Australian Government

FUTURE DIRECTIONS

for the Consumer Data Right

consumers • choice • convenience • confidence

October 2020

INQUIRY INTO FUTURE DIRECTIONS

for the Consumer Data Right

consumers • choice • convenience • confidence

October 2020

ISBN 978-1-925832-19-8

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

Contents

Foreword

The Consumer Data Right (CDR) is a landmark in the development of Australia's digital economy. It gives Australians more control over their information, more choice in their products and services, more convenience in managing their lives and more confidence in using their data. Consumers can now share the data they have, with the businesses they select, for use as they choose. The first stage of the CDR – Open Banking – is already helping Australians, but the journey has just begun.

Australian consumers rely on digital interactions and are increasingly using and sharing more of their data. The impact of COVID-19 has accelerated this trend, as more activities have become digital and data-dependent, from online shopping to virtual meetings. Our digital infrastructure needs to become even more effective, inclusive and safer for use by Australian consumers, sustained by an innovative, productive and competitive data ecosystem. This Inquiry has found that to realise these aims, the CDR needs to develop in four directions:

Towards data-empowered consumers – Functionality of the CDR should be expanded to deliver more convenience to consumers. The CDR should, for example, allow consumers to authorise others to digitally initiate actions, such as switching providers and initiating payments, and provide certainty to consumers through CDR dictionaries and improved consent management.

Towards an economy-wide foundation – Broader participation in the CDR should be encouraged to create more choices for consumers. It should foster new ideas through innovative data sets and interoperability. Growth of opportunities to use the CDR to compete for customers should be encouraged through flexibility in sector assessments and reciprocity in sharing.

Towards an integrated data ecosystem – Specialisation and cooperation within the CDR should be enhanced, and interaction with the digital economy opened up, to create a data ecosystem which gives confidence to consumers. The CDR should allow trusted advisers to participate and enable graduated accreditation. Its infrastructure and standards should be leveraged for wider application.

Towards international digital opportunities – Connections with similar overseas frameworks should be pursued to provide broader choices for Australian consumers and opportunities for start-ups and digital businesses. Australia should be at the forefront of the cross-border progress in consumer-driven data frameworks.

This future CDR will provide greater everyday benefits to Australian consumers. Consumers will be able to safely use online services or apps on their mobile phone to:

- notify them which of their bills are due, arrange for bills to be paid at the best times, and move their money between their accounts to minimise interest costs and fees

- advise them in real time which services and plans are best for them, switch them onto those services and plans, and provide reports on the money saved, and
- give them an up-to-date dashboard showing who they are sharing data with, how it is being used, and allow them to change those things, or make the sharing stop.

By making data work for them, the future CDR should reduce the time consumers take on their 'life admin' so they can spend more time on what they enjoy and what really matters. Or enable more effective help to be found by consumers suffering hardship. The future CDR ought to provide start-ups and other digitally-engaged businesses the clarity, certainty and consistency needed to invest in Australia's digital economy. In this way, the future CDR can provide a sustainable, robust and resilient foundation for Australian consumers and businesses to engage with, and safely benefit from, the exchange of data and the increased productivity it supports.

In developing its 100 recommendations, this report considers a broad landscape of issues such as artificial intelligence, behavioural biases, bundled products, consent taxonomies, data literacy, digital identification, extensible functionality, fine-grained authorisations, information security, international consistency, liability allocation, leveraging standards, payment systems, privacy safeguards, risk and responsibility, online vulnerability, streamlined switching, trust and trusted advisers, usage consents, voluntary data sets and vulnerable customers. The issues traverse the fields of technology, data science, law, regulation, behavioural science, economics, consumer welfare and public policy. To navigate this complexity, the four simple principles of the CDR's original design remain an essential compass – the CDR should be consumer-focused, encourage competition, create opportunities and be efficient and fair.

