Australian Government
The Treasury

Consumer Data Right

Government Response to the *Inquiry into Future Directions for the Consumer Data Right*

consumers · choice · convenience · confidence

December 2021

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Government Response to the Final Report of the *Inquiry into Future Directions for the Consumer Data Right*

Executive Summary – Government response to the *Inquiry into Future Directions for the Consumer Data Right* (the Inquiry)

The Inquiry was asked to examine how the Consumer Data Right regime could be expanded in functionality and leveraged with other initiatives in the digital economy. This was aimed at improving consumer (including business) outcomes and supporting competition and innovation.

The Government endorses the findings of the Inquiry that the future of the Consumer Data Right (CDR) should be directed towards: (i) greater consumer data empowerment with deeper functionality, (ii) an economy-wide foundation, (iii) a more integrated data ecosystem; and (iv) realising international digital opportunities. In implementing its response, the Government will be guided by the high-level principles of safety, efficiency and effectiveness of CDR and its clarity in relation to other laws and regulation.[1]

The Inquiry received 73 submissions in response to its Issues Paper, and consulted with a wide range of interested organisations and groups, including representatives from the banking and energy sectors, consumer interest groups, payment systems and service providers, fintechs, mortgage and finance providers, financial service providers and overseas counterparts. Since the release of the Inquiry's Report, the Treasury has conducted further targeted and public consultation to inform the Government's Response; engaging with 75 stakeholders over the course of 35 consultations and receiving 63 submissions, as well as hosting interactive workshops and ongoing, well-attended engagement forums.

The Government will expand the functionality of the CDR regime to include support for consumer-directed third-party action initiation with appropriate consumer and privacy safeguards.[2] This will provide consumers with improved sources of assistance when interacting with their existing or prospective service providers.

Action initiation functionality will be applied in several phases. Its application to banking will prioritise enabling third party payment initiation, complementing current developments and infrastructure in the payment industry. This will enable new, competitive and consumer-focused payment services to develop. The Government will also prioritise CDR being extended to support consumers to manage their existing information and products and eventually to switch to new products and providers, which will bring major savings to households and businesses.[3]

The Government agrees to progress a range of enhancements to CDR data sharing including improving access to CDR-driven services to support the development of a competitive CDR ecosystem; supporting voluntary use of this safer data sharing channel by businesses; and improving consumer control over their data,[4] some of which are already being progressed.[5] The Government disagrees with recommendations relating to the extension of the principle of reciprocity.[6] The reasons for this include that the

[1] Recommendations 1.1 and 1.2.
[2] Action initiation framework: Recommendations 4.1 to 4.23; and consumer safeguards: Recommendations 7.1 to 7.6 and 7.11.
[3] Recommendations 5.1 to 5.13, 5.15, 5.16, and 5.18 to 5.21.
[4] Recommendations 6.1, 6.12 to 6.16, 6.18, 6.19, and 6.21 to 6.24.
[5] Recommendations 6.2 and 6.3 (already progressed), and Recommendations 6.4 to 6.8 (under consideration).
[6] Recommendations 6.9 to 6.11.

sectoral designation process remains the most viable means of expanding the scope of CDR in a targeted, strategic manner, while balancing industry concerns about creating barriers to CDR participation.

The Government notes the recommendations on leveraging the CDR's 'data safety licence' and aligning data safety accreditations[7] and will explore opportunities to leverage the data standards capabilities of the Data Standards Body and the CDR's 'data safety licence', to support the broader digital economy strategy and other Government initiatives.[8]

The Government will engage with international digital standards setting bodies and pursue greater cooperation with other jurisdictions on consumer-directed data portability.[9]

The Government notes a number of recommendations are directed toward independent standard setting or regulatory bodies (including the Data Standards Body[10] and the Australian Securities and Investments Commission[11]) and those for industry attention.[12]

The Government will work with private and public sector stakeholders to develop an integrated roadmap for the prioritised implementation of the CDR reforms.[13] A consumer education campaign will support the sectoral roll out of the CDR. The Government remains committed to encouraging CDR services that focus on the needs of vulnerable consumers and strong consumer and privacy advocate representation in developing the CDR,[14] and notes the recommendation on providing for grants or other support.[15]

Once the key reforms have been put in place and been in operation for 24 months, a post-implementation review will be conducted to assess their operation. This review will also consider whether to prohibit the practice of making payments through giving third party access to consumers' digital banking portals.[16]

The final detail or technical requirements of the proposed reforms will be settled following further stakeholder consultations, including as part of rule making and standard making processes. Similarly, as recommended by the Inquiry, final positions on some recommendations will only be determined following detailed privacy, information security or regulatory impact assessments. Final decisions on the scope of application of payment initiation and action initiation to the banking sector will be subject to further consultation and analysis.

[7] Recommendations 8.5 and 8.6.
[8] Recommendations 8.1 and 8.4 to 8.8.
[9] Recommendations 8.11 to 8.14.
[10] Recommendation 3.1, 8.2, 8.3, 8.9 and 8.10.
[11] Recommendation 5.14.
[12] Recommendation 6.17 and 6.20.
[13] Recommendations 9.1 to 9.3.
[14] Recommendations 7.7, 7.8 and 7.10.
[15] Recommendation 7.9.
[16] Post-implementation review: Recommendation 9.4; and payments through third party access to digital banking portal: Recommendation 5.17.

The Government is committed to maintaining the high levels of privacy protection provided by the CDR. The Government will continue to maintain close consultation with consumer and privacy groups; conducting privacy impact assessments for all key design decisions that may have a substantial impact on privacy; and the ongoing involvement of the Office of the Australian Information Commissioner in the design of the system at the legislative, rulemaking and standard setting stages.

Detailed Government response to the recommendations of the Inquiry

The *Inquiry into Future Directions for the Consumer Data Right* made 100 recommendations that are arranged in 6 parts (generally following the chapter structure of the report):

- Part 1: Action initiation framework – outlines recommendations on how the CDR's functionality should be expanded to include action initiation (Chapter 4);
- Part 2: Action initiation in the banking sector – sets out recommendations on how action initiation should be implemented to support applying for and managing products in the banking sector, including to enable third party initiation of payments with the authority of the consumer (Chapter 5);
- Part 3: Data sharing enhancements – includes recommendations on potential enhancements to the existing CDR ecosystem, including tiered accreditation, support for sharing voluntary data sets, and improvements to consent processes (Chapter 6);
- Part 4: Consumer safeguards – makes recommendations for further consumer safeguards to ensure trust in the CDR, including ensuring appropriate privacy protections (Chapter 7);
- Part 5: Opportunities for connecting the Consumer Data Right to the data economy – makes recommendations to leverage existing CDR infrastructure to support the broader digital economy and to increase engagement internationally (Chapter 8); and
- Part 6: CDR Roadmap and other recommendations – recommends a CDR roadmap for implementing the Inquiry's recommendations, broad guiding principles for the CDR and other recommendations to assist in the implementation of the CDR (Chapters 1, 3 and 9).

