguards. We suggest Treasury consider the clearest way to do this, for example through an amendment to the definition of 'accredited data recipient' or through amendments to the Privacy Safeguards themselves. We recommend this matter is addressed in the Bill, rather than in the consumer data rules. As explained further in Part 7, we also recommend Treasury consider and engage in relation to a concurrent amendment to the Privacy Act.

Recommendation 3: Treasury revisit the drafting of the Bill to ensure that the Privacy Safeguards apply to accredited action initiators when they collect, use or disclose CDR data (for which there is one or more CDR consumer) in the CDR action initiation system. This should be clear on the face of the legislation.

Impact on regulation of the CDR system

In order for privacy and confidentiality to be effectively protected in CDR action initiation, the Information Commissioner must be able to monitor and enforce relevant privacy and confidentiality

an action on their behalf, without the consumer first having their CDR data shared between a data holder and accredited data recipient'.

[34] Explanatory materials, example 1.4, page 16.

protections. In addition to the matters outlined above, applying the Privacy Safeguards in the way proposed in the Bill could have a significant impact on the Information Commissioner's ability to effectively regulate the privacy-related aspects of CDR action initiation.

The Information Commissioner has a range of functions and powers under both the Privacy Act and the Competition and Consumer Act directed towards protecting the privacy of individuals by ensuring the proper handling of personal information. These functions and powers enable the Information Commissioner and OAIC to effectively co-regulate the CDR system with the ACCC.

The Information Commissioner's powers under the Competition and Consumer Act generally only apply in relation to the Privacy Safeguards, or consumer data rules related to the Privacy Safeguards or the privacy or confidentiality of CDR data. Subject to any privacy-related consumer data rules made for action initiation, this means that many of the Information Commissioner's compliance and enforcement powers will not be engaged if:

- an accredited person is not an accredited data recipient for relevant CDR data (so is not bound by all relevant Privacy Safeguards), or
- an action initiation entity handles non-CDR data through action initiation processes (so is not bound by any Privacy Safeguards).

Importantly, this includes the Commissioner's powers to conduct an assessment relating to the management and handling of CDR data,[35] investigate acts or practices that may breach the Privacy Safeguards (if they applied),[36] and accept enforceable undertakings or seek injunctions in relation to compliance with the Privacy Safeguards (if they applied).[37]

In some circumstances, equivalent powers may be engaged under the Privacy Act.[38] However, there are differences in the scope of entities' obligations under the Privacy Act (noting the APPs tend to be less prescriptive than the Privacy Safeguards) and accordingly, the Information Commissioner's powers. As explained in Part 7 of this submission below, there also appear to be situations in which the Privacy Act, including the APPs and the notifiable data breaches scheme, may not apply to an action initiation entity. This would mean the Information Commissioner may have no power to regulate and enforce the handling of personal information through CDR action initiation. This could also present difficulties for the handling of complaints by recognised CDR external dispute resolution schemes.

In our view, regulatory gaps of this kind would undermine the integrity of privacy and confidentiality protections in the CDR system, which would in turn have a negative impact on consumer confidence in the CDR system overall. For example, while the Information Commissioner regulates the privacy aspects of the CDR system, due to the regulatory gap, the OAIC may not be able to handle a complaint in relation to all personal information handling through CDR action initiation. We therefore restate

[35] Competition and Consumer Act, section 56ER.

[36] Competition and Consumer Act, section 56ET.

[37] Competition and Consumer Act, sections 56EW and 56EX.

[38] For example, the Information Commissioner's powers to conduct assessments relating to the APPs and certain other matters (Privacy Act, section 33C), conduct investigations (Privacy Act, Part V), accept enforceable undertakings (Privacy Act, section 80V) and seek injunctions (Privacy Act, section 80W).

our above recommendations that Treasury consider options to rectify the identified Privacy Safeguard issues created by the Bill.

Part 7: Privacy Act coverage for all action initiation entities

In the current CDR system, all accredited persons are regulated by the Privacy Act in relation to personal information that is not CDR data.[39] This is an important safety net. It allows consumers to have confidence that entities accredited to receive their information through the CDR system have privacy obligations, even where Privacy Safeguards may not apply, or the accredited person is providing services outside the CDR system. It also ensures that the personal information handling practices of accredited persons can be effectively monitored and regulated, and that entities have certainty about their privacy obligations. While existing provisions will mean that the Privacy Act applies to all accredited persons who are accredited action initiators, the Bill does not propose to apply the Privacy Act to all action service providers.