And two everyday analogies have helped us shape future directions:

Sharing consumer data can be like swimming at the beach – it can be enjoyable and healthy, but it also can be unpredictable and dangerous, particularly for those not aware of the hazards. The CDR represents the flags showing where it is safer for consumers to swim, where information and warnings can be found and where the CDR regulators are on duty. Just as beach safety is designed to allow everyone who chooses to swim to enjoy the water and waves, the CDR design needs to recognise that all consumers who choose to share their data should enjoy the benefits, whether they are digitally-literate or not. This report recommends where, and how, these CDR 'flags' should be placed in the future.

Sending consumer data can be like driving in the bush – it can be exciting and engaging, but narrow, winding roads can make the trip slow and unsafe. The CDR is the new highway for driving consumers' data quickly and securely to their chosen destinations. Safeguards are the safety barriers, standards its speed limits, accreditation its driving licences and the CDR regulators are the highway patrol. But just as other rules and protections also apply to drivers on the roads that connect highways to destinations, the CDR design needs to recognise that other regulation applies to the products and services provided using CDR data. This report recommends where, and how, this CDR 'highway' should be extended and connected to these other roads, in the future.

Reaching this milestone in our CDR journey has taken much thought, discussion, work and investment from many people over many years. But we are at a waypoint not the endpoint.

It has been a distinct privilege to lead this Inquiry. I am very grateful to the many people who took the time to contribute submissions and (virtually) meet with me, particularly through such disrupted times. A vast amount of expertise, experience and knowledge has been generously contributed by the academic, consumer, corporate, data, energy, finance, fintech, government, professional, regulatory, scientific and technological communities of Australia and beyond our shores. The enthusiasm and engagement of these experts shows that CDR's future is in good hands. Finally, my very deep thanks go to the committed, professional and knowledgeable officers of my secretariat, whose support and hard work made conducting this Inquiry possible.

Scott Farrell

Executive Summary

What was the Inquiry asked to do?

On 23 January 2020, the Treasurer, the Hon Josh Frydenberg MP, announced the Inquiry into Future Directions for the Consumer Data Right (CDR) (the Inquiry).

The Inquiry was asked to make recommendations on options to expand the CDR's functionality. This includes how the CDR could be expanded to include 'write' access so that consumers could not only choose to share their data through the CDR, but also apply for and manage products including, for Open Banking, by initiating payments.

The Inquiry was also tasked with examining how the CDR could be used to overcome barriers to consumers conveniently and efficiently switching between products and providers, and to consider ways to ensure that the CDR promotes innovation in a manner inclusive of the needs of vulnerable consumers.

Lastly, the Inquiry was asked to identify opportunities to leverage the CDR to enhance opportunities for Australian consumers, businesses and the Australian economy, and to leverage the CDR infrastructure to support productivity and a safe and efficient digital economy.

Overview of future directions and recommendations

The Inquiry has been guided by the same four key principles that guided the CDR from its inception and through the implementation of Open Banking. These are that the CDR should be consumer focused, encourage competition, create opportunities and be efficient and fair.

The process of completing the Inquiry has been highly consultative. The Inquiry has considered formal submissions from 73 interested parties in response to its Issues Paper. It has also met virtually with over 300 representatives from industry, peak bodies, consumer groups, regulators, government and academia, including parties in overseas jurisdictions. Further information on consultation undertaken by the Inquiry is contained in Chapter 1. Public submissions are listed at Appendix B.

The Inquiry has reported on future directions and recommendations for the CDR in the following chapters:

- **Chapter 1** introduces the Inquiry's Terms of Reference, background information, the guiding principles of the Inquiry and the key themes from submissions.
- **Chapter 2** presents the four future directions for the CDR.
- **Chapter 3** sets out the switching journey in Figure 3.1 and the role of CDR on this journey. It examines the risks and benefits of switching and barriers faced by consumers who wish to switch.