Part 1: Action initiation framework

Recommendation	Government response
4.1 – Action initiation through the Consumer Data Right The Consumer Data Right should be expanded to enable third parties, with a consumer's consent, to initiate actions beyond requests for data sharing. This expansion should build on trust developed in the system through the successful operation of the regime in enabling data sharing.	**Agree** Action initiation is complementary to data sharing in enabling third party services to help consumers overcome barriers to decision making and participation by undertaking actions on their behalf. The infrastructure created to enable CDR data sharing arrangements also provides the underlying elements required for action initiation. Leveraging consumer trust in the operation of the current data sharing system will contribute to the successful operation of the CDR as it supports the initiation of actions beyond just requests for data sharing.
4.2 – Framework and sector designation powers for action initiation The expansion of Consumer Data Right functionality to include action initiation should be implemented primarily through amendments to Consumer Data Right framework in the *Competition and Consumer Act 2010*. These amendments should delegate powers to the Consumer Data Right rule maker and Data Standards Chair where appropriate. The amendments should set out the associated powers for the making of Rules and Standards and enable the designation of actions within a sector by the Minister.	**Agree** It is desirable to leverage the existing CDR framework to create a generic action initiation framework. Greater consistency across arrangements for different action types, including data sharing which is a type of action, will promote greater ecosystem adoption of action initiation as participants will face a lower cost burden to build and comply with the requirements.

Recommendation	Government response
4.3 – Sector assessment for action initiation Sectoral assessments should be required prior to the designation of action initiation in a sector. The process for conducting a sectoral assessment for action initiation should be analogous to that for data sharing. Sectoral assessments for action initiation should consider particular classes of actions based on the matters in subsection 56AD(1) of the *Competition and Consumer Act 2010*, adapted as required. Additionally, the sectoral assessment should consider sector-specific regulatory barriers that may prevent action initiation from being facilitated safely, efficiently and effectively, and the digital maturity of the sector to implement action initiation. The OAIC should also consider specific classes of actions when assessing potential privacy and confidentiality implications of designating a sector.	**Agree** Noting that Government will consider lessons-learnt from current assessment and designation processes, including ensuring flexibility to enable designation of data sets and or action types across multiple sectors.
4.4 – Alignment between the Consumer Data Right and sector-specific regulation When conducting sectoral assessments, consideration should be given to whether regulatory and legal changes are required and appropriate to enable action initiation within a sector.	**Agree** Any potential changes will be developed in consultation with sectoral regulators and policy makers.
4.5 – Action initiation process Action initiation through the Consumer Data Right should be based on the existing consent, authentication and authorisation processes currently used for data sharing, with appropriate amendments.	**Agree** It is desirable to leverage the existing CDR framework for the action initiation process. Greater consistency across arrangements for different action types, including data sharing which is a type of action, will promote greater ecosystem adoption of action initiation as participants will face a lower cost burden to build and comply with the requirements.

Recommendation	Government response
4.6 – Supported instructions for action initiation Action initiation in the Consumer Data Right should only enable an accredited person to initiate actions which the consumer is already able to perform with a data holder. Action initiation should not be used to force data holders to perform actions which they would not otherwise offer, or which are prohibited under other regulation. This principle should be used to steer consideration of what actions are designated for action initiation.	**Agree** The CDR will be designed to be a channel for providing instructions to act, rather than playing a role in carrying out those actions (which will be left to service providers to do in line with their existing processes and integrations). This means that the CDR will not seek to create a competing action layer or force data holders to perform actions they would not otherwise offer.
4.7 – Exclusion from action initiation Certain actions that are deemed to be of significant risk to consumers' security or privacy should be excluded from being able to be actioned through the Consumer Data Right. Such actions should be determined through consultation with industry and consumer representatives during the sectoral assessment and implementation within a sector. The updating of passwords is an example of one such excluded action.	**Agree** The Government will consult on options to manage any risks associated with different types of actions. Where risks cannot be adequately managed for a type of action, those actions will be excluded from the CDR.
4.8 – Accreditation for action initiation The accreditation regime should be extended to include tiered accreditation for action initiation, with those actions posing greater potential risk to the consumer requiring higher tiers of accreditation.	**Agree** Information security assessments will be undertaken to determine an appropriate framework for tiering, including which actions require which levels of accreditation (or not require accreditation).
4.9 – Accredited persons' interactions with other regulatory regimes As sectors are designated for action initiation, the relevant sectoral regulators should examine whether additional guidance or education material should be provided to assist persons seeking accreditation understand how the services they propose to provide using the Consumer Data Right could be treated under existing regulatory regimes. Prospective accredited parties should be encouraged to consider these issues.	**Agree**

Recommendation	Government response
4.10 – Consent to send instruction and consent to initiate action Accredited persons should be required to obtain access and usage consents to initiate actions for consumers. These consents should be voluntary, express, informed, specific as to purpose, time-limited and easily withdrawn.	**Agree** The recommended consent requirements are consistent with the existing consent model in CDR Read Access. Details of consent requirements will be settled at the rulemaking and customer experience standard setting stages.
4.11 – Consent processes and consumer experience Action initiation consent processes should be subject to Consumer Experience Standards and Guidelines to ensure that processes produce genuine consent. The Data Standards Chair should consider additional safeguards which balance the need for security with consumer experience where appropriate.	**Agree**
4.12 – Ongoing consent arrangements Consumers should be able to provide consents to accredited persons to initiate actions on their behalf on an ongoing basis, within the consent's time limit. Additional safeguards should also be considered for inclusion in the Rules.	**Agree** The recommended consent requirements are consistent with the existing consent model in CDR Read Access. Details of consent requirements will be settled at the rulemaking and customer experience standard setting stages.
4.13 – Restrictions on unnecessary actions The Rules should restrict accredited persons to only being able to request access consents for actions that are relevant to the provision of a service.	**Agree** This principle for action initiation is consistent with the existing 'data minimisation principle' for data sharing in the CDR rules and which similarly aims to embed consumer safeguards into the regulatory framework. Details of consent requirements will be settled at the rulemaking and customer experience standard setting stages.
4.14 – Authentication requirements by data holders Data holders should be obliged to authenticate consumers prior to requesting action initiation authorisations. Authentication requirements should be reviewed by the Data Standards Body to ensure they reflect the risks associated with action initiation.	**Agree** The details of authentication requirements are to be settled following information security assessments.