The OAIC's view is that as in CDR data sharing, as a safety net for consumer privacy the Privacy Act should apply to CDR entities who receive consumer information through CDR action initiation (i.e. action service providers and accredited action initiators). This would ensure there is protection for the handling of personal information by action initiation entities in all circumstances. It would also mitigate the risk that, in future, action initiation entities could handle personal information connected with the CDR in a way that is unregulated and inconsistent with CDR consumer expectations.

To this end, and as explained in this part, the OAIC recommends that Treasury engage with the Attorney-General's Department about applying the Privacy Act to all action service providers (regardless of their status). We also recommend Treasury engage with the Attorney-General's Department regarding the existing application of the Privacy Act to accredited persons, to ensure it remains fit for purpose in the context of CDR action initiation. We recommend Treasury consult with and involve the OAIC in this engagement with the Attorney-General's Department.

Action service providers that are small business operators

The Bill is drafted so that only a limited number of Privacy Safeguards will apply to action service providers.[40] At a high level, Privacy Safeguards will only apply when action service providers are collecting CDR data from a CDR participant under (or purportedly under) the consumer data rules,[41] and in relation to data the action service provider has disclosed under the consumer data rules.[42] This means the Privacy Safeguards generally will not apply to an action service provider in relation to the

[39] Privacy Act, section 6C and subsection 6E(1D).

[40] These are Privacy Safeguard 1 (open and transparent management of data), Privacy Safeguard 3 (soliciting CDR data from CDR participants under the consumer data rules), Privacy Safeguard 4 (dealing with unsolicited CDR data from participants in CDR); Privacy Safeguard 10 (notifying of the disclosure of CDR data), Privacy Safeguard 11 (quality of CDR data), and Privacy Safeguard 13 (correction of CDR data). The explanatory materials indicate this is intended to '*manage risks associated with the flow of CDR data in the instruction layer*' and '*risks [that] are specifically attributable to the CDR*': explanatory materials, paragraph 1.132.

[41] Privacy Safeguards 3 and 4.

[42] Privacy Safeguards 10, 11 and 13. Note that Privacy Safeguard 1 also applies to action service providers generally.

use or disclosure of personal information, or the collection of information otherwise than under (or purportedly under) the consumer data rules. Instead, the Privacy Act and APPs are intended to be the primary source of privacy obligations for action service providers, subject to existing exemptions in that Act.[43]

The Privacy Act and APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.[44] Among other things, the Privacy Act generally requires organisations to only collect personal information if the information is reasonably necessary for one or more of the organisation's functions or activities.[45] The Privacy Act also requires entities to destroy personal information (or ensure it is deidentified) where it no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs (unless an exception applies).[46] Further, the notifiable data breaches scheme in the Privacy Act requires entities to notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Currently, and with some exceptions, the Privacy Act does not apply to organisations with an annual turnover of less than $3 million (small business operators).[47] As the Bill does not propose to alter this exemption for action service providers in the CDR system, where action service providers are small business operators, they generally will not be covered by the Privacy Act. This means that where the Privacy Safeguards do not apply, action service providers who are small business operators may have no privacy obligations in relation to personal information collected through CDR action initiation.

The OAIC's view is that facilitating the disclosure of personal information to action service providers who are not bound by the Privacy Act, and therefore have fragmented and incomplete privacy obligations in relation to that information, would be inconsistent with CDR consumers' expectations. It may also undermine trust in the CDR as a safe and secure system.

The OAIC appreciates that all declared action service providers will be data holders, and currently no active data holders would be small business operators within the meaning of the Privacy Act. However, we consider that the legislation for CDR action initiation should be forward-looking and drafted to guard against risks to privacy in the future rollout of the system. These risks include that:

- the Bill provides for the Minister to approve persons who are not data holders to become 'voluntary action service providers',[48] and it appears these voluntary action service providers could be small business operators and therefore not regulated by the Privacy Act, and
- as the CDR rolls out to new sectors for data sharing and action initiation, it appears that at some stage data holders who are declared as action service providers may be small business operators and therefore not regulated by the Privacy Act. Unlike other data holders, a central part of these action service providers' role will be to collect new consumer data through the CDR. This creates risks which do not exist for other data holders, who will always have a pre-

[43] Explanatory materials, paragraph 1.131.

[44] Australian Privacy Principles Guidelines, Chapter A: Introductory matters (oaic.gov.au), paragraph A.6.