- **Chapter 4** outlines how the CDR's functionality could be expanded to include action initiation, including a framework for action initiation and the action initiation process.
- **Chapter 5** examines how action initiation could enable customers to apply for and manage products, including initiating payments, in the banking sector.
- **Chapter 6** examines potential enhancements to the CDR ecosystem, including tiered accreditation, voluntary data sets, consent taxonomies and consent management.
- **Chapter 7** considers the consumer safeguards that are necessary to ensure trust in the CDR, including privacy protections.
- **Chapter 8** explores the opportunities available to leverage CDR infrastructure, including in relation to digital identity solutions, standard setting and the accreditation regime. It also looks at how the CDR can be leveraged with similar regimes internationally.
- **Chapter 9** outlines a roadmap for the Inquiry's recommendations, taking into consideration initial sector assessment and priorities for implementation.

Additional reference information on Inquiry matters and issues are dealt with in the appendices.

Chapter 1 – Introduction to the Inquiry

As the CDR rolls out into the banking sector, the Inquiry was announced to consider future directions for the CDR. The Inquiry has been guided by the principles of a CDR that is consumer focused, encourages competition, creates opportunities and is efficient and fair. For the digital economy to work safely, efficiently and fairly, the CDR needs to function effectively in conjunction with other frameworks and regulations, including those related to consumer protection, information security, data protection and sectoral regulation. A balanced approach to safety, efficiency and effectiveness is needed. This may involve some enhancements to existing laws and regulations.

Chapter 2 – Future Directions for the Consumer Data Right

There are four future directions for the CDR. These are:

1. Beyond data sharing, *towards data-empowered consumers*
2. Beyond open banking, *towards an economy-wide foundation*
3. Beyond a standalone system, *towards an integrated data ecosystem*
4. Beyond Australia's borders, *towards international digital opportunities*

These future directions show the ways in which the CDR should expand to strengthen the foundations of Australia's digital economy. The implementation of the recommendations from the Inquiry should be expedited to deliver on the CDR's benefits to Australia and Australians.

Chapter 3 – Expanding the Consumer Data Right to support switching

The CDR currently assists consumers to identify products that best suit their needs based on analysis of their consumer data and the range of products on the market. Expanding the CDR to help

consumers switch easily and conveniently between products will provide even greater consumer benefit and, importantly, cost savings. The CDR can be used to overcome behavioural and practical barriers to convenient and efficient switching between products and providers. Encouraging consumers to use the CDR to switch and realise its benefits will require consumer trust and confidence in the system. An expanded CDR will support services that could assist with tailored product identification and switching and facilitate general management of a consumer's data. Analysis and comparison of all available products, including bundled products, should be enabled by the CDR. The Inquiry discusses how switching in some sectors is impacted by sector-specific legislative or regulatory frameworks that may need to be reviewed to deliver the most streamlined consumer experience.

Chapter 4 – Action initiation framework

The CDR provides a secure set of channels through which accredited persons can communicate with data holders. These channels should also be opened to suitably accredited persons to initiate actions on a consumer's behalf with the consumer's consent. Enabling action initiation in this way would allow the CDR to facilitate a much broader range of functions, and increase the range of products and services available to consumers.

The legislation that gives legal basis to the CDR should be amended to enable action initiation. Action initiation should also be governed by the Rules and Standards. As with data sharing, the suitability of sectors for CDR action initiation should be determined through a sectoral assessment process.

In enabling action initiation through the CDR, the current consent framework should be maintained to ensure that the system promotes confidence among consumers. This framework should also be bolstered by enabling additional authorisation processes to allow data holders to confirm the validity of action initiation requests received through the CDR. This will help enable data holders to comply with their other obligations and protect consumers.

Chapter 5 – Action initiation in the banking sector

The CDR should be expanded in the banking sector to include action initiation. There should be two broad classes of actions – 'payment initiation' and 'general action initiation' – in the banking sector.