Recommendation	Government response
4.15 – More explicit requirements for accredited persons to authenticate customers The Consumer Data Right should include explicit requirements for accredited persons offering action initiation enabled services to authenticate customers in circumstances where there is an ongoing provision of service to that customer. These requirements should be based on international standards on authentication processes.	**Agree**
4.16 – Authorisation to take a specific action Whether the taking of a particular action should require a specific authorisation to be given to a data holder should depend upon the nature of the action requested and other factors, such as the value of the transaction and existing practices and processes in the sector. These requirements should be enabled in the Rules and specified through the Standards.	**Agree** The circumstances in which "step-up" authentication will be required or allowed will be determined through the rulemaking and standard setting processes.
4.17 – Data holders to require explicit consumer authorisation to accept instructions Data holders should only progress actions initiated by accredited persons when they have received the consumer's explicit authorisation to do so. The Data Standards Body should investigate the benefits of enabling fine-grained authorisation for specific action classes, with recommendations being driven by consumer experience and security considerations.	**Agree** The extent to which fine-grained authorisation will be implemented will be determined through standard setting processes.
4.18 – Obligation to act Data holders should be obliged to progress actions initiated by an accredited person for which the consumer has provided a valid authorisation to the same extent as they would otherwise be obliged to progress such an action were the request provided directly by the consumer through another channel. Data holders should not be able to discriminate based on the channel through which the instruction was received.	**Agree** Data holders should not be able to discriminate based on the channel through which the instruction was received, except when justified by the particular risks associated with the channel when permitted by the CDR rules.

Recommendation	Government response
4.19 – Existing data holder obligations Data holders should remain subject to any requirements imposed on them by other regulatory regimes and measures may need to be built into the Consumer Data Right to facilitate this. The Consumer Data Right should similarly contain provisions to assist data holders in managing commercial risks, such as fraud, when assessing actions initiated by accredited persons on the consumer's behalf. Data holders should remain capable of conducting reasonable step-up authentication measures to ensure the validity of any requests. The way in which these measures are conducted should be commensurate to the risk of the action being requested and not detract from the rights of access granted to accredited persons.	**Agree** The CDR will be designed to be another channel for providing instructions to act. This is not intended to change the existing regulatory requirements imposed on data holders. However, the CDR may have a role in ensuring that the data holder receives the information it needs to comply with its own requirements and the regulatory requirements regarding an action requested via the CDR. Information security assessments are required to determine appropriate mechanisms to enable data holders to effectively manage associated risks.
4.20 – General liability for action initiation For action initiation, the general liability framework should extend the principle underpinning the operation of section 56GC of the *Competition and Consumer Act 2010*. This will protect data holders from liability when acting in compliance with the Consumer Data Right regime in response to an action initiation instruction for which they have received the consumer's authorisation to accept. For the avoidance of doubt, the data holder continues to be subject to any regulatory or legal obligations that would otherwise apply if the instruction had come directly from the customer.	**Agree** The recommended principle-based approach to general liability for action initiation is consistent with the current arrangements in place for CDR data sharing. The general liability framework may need to be tailored for different action types. Where there are particular sectoral regulation liability allocation rules for specific classes of action CDR should consider whether it should depart from the general liability allocation rule. The final terms of how liability is allocated will be determined through legislative and rulemaking processes.
4.21 – Notification of action initiation In designing the Consumer Data Right framework, processes should be included to enable consumers to be notified when an action is initiated on their behalf by an accredited person.	**Agree**
4.22 – Cessation Accredited persons should be required to cease acting on the consumer's behalf through the Consumer Data Right when they no longer have a valid consent. Accredited persons should be required to communicate this cessation to the data holders to whom they could previously send actions.	**Agree** This principle for action initiation aims to ingrain consumer safeguards into the regulatory framework.

Recommendation	Government response
4.23 – Record keeping Accredited persons and data holders should be required to keep records of the actions that were initiated through the Consumer Data Right, as well as records of the consumer's consents and authorisations.	**Agree** This principle for action initiation is consistent with the existing framework for data sharing.

Part 2: Action initiation in the banking sector

Recommendation	Government response
5.1 – Designation of the banking sector for action initiation The banking sector designation under the Consumer Data Right should be extended to include action initiation, including payment initiation. The designation process should include thorough regulatory and privacy impact assessments and detailed consultation on the designation instrument prior to a final decision by the Minister. The banking sector designation should specifically set out the classes of general action initiation and payment initiation that should be supported.	**Agree** Noting that the design and implementation of the designation process for action initiation will take into account any lessons learnt from existing CDR designation processes for data sharing in the banking, energy and telecommunications sectors and the CDR Strategic Assessment.
5.2 – Prioritising bank account-to-account payments Bank account-to-account payment initiation through the Consumer Data Right should be prioritised so its design can be coordinated with developments in the Australian payments industry and to expedite the benefits it can bring to customers.	**Agree** As has been the case with CDR Open Banking, it would be expected that the roll-out of payment initiation will be phased to enable efficient and orderly implementation and will take into account the Government response to the Review of the Australian Payments System.

Recommendation	Government response
5.3 – Bank obligation to support Consumer Data Right payment initiation Consumer Data Right payment initiation should apply to all authorised deposit-taking institutions subject to the mandatory data sharing obligation under Open Banking. These authorised deposit-taking institutions should be obliged to provide access to third party payment initiation and process any valid payment instruction received from an appropriately accredited person through the Consumer Data Right, as if it had been provided by the customer through any other digital channel. Banks should continue to be subject to existing obligations placed on them by other regulatory regimes.	**Agree** This is subject to the Government commitment to due process before designation as set out in its acceptance of Recommendation 5.1, with the exact details of the entities, accounts and payment types to be further scoped.
5.4 – Broad and extensible payment instruction functionality Consumer Data Right payment initiation functionality should be broad and extensible, including the list of payment functionality in Table 5.3A. Both payer and payee payment initiation should be enabled to initiate payments (with consumer consent), to allow flexible ongoing payment initiation consents and authorisations, and permit step-up authentication by the customer's authorised deposit-taking institution when required. Payment-related action functionality, such as registered payee management, should complement payment initiation functionality and be considered part of general action initiation.	**Agree** This is subject to the Government commitment to due process before designation as set out in its acceptance of Recommendation 5.1.
5.5 – Coverage of accounts Consumer Data Right payment initiation should apply to the bank accounts in Table 5.4 that ordinarily support payment functionality for customers. The Consumer Data Right should not require authorised deposit-taking institutions to provide new payment functionality in the accounts provided, only a new channel for using existing functionality exercisable with the customer's authority.	**Agree** This is subject to the Government commitment to due process before designation as set out in its acceptance of Recommendation 5.1.