[45] See APP 3.

[46] See APP 11.

[47] See Privacy Act, section 6C.

[48] Bill, item 34, subsection 56AMB(2).

existing relationship with the consumer and whose primary position in the CDR system is to disclose data they have already collected outside the CDR system.

The OAIC recognises that under the Bill, the consumer data rules may include rules regarding the criteria for a person to be approved as a voluntary action service provider,[49] and this could include a requirement to consider existing privacy protections that apply to the person seeking approval.[50] If the consumer data rules made Privacy Act coverage a criterion for entities to become voluntary action service providers, this could partially mitigate the risk that action service providers will not be regulated by the Privacy Act.[51] However, we do not consider this is a complete and robust solution, especially noting our above comments about whether small business operators may be declared as action service providers in future. For the reasons outlined in Part 8, our view is also that it is preferable that this matter is dealt with in enabling legislation, rather than future rules.

Separately, we note that in the OAIC's submission to the Attorney General's Department's Discussion Paper on the Review of the Privacy Act, we recommended that the small business exemption be removed from the Privacy Act.[52] If this change were made, it would ensure Privacy Act coverage for action service providers, regardless of their annual turnover (subject to any other applicable exemptions). However, as the Bill will enable action service providers to collect data through the CDR system and execute actions using that data, it is necessary for the privacy obligations of action service providers to also be considered as part of the broader process involved in this Bill. This would reflect the approach taken to accredited persons in subsection 6E(1D) of the Privacy Act and limit coverage gaps through aligning the timing of action initiation in the CDR with amendments to the scope of the privacy obligations.

The OAIC therefore recommends that Treasury engage with the Attorney-General's Department about applying the Privacy Act to action service providers, regardless of their status. We suggest Treasury consider and engage about whether this could be achieved through a provision similar to subsection 6E(1D), which applies the Privacy Act to accredited persons. We recommend Treasury consult with and involve the OAIC in this engagement.

Recommendation 4: Treasury engage with the Attorney-General's Department about applying the Privacy Act to action service providers, regardless of their status. We ask that Treasury consult with and involve the OAIC as part of this engagement.

Accredited action initiators that are small business operators

If a small business operator is an accredited person, subsection 6E(1D) of the Privacy Act will mean that the Privacy Act applies to that entity in relation to personal information that is not CDR data. We understand that as accredited action initiators will be accredited persons,[53] the Privacy Act would apply

[49] Bill, item 48, paragraph 56BHA(1)(b).

[50] Explanatory materials, paragraph 1.108.

[51] Noting that small business operators could elect to become covered by the Privacy Act under existing processes in that Act: Privacy Act, section 6EA.

[52] Privacy Act Review Discussion Paper submission (oaic.gov.au), recommendation 17.

[53] Bill, item 34, section 56AMC.

to these entities in the same way. This means all accredited action initiators will have some Privacy Act coverage.

However, as explained in Part 6, the Competition and Consumer Act defines CDR data by reference to the data specified in designation instruments,[54] and existing designation instruments specify broad classes of information.[55] While the designation instruments also specify data holders,[56] the instruments do not always clearly require the specified classes of information to be held by (or on behalf of) specified data holders. This means that some personal information held by an accredited person may be CDR data, even if the accredited person did not collect that information through the CDR system.

Together, the drafting of subsection 6E(1D) in the Privacy Act and the definition of CDR data in the Competition and Consumer Act mean that accredited persons who are small business operators will not be regulated by the Privacy Act in relation to data that *is* CDR data. This could leave gaps in privacy protection for CDR consumers. For example, as noted in Part 6, there may be circumstances in which neither the Privacy Safeguards nor APPs apply to a consumer's personal information,[57] or where the notifiable data breaches scheme does not apply to an accredited person in relation to certain CDR data that is personal information.[58]

As outlined above, the OAIC's view is that this would be inconsistent with consumer expectations and may undermine trust in the CDR system. Our view is that this potential gap in privacy protection could impact consumers in both CDR data sharing and action initiation, and should be closed for the benefit of all CDR consumers. That said, we consider the gap is more likely to eventuate in CDR action initiation. This is because in CDR data sharing, the Privacy Safeguards will generally apply in relation to the CDR data an accredited person collects, uses and discloses. As outlined in Part 6, there appear to be gaps in the application of the Privacy Safeguards to accredited persons in action initiation. This means an accredited action initiator may be more likely than other accredited persons to have no privacy obligations in relation to a consumer's personal information.