Bank account-to-account payment initiation should be prioritised to leverage developments in the Australian payments industry. CDR payment initiation's design features should enable a customer to authorise a suitably accredited person to use the CDR to initiate a payment on their behalf. Broadly, it should apply to all authorised deposit-taking institutions (ADIs) and accounts subject to CDR data sharing and have broad and extensible functionality. It should allow for competition among payment systems and the initiation of payment instructions through standardised application programming interfaces. CDR payment initiation should provide a consistent and integrated consumer experience with data sharing. ADIs may also charge reasonable fees for complying with payment initiation requirements. The allocation of liability under CDR payment initiation should be principles-based, building on existing compensation arrangements. The ePayments Code should be updated to clarify how its liability provisions apply when a third party initiates a payment.

A CDR payment initiation roadmap should be published in consultation with the payments industry. CDR agencies should engage with operators of major payment systems to explore opportunities to align third party payment initiation arrangements with the CDR payment initiation design features. Once CDR payment initiation is fully in place, strong consideration should be given to prohibiting the use of third party access to a customer's digital banking portal to make payments.

General action initiation in the banking sector should enable product applications, updating details, managing products and closing a product or account. However, certain information should be explicitly excluded from change due to privacy and safety concerns. Priority should be given to product applications and establishing new customer relationships in developing general action initiation to support switching. The CDR should enable consumer-directed sharing of Know Your Customer outcomes when the reliance provisions are expanded.

Chapter 6 – Read access enhancements

The CDR framework should encourage participation by consumers, accredited data recipients (ADRs) and service providers in the data economy. This means enabling the broad range of specialised services provided by participants in the data economy to flourish in the CDR, and for accreditation requirements to be calibrated according to the level of risk participants are required to manage. Where participants receive accreditation, they should be willing to provide, as well as receive consumer data at consumers' request.

The range of data utilised in the CDR environment should not be limited only to data identified in the process of sectoral designation. The CDR provides a strong framework for data sharing and standards that can be utilised for a broad range of data sets, a process that encourages the use of voluntary data sets should be developed.

Consents and authorisations form the foundation of the CDR, outlining the terms on which a consumer agrees to engage with the regime. The language in these consents should therefore be as accessible to consumers and accredited persons as possible, enabling all parties to engage confidently in the system. Consumers should also be empowered to more easily keep track of their consents, making it more convenient to engage with the regime.

Chapter 7 – Consumer safeguards

Additional consumer safeguards will be required as the CDR's functionality expands to ensure consumers benefit, and their rights are protected. Key CDR data sharing consumer protections should be extended and adapted for CDR action initiation, with consumers having access to appropriate remedies if accredited persons or data holders act without appropriate consumer consent or authorisation.

Additionally, the Inquiry considers that the CDR regime should oblige an accredited person to act efficiently, honestly and fairly in initiating actions. In some sectors, it may be appropriate that a higher standard apply either generally or in relation to particular actions. As existing laws and regulations and sectoral specific regulation will continue to apply to businesses that provide products and services using the CDR, the interaction and potential overlap between industry-specific

consumer protections and the CDR regime should be considered when assessing a sector for designation.

Consideration of the needs of vulnerable consumers, and the participation of consumer representatives, will be important in developing a safe and inclusive CDR, while consumer education will remain a crucial tool in building understanding and trust in the CDR.

As action initiation will require additional data to be exchanged to realise the action, privacy and information security assessments must take place to ensure proportionate and appropriate protections are in place.

Chapter 8 – Opportunities for connecting the CDR to the data economy

The CDR of the future will require a mechanism for ensuring customers are who they purport to be. The level of customer authentication required is likely to be variable for different data sets and different actions in different sectors. A minimum authentication assurance standard, applicable to both data holders and accredited data recipients, should be developed which supports interoperability and flexibility for participants, and meets consumer experience standards.

As Australia's digital economy grows, the established framework and infrastructure supporting the CDR has potential for wider use domestically and internationally. The Data Standards Body expertise in data standards setting should be available for government data sharing initiatives, while the data safety assurances provided by the CDR accreditation process can be leveraged by regimes outside the CDR where similar data protections are required. The CDR should not seek to duplicate regulation imposed by external regulators or industry frameworks. Where applicable the CDR should align with, or recognise external accreditations held by participants.