Recommendation	Government response
5.6 – Competition in the payments system The Consumer Data Right payment initiation should be designed to allow competition among payment systems in order to improve consumer outcomes. By enabling flexibility in implementation, Consumer Data Right payment initiation should leverage future developments in the payments system.	**Agree** Noting that the Government's implementation program may prioritise the timing of CDR support for some payment systems over others. The CDR should as far as possible be payment system agnostic. If a covered account supports payments over a particular system, then prima facie the CDR should support instructions for such payments to be made.
5.7 – Accreditation for payment initiation Only an appropriately accredited person should be allowed to initiate payments through the Consumer Data Right. An assessment should be conducted by the Consumer Data Right rule maker to determine whether additional requirements to the unrestricted accreditation tier should be placed on those seeking to initiate payments, including how information security and insurance requirements should be adjusted. This assessment should also consider whether different tiers of accreditation for payment initiation could be enabled.	**Agree**. Implementation of this recommendation will also take into account the Government's response to the Review of the Australian Payments System, and in particular the proposed licensing arrangements for payment service providers.
5.8 – Standardised payment initiation application programming interfaces Authorised deposit-taking institutions should be obliged to receive a Consumer Data Right payment initiation instruction from an appropriately accredited person through a standardised application programming interface. Consumer Data Right agencies should engage with operators of major payment systems to develop Consumer Data Standards for bank account-to-account payment initiation that are, as far as possible, not specific to a particular payment system. The NPP API Framework, the UK Open Banking standards and standards used for international payments should be used as important reference points for developing these standards.	**Agree** The use of standardised application programming interfaces is consistent with the current data sharing framework for CDR Read Access. Noting that in part, this recommendation is dependent upon the cooperation of private operators of major payment systems.

Recommendation	Government response
5.9 – Cost of providing payment initiation Authorised deposit-taking institutions should be entitled to charge for complying with Consumer Data Right payment initiation requirements. The ACCC should be empowered to intervene if unreasonable fees are charged.	**Agree** Arrangements will be put in place to ensure that any fees charged do not have the effect of unjustifiably discriminating against the CDR channel in comparison to other channels through which the customer or their agents may ask for actions to be taken.
5.10 – Consent-driven payment initiation Consumer Data Right payment initiation should require the explicit consent of the consumer regarding the types of payments that are being enabled, and the purposes for which these payments are being allowed.	**Agree** The Government is committed to ensuring that the CDR remains a consumer consent-driven right.
5.11 – Authentication requirements for payment initiation Authentication requirements for authorised deposit-taking institutions and accredited persons engaged in payment initiation should be determined based on an assessment of the risks inherent to payment initiation, as well as the need for consistency in the consumer experience.	**Agree**
5.12 – Fine-grained payment initiation authorisation Consumers should be able to provide some level of specificity to their banks when authorising them to accept payment initiation instructions from an accredited person through the Consumer Data Right. The level of specificity required should be determined in the Rules and Standards.	**Agree** The extent to which fine-grained payment initiation authorisation will be possible and practical will be explored through the rulemaking and standards setting processes.

Recommendation	Government response
5.13 – Consistent and integrated consumer experience Consumer Data Right payment initiation should be designed to integrate into the rest of the Consumer Data Right to provide a consistent experience for consumers. Subject to consumer experience testing by the Data Standards Body, this should include the ability to provide consents and authorisations for data sharing, action initiation and payment initiation through a single process. Consumer Data Right agencies should engage with operators of major payment systems to support the alignment of payment consent mechanisms with the Consumer Data Right's consumer experience standards and guidelines.	**Agree** Noting that, in part, this recommendation requires the cooperation of private operators of major payment systems.
5.14 – Allocation of liability and supporting fraud mitigation The existing compensation arrangements between the bank and the customer, including under the ePayments Code where it applies, should continue to apply to payments initiated through the Consumer Data Right. For the purposes of applying these arrangements, the conduct of the accredited person should be taken as being akin to the conduct of someone who the bank and customer have agreed can operate the account on the customer's behalf. An accredited person should be responsible for losses arising from its own conduct, including when they result in an unauthorised payment from the consumer's bank account. In this case, to the extent that the bank (because it has compensated the customer for the loss) or the customer suffers a loss from the unauthorised payment then they should have a direct right of action for compensation from the accredited person. The ePayments Code should be updated to further clarify how its liability provisions would apply when a third party initiates a payment. Consumer Data Right information security requirements should be updated for payment initiation and to support fraud mitigation processes.	**Agree** The final terms of how liability is allocated will be determined through legislative drafting and rule-making processes. As the CDR rolls out to new sectors and new action types, it might be applied to other action types for which there are existing liability allocation rules (like the ePayments Code for payments). When this occurs, the CDR should also similarly consider parting from the default liability allocation rules proposed in Recommendation 4.20.

Recommendation	Government response
5.15 – Consumer Data Right payment initiation roadmap A Consumer Data Right payment initiation roadmap should be published, informed by consultation with the payments industry and interested stakeholders, to set clear expectations and drive the implementation of Consumer Data Right payment initiation. The roadmap should particularly draw on the timetable in the New Payments Platform's Roadmap as a critical development in the Australian payments infrastructure.	**Agree** A roadmap for the implementation of action initiation, including payment initiation, will be developed in consultation with stakeholders and taking into account the parallel development of other affected private and public sector initiatives.
5.16 – Opportunities for alignment in implementing Consumer Data Right payment initiation In implementing Consumer Data Right payment initiation, authorised deposit-taking institutions should meet the recommended design features. CDR agencies should engage with the operators of major payment systems, including the New Payments Platform, to explore opportunities to align third party payment initiation arrangements with those recommended for Consumer Data Right payment initiation. This should be conducted with a view to facilitating the utilisation of those arrangements by banks to meet their Consumer Data Right payment initiation obligations, so that implementation is expedited and compliance costs are minimised.	**Agree** Noting that this recommendation is dependent upon the cooperation of private operators of major payment systems. CDR agencies will engage with payment system operators to explore opportunities to align or leverage off other payment initiation arrangements in ways that ensures that CDR payment initiation remains, as far as possible, payment system agnostic in its operation.
5.17 – Payments through a third party access to digital banking portal Once Consumer Data Right payment initiation is implemented by authorised deposit-taking institutions, strong consideration should be given to prohibiting the making of a payment through third party access to digital banking portals. This should be considered as the implementation of the required design features for Consumer Data Right payment initiation nears full implementation and becomes widely accessible on reasonable terms to consumers and accredited persons.	**Agree** Any final decision of whether to prohibit screen scraping in relation to payment services will be considered in the proposed post-implementation review's assessment of the CDR's efficacy. That review will include the consideration of whether the CDR provides an appropriate and cost-effective alternative to digital data capture and action initiation.