The OAIC therefore recommends that Treasury consider whether the existing language in subsection 6E(1D) of the Privacy Act would adequately protect all personal information handled by small business operators who are accredited persons in CDR action initiation. We recommend Treasury also

[54] Competition and Consumer Act, subsection 56AI(1).

[55] See Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, sections 6–9; Consumer Data Right (Energy Sector) Designation 2020, sections 7–10; Consumer Data Right (Telecommunications Sector) Designation 2022, sections 6–9.

[56] Designation instruments specify the persons who hold specified classes of information, or on whose behalf the information is held: Competition and Consumer Act, section 56AC(2)(b). These entities will be data holders for that information under section 56AJ(2).

[57] For example, if CDR data was disclosed to an accredited person otherwise than under the consumer data rules (e.g. from a consumer or third party), and the data was not derived from data collected under the consumer data rules, the accredited person would not be an accredited data recipient for that data: Competition and Consumer Act, subsection 56AK(c). As outlined in Part 6, Privacy Safeguards 5–13 would not apply to the accredited person in relation to that data. As the information is CDR data, the Privacy Act also would not apply to the accredited person in relation to that data, leaving a gap in the privacy obligations of the accredited person.

[58] See the example in footnote 57. In this case, the Competition and Consumer Act would not apply the notifiable data breaches scheme to the accredited person, because section 56ES applies to accredited data recipients (but not all accredited persons). As the data is CDR data, the notifiable data breaches scheme in Part IIIC of the Privacy Act also would not apply.

engage with the Attorney-General's Department about this matter, and involve the OAIC in this engagement.

Recommendation 5: Treasury consider whether the existing language in subsection 6E(1D) of the Privacy Act would adequately protect all personal information handled by small business operators who are accredited persons in CDR action initiation. We recommend that Treasury engage with the Attorney-General's Department about this matter, and involve the OAIC in this engagement.

Part 8: Balance between legislation and other instruments

The OAIC acknowledges the need to tailor the regulatory framework for different sectors and action types as the CDR is rolled out to action initiation. However, to the extent possible, the OAIC considers that the core privacy framework should be included in primary legislation.[59] This will assist consumers and participants to understand the privacy protections applicable in CDR action initiation. It will also guard against inadvertent or unforeseen risks to privacy by preventing deviation from core requirements and ensuring consistency with central privacy and security principles across sectors and participation types (i.e. data sharing and action initiation).

On its own, the Bill does not present the complete framework for privacy and security in CDR action initiation. While the Bill includes some core privacy protections,[60] many features of the privacy framework have been left for the consumer data rules or consumer data standards. This includes requirements related to consent, authorisation and authentication. While the OAIC recognises that the approach in the Bill is similar to the approach taken in the legislation for CDR data sharing, we consider there are opportunities for further detail to be included in the Bill.

For example, Treasury has proposed a new section 56BZB, which would require accredited persons to only initiate a CDR action in accordance with a consumer's valid request. This creates a foundation for ensuring that action initiation requests are consumer driven, while appropriately leaving detailed process requirements to the consumer data rules and standards. We suggest Treasury consider taking a similar approach to including core privacy requirements in the legislation. Establishing significant elements of the privacy framework for action initiation in this way will help to limit and guard against later expansions to the scope of the CDR action initiation system outside of legislative processes. This approach would also solidify that privacy and security are fundamental to the CDR, and critical to ensuring consumer privacy is protected, thereby building and maintaining consumer trust in the CDR system.

To this end, we recommend that where possible, key features of the privacy and security framework should be included in the Bill, rather than consumer data rules or other instruments. In any event, we recommend whichever approach Treasury adopts, it should clear on the face of the Bill and explanatory

[59] On this point, see also the OAIC's submission in response to the Statutory Review of the Consumer Data Right - Issues Paper (treasury.gov.au).

[60] This includes the Privacy Safeguards, section 56BZB (which provides that accredited persons may only initiate CDR actions in accordance with a consumer's valid request), and section 56AMC (which requires the entities who may initiate an action on a consumer's behalf to be accredited).

materials. Where the matter will be dealt with in the consumer data rules this should be stated in the explanatory materials.

Recommendation 6: The Bill be amended so that significant elements of the CDR action initiation privacy and security framework, including the framework for consent, authorisation and authentication, are included in the Competition and Consumer Act.

Recommendation 7: If key elements of the CDR privacy framework will be dealt with the consumer data rules, this should be stated and explained in the explanatory materials.