The CDR presents significant opportunities for consumers and entities providing data-driven services. Under the CDR, the additional data shared, with the consent of the customer, provides opportunities for entities to use artificial intelligence (AI) technologies for product innovation and insights into a business's consumer base. There is a need for further guidance about transparency requirements relating to data aggregation activities such as the use of algorithms.

While there are a range of different approaches in international data portability regimes, there is scope for interoperability. To further this, Australia should continue to use open international standards where available, streamline accreditation to recognise foreign regimes where appropriate and seek mutual recognition with the United Kingdom. Australia should seek an opportunity to convene an international forum and formalise existing dialogue with international policy bodies.

Chapter 9 – Consumer Data Right Roadmap

The Inquiry recommendations have identified a broad range of initiatives that play an important role in the future success of the CDR. To enable effective implementation and maximum benefit to consumers, the path forward must be planned with an understanding of which CDR components complement one another, and what costs are likely to be incurred by participants. An integrated CDR

Roadmap must be developed signalling the major steps to be taken as the CDR develops to enable investors in the data economy to prepare accordingly.

Engagement with stakeholders will remain a priority as the CDR grows. This includes consultation with external reviews and consultations relevant to the data economy within and outside government. Post implementation reviews will enable lessons from implementation to feed into the ongoing work as further sectors and capabilities are introduced to the CDR.

Summary of recommendations

Chapter 1 – Introduction to the Inquiry

Recommendation 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.

Recommendation 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.

Chapter 3 – Expanding the Consumer Data Right to support switching

Recommendation 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.

Chapter 4 – Action initiation framework

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 5 – Action initiation in the banking sector

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 6 – Read access enhancements

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 7 – Consumer safeguards

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 8 – Opportunities for connecting the Consumer Data Right to the data economy

Customer authentication in the Consumer Data Right

Recommendation 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.

Recommendation 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.

Recommendation 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.

Leveraging standard setting and the Data Standards Body

Recommendation 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.

Leveraging the accreditation regime

Recommendation 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.

Recommendation 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'.

Recommendation 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.

Linkages with the AI Ethics Framework

Recommendation 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.

Linkages and interoperability with international data portability regimes

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 9 – Consumer Data Right Roadmap

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Chapter 1: Introduction to the Inquiry

This chapter introduces the Inquiry and the Consumer Data Right (CDR). It outlines four key principles that have guided the CDR's development to date and the broader context of the CDR, before turning to the consultation process that informed this report.

The CDR gives consumers, including individuals and business customers, the right to safely access certain data about them held by businesses. It gives them the right to direct the data holder to transfer that information[1] to accredited, trusted third parties of their choice. The CDR allows consumers better access to information on products available to them. Data holders are also required to provide access upon request to specified information about their products.[2]

Generally, efficient markets work well when: customers make free and informed choices; there is transparent price and quality of products and services; there is a level playing field between competitors and low barriers to entry for new market entrants. The CDR aims to support the efficient and fair operation of markets and improve consumer and business outcomes by addressing well-known economic distortions of information asymmetries, transaction costs and behavioural biases.

The CDR has begun its roll out in the banking sector and the preparations are underway for the energy sector. The potential benefits of the CDR are significant and the economy-wide approach is designed to ensure broader benefits to consumers across the digital economy. Given the nascent stage of the CDR, clarity on its future directions would well-serve the CDR regime and its participants.

Inquiry into Future Directions for the Consumer Data Right

On 23 January 2020, the Treasurer, the Hon Josh Frydenberg MP, announced the Inquiry into Future Directions for the Consumer Data Right (the Inquiry), to be led by Mr Scott Farrell.