Recommendation	Government response
5.18 – General action initiation in the banking sector General action initiation in the banking sector should enable product applications, updating details, managing products, closing a product, ending a customer relationship, and other associated general actions. These include general actions that support payments referred to in Recommendation 5.4. Certain information should be explicitly excluded from being subject to change through Consumer Data Right action initiation due to concerns for consumers' privacy and safety. These classes of information should be identified through regulatory and privacy impact assessments, and through consultation with industry and consumer groups.	**Agree** This is subject to the Government commitment to due process before designation as set out in its acceptance of Recommendation 5.1. The CDR legislative framework will provide the flexibility for it to potentially be applied to all actions that are available to customers in respect of any designated goods or services. In the banking sector, the eventual scope of covered actions will align with the scope as recommended, however implementation will occur in a phased manner with some actions being prioritised over others. See Recommendation 5.19.
5.19 – Prioritising product applications to support switching To support the streamlining of switching, product applications and establishing new customer relationships should be prioritised in the phased implementation of general action initiation in the banking sector. The Consumer Data Right rule maker should determine the order of prioritisation of general action initiation in consultation with consumer groups, the banking sector, accredited persons and other stakeholders.	**Agree** Subject to the Government's commitment in response to Recommendation 5.15 to develop an implementation roadmap (including the prioritisation of reforms) in conjunction with stakeholders. The general prioritisation of general action initiation will commence with payment-adjacent actions, with phased and some parallel and some sequential implementation of other action classes, such as managing customer information and products, product applications, and establishing relationships with new customers. The phased implementation of general action initiation in the banking sector will be informed by a framework used to assess the scope and priority of actions within each action class. Action initiation instructions will be assessed against indicative criteria including value realisation, implementation complexity, synergies with the implementation of other payment initiation and non-payments actions and whether parallel initiatives exist outside of the CDR.

Recommendation	Government response
5.20 – Sector-specific regulation Relevant regulators, including ASIC, should provide guidance as to how the provision of services by an accredited person using Consumer Data Right data sharing or action initiation could impact upon whether the accredited person needs to obtain additional licences.	**Agree**
5.21 – Identity verification assessments The Consumer Data Right should support consumer-directed sharing of Know Your Customer outcomes to the extent to which reliance is allowed on that outcome, in the event that proposed amendments to the reliance provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* are passed by Parliament.	**Agree** On 10 December 2020 the Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* increasing the extent to which reliance may be placed on other businesses' Know Your Customer assessments. To the extent that it does not already do so, the application of the CDR will be extended to allow sharing of KYC outcomes. The priority of these reforms will be determined as part of the creation of the implementation roadmap (see Recommendation 9.3).

Part 3: Data sharing enhancements

Recommendation	Government response
6.1 – Consumer Data Right to support specialisation and a sophisticated data ecosystem The Consumer Data Right should support the specialisation of services to allow businesses to design their own business models, promote innovation and support a safe and efficient digital economy.	**Agree**

Recommendation	Government response
6.2 – Outsourced service providers The Consumer Data Right should allow third parties to collect and disclose data on behalf of an accredited data recipient under an appropriate outsourcing arrangement without separate accreditation. The accredited data recipient would retain liability, and the outsourced service provider would need to comply with existing Standards.	**Agree** The CDR Rules 3.0 implement this recommendation. Unaccredited outsourced service providers are now able to collect and disclose CDR data on behalf of an accredited data recipient without separate accreditation.
6.3 – Accredited data recipient to accredited data recipient transfers The Consumer Data Right should allow transfers from an accredited data recipient to another accredited data recipient with customer consent, including transfers via arm's length intermediaries to an accredited data recipient.	**Agree**, noting that this has now been implemented as part of the CDR Rules 2.0.
6.4 – Authorised representatives CDR data should be able to be released to a CDR-authorised representative of an accredited data recipient, with the customer's consent. The authorised representative should be able to hold a lower tier of accreditation, in light of the principal accredited data recipient providing data access, taking on liability for Consumer Data Right compliance and taking on responsibility for putting in place arrangements to ensure compliance. The design of arrangements should have close regard to the role of authorised representatives under the Australian financial services licensing regime.	**Agree** The CDR Rules 3.0 implement this recommendation. The CDR representative rules enable persons accredited to the unrestricted level to provide goods/services to consumers using CDR data. The unrestricted accredited person will be liable for its representatives' compliance with CDR Rules, including uses and disclosures outside a representative arrangement.
6.5 – Data holders to receive CDR data from their sector The Consumer Data Right should allow data holders to receive CDR data relating to their sector from other data holders and accredited data recipients without requiring additional accreditation.	**Agree**

Recommendation	Government response
6.6 – Providing CDR data outside the system to regulated parties The Consumer Data Right should allow regulated third parties operating outside the Consumer Data Right ecosystem to receive varying levels of data with the consent of the consumer, with reference to the level of regulation of the recipient. This access should include transfers of CDR data or derived data for regulated activities or for regulatory compliance activities at the customer's direction.	**Agree** The CDR Rules 3.0 implement this recommendation. Under the new 'trusted adviser' rules consumers can consent to disclosing their CDR data to certain professional classes specified in the rules, including lawyers, accountants, tax agents, BAS agents, financial advisers, financial counsellors, and mortgage brokers.
6.7 – Data for low risk public benefit uses The Consumer Data Right should allow non-accredited parties operating outside the Consumer Data Right ecosystem to receive varying levels of data with the consent of the consumer, subject to appropriate restrictions, if they provide low risk services for public benefit.	**Agree** See response to Recommendation 6.4. Financial counsellors are recognised as providing low risk services for public benefits and are included as a class of trusted adviser in the CDR Rules 3.0.
6.8 – Insights to non-accredited persons The Consumer Data Right should allow non-accredited third parties operating outside the Consumer Data Right ecosystem to receive, from a data holder or accredited data recipient, lower risk insights data derived from CDR data.	**Agree** The CDR Rules 3.0 implement this recommendation. New rules allow a consumer to consent to an accredited data recipient disclosing limited data 'insights' about them to any person. Insight disclosures are only permitted for specific purposes where the consumer is fully informed about what the insight would reveal about them.

Recommendation	Government response
6.9 – Cross-sector application of reciprocity The Consumer Data Right principle of reciprocal obligations of an accredited data recipient to respond to a consumer's data sharing request should not be limited by the scope of sectoral designations at the time of accreditation. Accredited data recipients should be obliged to comply with a consumer's request to share data which is the subject of a sectoral designation as well as equivalent data held by them in relation to sectors which are not yet designated.	**Disagree** The sectoral designation process remains the most viable means of expanding the scope of CDR in a targeted, strategic manner, which balances industry concerns about creating barriers to CDR participation. These concerns are particularly acute with CDR currently being in its infancy as an economy-wide data sharing regime. Stakeholders have raised concerns that reciprocity requirements in their current form act as a disincentive to some firms entering the CDR regime as ADRs. Presently, these requirements mandate reciprocal sharing by ADRs only with respect to data that is within the scope of a CDR designation instrument. Broadening the scope of these requirements to also apply to 'equivalent data' that is undesignated would exacerbate this issue, while creating additional complexity and resourcing pressures at the accreditation stage. If future issues arise about data holding entities entering the CDR as ADRs and whether they should be required to share equivalent data, interventions can be effectively implemented through revisions to the rules where a strong policy rationale for this exists.
6.10 – Identifying equivalent data Equivalent data should exclude materially enhanced data and voluntary data sets. Equivalent data applicable to a person seeking accreditation as an accredited data recipient should be identified by the accreditor during the accreditation process. Identification of equivalent data should be subject to the same principles which apply to the selection of data sets through the formal sectoral assessment and designation process. Guidelines on the identification of equivalent data should be published by the regulator.	**Disagree** See comments on Recommendation 6.9.
6.11 – Exclusion from reciprocal data sharing obligations Accredited data recipients should be excluded from reciprocal data sharing obligations if they are below a defined minimum size.	**Disagree** See comments on Recommendation 6.9.

Recommendation	Government response
6.12 – Accreditation criteria The accreditation criteria should not create an unnecessary barrier to entry by imposing prohibitive costs or otherwise discouraging suitable parties from participating in the Consumer Data Right. A tiered, risk-based accreditation model should be used to minimise costs for prospective participants.	**Agree**
6.13 – Tiering of accreditation Regulation of the Consumer Data Right should be able to allow tiering of accreditation requirements based on factors, including the risks associated with the accessible CDR data and the activities that could be undertaken with it.	**Agree** CDR Rules 3.0 established a sponsored level of accreditation and CDR representatives. The models draw on this recommendation and lower barriers to entry for participants. As more sectors of the economy are designated, additional risk-based levels of accreditation may be considered.
6.14 – Inclusion of data The process and criteria for clearing or disallowing new Consumer Data Right data set standards should not discourage or exclude the provision of any data sets that are suitable for use in the Consumer Data Right. This should include data sets within a designated sector that have not been designated, and data sets from sectors not designated.	**Agree-in-principle** Stakeholder feedback received through the CDR Strategic Assessment process indicates that non-designated (voluntary) data sets present key opportunities for expansion of the CDR regime across the economy. Flexible mechanisms (such as the CDR rules or designation processes) could be used to target voluntary data sets for inclusion in the CDR.
6.15 – Process for introducing voluntary data sets The Data Standards Chair should be able to approve standards for new voluntary data sets developed using different pathways. These pathways should include design by the Data Standards Body under a fee-for-service model upon request, industry-led design, or individual firms introducing bespoke data sets. There should be a set period of time that the Data Standards Chair has to clear or disallow any standards that do not meet the specified criteria or benefit consumers.	**Agree-in-principle** See comments on Recommendation 6.14. Further to comments at Recommendation 6.14, we note that where voluntary data sharing under the CDR requires a process for setting or reviewing standards, this process should be secondary to the process for creating standards for mandatory data sharing under the CDR. This is consistent with the policy and legislative framework of the CDR. Furthermore, decisions about bringing voluntary data sets into the regime should be made strategically in policy-making to drive a vibrant data ecosystem.

Recommendation	Government response
6.16 – Guidelines for voluntary data sets Guidelines should be provided outlining specific criteria that new data sets and their associated standards need to meet for inclusion in the Consumer Data Right environment.	**Agree-in-principle** See comments on Recommendations 6.14 and 6.15.
6.17 – Maintenance of industry designed standards Standards for voluntary data sets introduced to the Consumer Data Right by industry participants must be maintained by industry participants. The Data Standards Chair should have the right to disallow such standards if they are not maintained to the level required.	**Agree-in-principle** See comments on Recommendations 6.14 and 6.15.
6.18 – Ongoing consumer experience research The Data Standards Body should continue to conduct ongoing consumer research in a consistent, principled way that is reflective of the needs of consumers, accredited persons and data holders. Where appropriate, the findings of this research should be given legal effect through recognition by the Rules or Standards.	**Agree**
6.19 – Consumer Data Right dictionary The Data Standards Body should include as part of the Consumer Experience Standards, a non-exhaustive dictionary outlining, in plain English, definitions of common terms used in Consumer Data Right consents. For usage consents, this should include common understandings of purposes.	**Agree** The Data Standards Body has indicated that it will consult with industry and consumer groups to identify opportunities to improve consumer consent processes. This process will involve consumer research and public workshops with the aim of developing appropriate solutions, which are expected to support the simplification of consent.
6.20 – Industry recommended and endorsed consents Industry and consumer groups should be encouraged to develop and endorse standard wording for Consumer Data Right consents for specific purposes, and accredited persons should be permitted to display these endorsements in their consent processes through icons, descriptions, links or other appropriate methods.	**Agree** Noting that this recommendation is directed towards and requires the cooperation of industry and consumer groups.

Recommendation	Government response
6.21 – No mandated central consent collection A central body should not be mandated to collect all consumer consent and authorisation information created by participants in the Consumer Data Right system.	**Agree** Consent data is sensitive. A decentralised management system, where industry competes to create user friendly management tools, is likely to be more secure and facilitate innovation.
6.22 – Sharable consent information Consent and authorisation data should be designated as CDR data to facilitate the secure provision of centralised consent management services at the consumer's direction. Consultation should be undertaken before determining who should be required to share this information, so as not to unduly increase barriers to entry into the system.	**Agree** Consideration will be given to the development of rules and standards for this data to be a voluntary data set within the CDR regime in advance of any future mandate.
6.23 – Limited action initiation for consent management Consumers should be able to authorise an accredited person to perform certain actions in regards to Consumer Data Right consents and authorisations on their behalf as a Consumer Data Right action. Consultation with industry and consumer advocates should be conducted prior to the full scope of actions being determined.	**Agree** See response to Recommendation 6.22.
6.24 – Privacy impacts of sharing consent information Prior to the designation of consent and authorisation information, the potential privacy impacts of facilitating the transfer of consent data should be separately reviewed. This process should pay special attention to the needs of vulnerable consumers.	**Agree** See response to Recommendation 6.22.

Part 4: Consumer safeguards

Recommendation	Government response
7.1 – Interaction with sector-specific consumer protections The interaction and potential overlap between industry-specific consumer protections measures and the Consumer Data Right regime should be considered when assessing the potential to designate a sector for data sharing or action initiation, with any barriers or conflicts between the regimes appropriately resolved.	**Agree**
7.2 – Suitability of persons for action initiation Regulatory settings for accreditation should enable the accreditor to take into account all matters relevant to the applicant's suitability to initiate actions of the type proposed. Requirements on persons seeking accreditation to advise the types of goods or services they propose to offer or, in the case of accredited persons, offer, consumers using CDR data should be extended to goods or services offered to consumers that involve the use of action initiation.	**Agree** Noting the importance of clear allocations of responsibility between CDR accreditation processes and sectoral licensing and regulation, regarding an applicant's suitability to carry out specific data driven activities.
7.3 – Remedies where instruction sent without a valid request If an accredited person sends action initiation instructions without obtaining a valid request from the consumer or complying with relevant Rules, consumers should have the right to take action against the accredited person. Other remedies (including civil penalties and suspension or revocation of accreditation), should also be available.	**Agree**
7.4 – Remedies where data holder does not have authorisation If a data holder acts on action initiation instructions without having obtained the consumer's authorisation to do so, the consumer should have the right to take action against the data holder. Other remedies (including civil penalties) should also be available.	**Agree**