The Inquiry was asked to make recommendations to the Treasurer on options to:

- expand the functionality of the CDR
- ensure the CDR promotes innovation in a manner that is inclusive of the needs of vulnerable consumers
- leverage CDR infrastructure to support the development of broader productivity enhancing standards and a safe and efficient digital economy, and
- leverage the developments of the CDR with other countries that are developing similar regimes to enhance opportunities for Australian consumers, businesses and the Australian economy.

[1] This is generally referred to in this report as a consumer's CDR data.
[2] This is generally known as product reference data or PRD.

The Inquiry's recommendations required an examination of:

- how the CDR could be expanded to include 'write' access to enable customers to apply for and manage products (including, for Open Banking, by initiating payments) through application programming interfaces (API)[3]
- linkages and interoperability with existing and potential frameworks and infrastructures, including the New Payments Platform
- how the CDR can be utilised to overcome behavioural and regulatory barriers to convenient and efficient switching between products and providers, and
- similar regimes being developed in other countries and how Australia should be engaging with these countries to leverage the CDR.[4]

Consistent with its Terms of Reference, the Inquiry has focused on future directions for the CDR rather than its current implementation or an assessment of which sectors it should be applied to next.

This report begins by setting out four key future directions for the CDR. The potential of the CDR is demonstrated in a switching example explored in a Customer Journey in Chapter 3.

The Inquiry makes 100 recommendations on topics including:

- expanding the CDR regulatory framework to enable consumers to initiate actions
- enhancing the CDR to support participation and competition in the data ecosystem
- empowering and protecting consumers, including those with vulnerabilities
- leveraging the CDR and its infrastructure domestically and internationally with other data regimes, and
- implementing the Inquiry's recommendations through a roadmap.

These recommendations provide a pathway for a CDR which is consumer focused, encourages competition, creates opportunities and is efficient and fair, consistent with the guiding principles outlined below.

Journey to the Inquiry

Australia's journey towards the CDR spanned several years, beginning with the 2014 Financial System Inquiry, which recognised that increased data sharing could improve financial services outcomes.[5] This was followed by the 2015 Competition Policy Review which recommended improving individuals' access to their own data to improve consumer outcomes.[6] Then, in May 2017, the

[3] An API is software designed to help other software interact with an underlying system.
[4] The complete Terms of Reference are included at Appendix A.
[5] Murray D, Davis K, Dunn C, Hewson C & McNamee B (2014) *Financial System Inquiry Final Report,* Australian Government.
[6] Harper I, Anderson P, McCluskey S & O'Bryan M (2015) *Competition Policy Review Final Report,* Australian Government.

Productivity Commission's Inquiry into Data Availability and Use (PC Data Inquiry) proposed the creation of an economy-wide, comprehensive right to enable consumers to control their data.[7]

In the 2017-18 Budget, the then Treasurer the Hon Scott Morrison MP announced the introduction of Open Banking and commissioned the Review into Open Banking in Australia (Open Banking Review), led by Mr Scott Farrell, to recommend the most appropriate model and implementation plan. The Government subsequently announced, in response to the PC Data Inquiry, that the CDR would initially be established in the banking, energy and telecommunications sectors.

In December 2017, the Open Banking Review provided its Report to the Treasurer, setting out recommendations on how the CDR could begin with Open Banking.[8] The Government accepted the Review's recommendations and began implementation of the CDR with the banking sector. A brief overview of the implemented CDR framework is included at Box 1.1 below.

The phased approach to implementation began with the four largest domestic banks sharing product reference data from 1 July 2019. From 1 July 2020 customers have been able to direct the four largest domestic banks to share certain deposit and card account data. Mortgage and personal loan data is scheduled to be shared from 1 November 2020. Smaller banks will follow from 1 July 2021 with a similar phased approach.

The implementation of the CDR in the energy sector is underway, with the Treasurer designating the energy sector on 26 June 2020. Consultation by the Australian Competition and Consumer Commission (ACCC), the Data Standards Body (DSB) and the Treasury is continuing to inform design of the proposed data access model and implementation in the energy sector. Progressively, the CDR will apply to a broader range of data holders and products throughout the Australian economy.