Recommendation	Government response
7.5 – Extending consumer protections for action initiation Consumer protections in Part IVD of the *Competition and Consumer Act 2010* and the Rules, including the prohibitions on holding out and misleading and deceptive conduct in relation to consumer consent, should be extended or adapted as appropriate to apply to action initiation, with appropriate and proportionate remedies available.	**Agree**
7.6 – Action initiation and accredited person's obligations to consumers Where an accredited person seeks, or has been granted, a consumer's consent to initiate actions with a data holder, the accredited person should be obliged to act efficiently, honestly and fairly in relation to initiating actions. In some sectors it may be appropriate that a higher standard (or additional obligations) apply, either generally or in relation to particular actions. This should be considered during sectoral assessment and rule making processes, and subject to consultation. If the accredited person fails to meet the standard of conduct required of them, the consumer should be able to take action against the accredited person. Other remedies (including civil penalties and suspension or revocation of accreditation) should also be available.	**Agree** Where an accredited person is given discretion in how to initiate a payment or general actions with a consumer's authority, they will be subject to a general duty to ensure they properly exercise that authority. The CDR will not duplicate or displace any equivalent duties that exist in sectoral regulation in relation to specific activities – however breaches of those sectoral regulations involving use of the CDR may impact their entitlement to participate in the system.
7.7 – Monitoring impact on vulnerable consumers The impact of the recommended reforms on vulnerable consumers in designated sectors, including the availability and suitability of services offered and any trends in Consumer Data Right complaint data received, should be monitored to assess whether any regulatory settings require adjustment. The ACCC should be responsible for this monitoring. Additionally, an evaluation of the impact of the Consumer Data Right system on the wellbeing of vulnerable consumers should be completed 24 months after action initiation's commencement. This assessment should be led by government in close collaboration with consumer representatives and industry.	**Agree** Both the ACCC and OAIC also have a role in monitoring and advising the Government on CDR-driven practices affecting vulnerable consumers.

Recommendation	Government response
7.8 – Consumer education program CDR agencies should coordinate the development and implementation of a timely consumer education program for new Consumer Data Right designations. Participants, industry groups and consumer advocacy groups should also be invited to participate, as appropriate, in developing consumer awareness and education activities.	**Agree** Due to the significance and complexity of the CDR as a whole-of-economy reform, considered and timely communication with consumers and industry is crucial. The Government will continue to invest in, and draw on, consumer research and feedback from CDR stakeholders to inform communications, education and awareness-raising activities.
7.9 – Encouraging innovation that benefits vulnerable consumers The Government should explore options to encourage the creation of products that use the Consumer Data Right to benefit consumers, including the establishment of a grants program to support developers to design and build such products. Government should seek input from consumer representatives and those providing services to vulnerable consumers in doing so.	**Noted** The Government reconfirms its commitment to the CDR being primarily directed at enabling consumers to realise the benefits in their own data, to gain access to new goods and services that better meet their needs and to realise savings through switching to products that provide better value for money. While the Government will explore the option of using grants to support CDR use cases to assist vulnerable people, it has not determined whether to do so at this time.
7.10 – Encouraging consumer representation in developing the Consumer Data Right The Government should explore ways in which interested consumer advocacy groups could be supported to contribute their expertise to the development of the Consumer Data Right and CDR-enabled products. This could include the engagement of consumer representatives in drafting guidance for accredited persons on the design of CDR-enabled products, which take into account vulnerable consumers' needs.	**Agree** The Government is committed to ensuring that consumer and privacy groups have a strong voice in CDR design and development. The Government will explore the appetite of consumer, privacy and industry groups to develop voluntary guidance for the design of CDR-enabled products.

Recommendation	Government response
7.11 – Protections for action initiation instructions to be considered in the privacy and security assessments 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. Information security protections for action initiation authorisation, consent and instruction data should be proportionate to the risks presented by misuse of this data. The assessments should occur before the legislation is settled to determine what should be captured in the primary legislation, the Rules or Standards.	**Agree** The Government is committed to strong information security protections for the regime. Information security and privacy assessments will occur in an iterative manner throughout the legislative, rulemaking and standard-setting processes for the implementation of CDR Action Initiation.

Part 5: Opportunities for connecting the Consumer Data Right to the data economy

Recommendation	Government response
8.1 – Support for development of authentication solutions interoperable with the Consumer Data Right The Consumer Data Right should continue to be developed in a manner that encourages the use of interoperable authentication solutions, based on compatible international standards.	**Agree**
8.2 – Minimum assurance standard for authentication to apply to data holders and accredited data recipients The Data Standards Body should develop a minimum assurance standard for authentication applicable to both data holders and accredited data recipients. The standard should support interoperability and flexibility for participants, provided minimum assurance standards and consumer experience standards are met. The standard should include provision of safe harbours for existing authentication requirements for current data sets and functions.	**Agree**

Recommendation	Government response
8.3 – Minimum assurance standard for authentication to include a risk taxonomy and matrix As part of the minimum assurance standard for authentication the Data Standards Body should develop a risk taxonomy and risk matrix against which assurance levels for particular data sets and Consumer Data Right functions in each sector can be determined with a degree of consistency. This taxonomy and matrix should form part of the minimum assurance standard used to inform the level of assurance required, noting that other considerations will also factor. It should consider the nature of data, likelihood of harm to consumers if data is misused and other key factors that the Data Standards Body considers appropriate. This should be developed in consultation with industry and consumers.	**Agree**
8.4 – Standards setting for data held by government The Data Standards Body should be available as a source of expertise in developing and maintaining data standards that other government initiatives, regulatory regimes and information technology systems could adopt. It should also be available as a central point for engagement in relevant international data setting fora.	**Agree** The Data Standards Body should continue to focus on CDR implementation, providing specialist advice as required and where appropriate on other Government data initiatives.
8.5 – Leveraging the Consumer Data Right data safety licence The 'data safety licence' and supporting register should be available to meet equivalent requirements in other regimes, in a way that is consistent with best practice cybersecurity risk management and broader cybersecurity frameworks.	**Noted** The Government supports reducing the burden for industry and will continue to have strong regard to the equivalent requirements in other regimes and pursue alignment where appropriate.
8.6 – Aligning data safety accreditations As an alternative to broader use of the 'data safety licence', or as an interim step (or in relation to international regimes), efforts should be made to align similar data safety 'accreditations'.	**Noted** See response to Recommendation 8.5.

Recommendation	Government response
8.7 – Recognising external data safety accreditation Where external data safety accreditations align with Consumer Data Right requirements, these could be recognised by the Consumer Data Right or at least enable their 'accreditation holders' to go through streamlined Consumer Data Right accreditation.	**Agree** See response to Recommendation 8.5. Any recognition would be subject to detailed information security assessments of the extent to which other accreditations provide equivalent outcomes to CDR accreditation.
8.8 – Guidance on artificial intelligence ethics in the Consumer Data Right Further guidance about transparency requirements relating to data aggregation activities such as the use of algorithms, the importance of privacy by design and the application of relevant ethical frameworks, including the AI Ethics Framework when utilising AI technologies for data within the Consumer Data Right regime should be included in a future version of the Privacy Safeguard Guidelines. In addition, the OAIC should consider, in consultation with the Consumer Data Right rule maker whether it may be appropriate to include consideration of these matters in its future assessments program.	**Agree-in-principle** The Government supports greater awareness and use of its AI Ethics Framework. The Government will consider whether any CDR specific guidance on this framework is necessary. The OAIC will also consider if CDR-specific guidance on these matters should be outlined in its future guidance as appropriate. The Government is committed to sectoral assessments seeking to identify and assess all relevant risks that may be associated with extending the scope of the CDR, including risks associated with the inappropriate use of AI.
8.9 – Using open international standards where available Open international standards should be used as a starting point for Consumer Data Right rules and standards where available and appropriate.	**Agree** The CDR should seek to use generally accepted international standards where appropriate.
8.10 – When diverging from open international standards Where divergences from open international standards are proposed, the reason for this should be clearly articulated during consultation, giving stakeholders a chance to comment on whether alignment or divergence would be the most appropriate course.	**Agree** See Recommendation 8.9.
8.11 – Streamlined accreditation The registration system for accredited data recipients (including underlying rules) should be updated to include a clear procedure for accreditation under equivalent foreign regimes to be considered (as appropriate) in meeting some or all of the requirements for participation in the Consumer Data Right.	**Agree** Any streamlined accreditation arrangements would be subject to detailed information security assessments of the extent to which other jurisdictions' accreditation systems provide equivalent outcomes to CDR accreditation.

Recommendation	Government response
8.12 – Seek mutual arrangement with the United Kingdom Australia should approach the United Kingdom with the prospect of creating a mutual bilateral recognition regime. This should include a process for identifying differences in registration requirements so any additional requirements in either regimes are clearly articulated.	**Agree** Noting the importance of sovereign privacy and security requirements for any mutual recognition regime. Any mutual recognition arrangements would be subject to detailed information security assessments of the extent to which the United Kingdom's accreditation provides equivalent outcomes to CDR accreditation. It would also be subject to consultation with the United Kingdom regarding the proposal and sufficient assurance that the personal information of consumers is provided commensurate privacy protections.
8.13 – Engage with New Zealand Australia should engage with New Zealand as it considers whether and how to develop a consumer data right including to explore options for mutual recognition of licensing for participants.	**Agree** On 31 May 2021 at the annual Australia-New Zealand Leaders' Meeting, in their joint statement the Prime Minister of Australia, the Hon Scott Morrison MP, and the Prime Minister of New Zealand, Rt Hon Jacinda Ardern, jointly committed to continue work towards interoperability on Consumer Data Rights. This was followed, in July 2021, by an announcement by the Government of New Zealand that it will implement a legislative framework to develop a consumer data right, and that it will look to align its system with Australia's CDR. On behalf of the Australian Government, the Treasury meets regularly with the New Zealand Ministry of Business, Innovation and Employment to discuss the respective consumer data right frameworks and will continue to engage closely.
8.14 – International forum The Government should seek opportunities to convene an international forum for policy makers considering, designing, implementing and maintaining consumer-controlled data portability regimes. In the interim, Australia should formalise existing relationships by establishing a quarterly dialogue with international policy bodies commencing with the United Kingdom, New Zealand, India and Singapore.	**Agree** The Government is committed to engaging regularly with other jurisdictions implementing consumer data portability regimes. On behalf of the Government, the Treasury is consulting key like-minded countries (including New Zealand, UK, India and Singapore) on the establishment of an international community of practice to discuss the design and implementation of consumer-controlled data portability frameworks. Any other interested countries could also be invited to participate in the international community of practice.

Part 6: CDR Roadmap and other recommendations

Recommendation	Government response
1.1 – Balanced approach to safety, efficiency and effectiveness The Consumer Data Right should be developed to be safe, efficient and effective. A balanced approach is needed to realise meaningful benefits to consumers and grow participation in the data ecosystem.	**Agree** This reflects the Government's current approach to implementation of the CDR.
1.2 – Clarity in relation to other laws and regulations The Consumer Data Right operates in conjunction with other laws and regulations, including sectoral regulation. However, amendments to these other laws and regulations may be required to enable the benefits of the Consumer Data Right to be fully realised. Similarly, the Consumer Data Right may enable new behaviours and practices which may warrant a government response through other laws and regulations. Consumer Data Right development and operational processes should identify emerging behaviours and practices of concern and refer them to appropriate policy makers and regulators. Government should articulate with clarity when a response should occur through the Consumer Data Right or other laws and regulations.	**Agree** The CDR will be designed to be another channel for providing instructions to act, rather than playing a role in carrying out those actions (which will be left to service providers to do in line with their existing processes and integrations). The CDR is not the appropriate mechanism by which sectoral regulation should be implemented, however it should ensure the relevant policy makers and regulators are informed of current or potential behaviours and practices of concern.
3.1 – Analysis and comparison of bundled products Analysis and comparison of bundled products should be facilitated by the Consumer Data Right. The Data Standards Body should consider the most appropriate and efficient method to better enable product reference data about the range of services available, including bundled products, to be provided to consumers and accredited persons.	**Agree**
9.1 – Sector assessments with product reference data Sector assessments and designation instruments should be able to focus solely on product data where the opportunity exists for product data already available outside the Consumer Data Right to be introduced to the Consumer Data Right system.	**Agree**

Recommendation	Government response
9.2 – Prioritisation of Inquiry recommendations Recommendations should be prioritised primarily based on the benefits they will provide consumers, including their contribution to new products, participation in the ecosystem, consumer protection and ease of implementation. Recommendations that can be progressed without legislative amendments should also be prioritised.	**Agree** Prioritisation of implementation will also take into account other factors, including whether concurrent design of some action types may contribute to the development of a consistent framework; and the timing of implementations by industry of other government and private sector initiatives.
9.3 – Integrated Consumer Data Right Roadmap The Government should create an integrated roadmap for the implementation of the Consumer Data Right, in collaboration with stakeholders in the private and public sectors. This roadmap should focus on key external projects in their implementation phases that will impact the Consumer Data Right.	**Agree** The Government will engage with industry, consumer groups and sectoral groups to develop a roadmap for implementation. The development of this roadmap will be an iterative process, reflecting that more certainty will emerge over time regarding what is required to design, build, test and launch the proposed reforms.
9.4 – Post-implementation review A post-implementation assessment of action initiation and payment initiation should be conducted approximately 24 months after the commencement date and report to the Minister with recommendations.	**Agree,** subject to a final decision on the timing of the implementation of reforms. The Review should take place only once the key reforms have been put in place and sufficient time has passed to enable a meaningful assessment of their operations and impacts.