Internationally, consumer-controlled data portability regimes similar to the CDR have been introduced, or further developed, in recent years. The regimes vary between regulatory-driven or market-driven approaches, the scope of data included and how standards are set. Some countries are, or are considering, expanding beyond Open Banking into other areas of the economy. While each regime is unique, there is scope for connectivity between regimes and an opportunity to share learnings.

Write access (referred to in this report as 'action initiation'), digital identity, the emergence of a new data ecosystem, and interoperability with other jurisdictions[9] were identified in the Open Banking Review for future consideration. These issues have grown in relevance in the context of the CDR, as has the generation of data from digital adoption and digitisation of services in the economy more generally.

It is an opportune time to examine how the CDR can be built upon to support a vibrant digital economy with consumers at its centre.

[7] Productivity Commission (2017) *Data Availability and Use*, Report No. 82.
[8] Open Banking Review.
[9] Open Banking Review, pp. 107-113.

It should be noted that the Inquiry has been prepared concurrently with a number of other reviews, consultations and inquiries considering related or overlapping matters. These include:

- the ACCC consultations on draft CDR rules
- the Senate Select Committee on Financial Technology and Regulatory Technology
- the ACCC's Home Loan Price Inquiry
- the Department of Prime Minister and Cabinet's Digital Technology Taskforce
- the Reserve Bank of Australia's (RBA's) Review of Retail Payments Regulation, and
- the Australian Securities and Investments Commission's (ASIC's) Review of the ePayments Code.[10]

As they are still in progress, the outcomes of these processes and the forthcoming review of the Privacy Act were not available to the Inquiry.[11] Given the breadth and range of inter-related issues, such as data use, innovation, security and privacy, it will be important that these policy issues and the outcomes of these processes are considered as the CDR roll out continues.[12]

Box 1.1 – The Consumer Data Right Framework

Legislation

The CDR has been established primarily through amendments to the *Competition and Consumer Act 2010* (the CCA) and the *Privacy Act 1988*. This enabling legislation:

- sets out the role, functions and powers of each of the ACCC, Office of Australian Information Commissioner (OAIC) and DSB
- outlines the overarching objectives, principles and framework for the CDR
- creates a power for the Minister (i.e. the Treasurer) to apply the CDR to new sectors, and
- enshrines a set of privacy protections for CDR data, which are built upon in the CDR Rules.

Who oversees the Consumer Data Right?

The Treasurer has overarching responsibility for the design and implementation of the CDR framework. The Treasurer has a direct role in designating new sectors, consenting to rules and appointing the Data Standards Chair. The Treasurer works in conjunction with the Attorney-General where the CDR impacts privacy policy. The Treasurer consults with those ministers who have portfolio responsibility for relevant sectors when carrying out the sector designation function or where rules may have significant policy impacts on a given sector.

[10] Some of these processes have been delayed due to the impact of the COVID-19 pandemic.
[11] The Inquiry has had regard to the Interim Report of the ACCC's *Home Loan Price Inquiry*, which was released in April 2020. The Senate Select Committee on Financial Technology and Regulatory Technology also released an Interim Report in September 2020.
[12] Ai Group submission, p. 14.

The CDR operates under a multi-regulator model, comprising of the ACCC, OAIC and DSB. These responsibilities may be reviewed and updated as the CDR roll out progresses.[13]

Sectoral assessments

Banking and energy are the first sectors to be designated under the CDR. Sectoral assessments will identify sectors of the economy to join the CDR. Following a sectoral assessment, advice is provided to the Treasurer on whether to designate a sector. The OAIC advises the Treasurer on the privacy impacts of designating a sector.

The Treasurer then determines whether to designate a sector. In considering a designation, the Treasurer has regard to a range of factors that impact the Australian economy. A 'sector' designation is more specifically a designation of the classes of entity and data in relation to which the CDR will apply and may not align with what is traditionally considered an industry sector.

Consumer Data Right Rules

The *Competition and Consumer (Consumer Data Right) Rules 2020* (the Rules) were made under the CCA. The Rules support the principle-based legislative provisions. They include general rules which would apply across sectors and sector-specific rules where needed for a specific sector.

The Rules impose requirements on a range of issues, including coverage of the CDR in a given sector within the bounds of the sector designation, consumer authorisation to transfer data, safe and efficient data transfer, consumer permissions to use data, information security controls, accreditation requirements and processes, dispute resolution, privacy safeguards, obligations to delete data and record keeping. Once a sector is designated, new rules are made which determine the rights and obligations of participants in that sector.

Consumer Data Standards

The Consumer Data Standards (the Standards) are mainly technical information technology (IT) specifications for the CDR. The Data Standards Chair has ultimate decision-making authority regarding the design of the standards. The DSB assists the Data Standards Chair to develop the standards in consultation with the ACCC, the OAIC, the relevant sector and open working groups. The working groups enable developing standards to be tested, examined and improved.

[13] Draft legislative amendments were released for consultation on 1 October 2020. The amendments are directed at supporting the Government's commitment to applying the CDR to key sectors of the economy, including Open Banking and in the energy sector. The proposed amendments increase the flexibility with regards to who undertakes the sectoral assessment and rulemaking functions alongside a range of minor and technical amendments.

Guiding principles of the Inquiry

The development of the CDR to date has been guided by four key principles which have also guided the Inquiry. These are that the CDR should:

- **Be consumer focused** – for the consumer, about the consumer and seen from the consumer's perspective
- **Encourage competition** – seek to increase competition for products and services so consumers can make better choices
- **Create opportunities** – provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector with better services enhanced by personalised data, and
- **Be efficient and fair** – implemented with safety, security and privacy in mind, so that it is sustainable and fair without being more complex or costly than needed.

Consumer focused

The CDR should promote a well-designed consumer experience. Data transfer and use should be driven and directed by consumers making informed choices. Consumers should have access to a practical means to resolve problems.

Consumers and other participants will not engage with a system that they do not trust. An important component of the CDR will be confidence that data remains protected, that any breach will be remedied, and that the system consumers have integrated into their lives will remain stable and accessible.

For consumers to be confident in the system they must have control of their own data. Consumers must be able to actively choose the consents and authorisations. Key aspects of the CDR system should be transparent — to consumers, participants and regulators. For the CDR to achieve this, consumer voices need to be heard through engagement in its continued implementation.

Encourage competition

The CDR is intended to provide consumers with more choice and to support firms wanting to provide better products and services. The CDR should not unreasonably lock out new participants and should not place unreasonable costs on existing participants. The CDR needs to be capable of balancing the needs of different participants – consumers and businesses – to ensure that the system is fair for all.

The CDR also needs to allow participants to connect to each other, requiring adequate specification of how participants connect. Industry and technical experience and expertise should be drawn on to prevent technology becoming a barrier to entry.

Create opportunities

Many consumer benefits should flow from as yet unforeseen new products and services. To enable innovation CDR needs to be flexible, future oriented and responsive to change.

As technology improves the best solution today may not be the best solution in the future. To incorporate these future solutions, the CDR needs to establish a vibrant and creative data sector that supports better services and is capable of implementing relatively rapid change, in a manner that allows participants to adjust.

Efficient and fair

The CDR should only do as much as is necessary to support industry-driven development of a system that meets consumer needs.

Regulatory costs impact innovation and can create significant barriers to entry to new participants. An excessive regulatory burden could be a disincentive to participation in the CDR. Similarly, if consumers are unaware of the CDR or feel insufficiently protected, they may lack the incentive to participate.

The CDR must, therefore, balance competing interests and incentives so that all prospective participants can efficiently and fairly share in the benefits of the regime.

Broader context of the Consumer Data Right

The CDR has a vital role to perform in providing consumers and businesses with a better way to engage with Australia's digital economy. However, the CDR should not be considered in isolation. For the digital economy to work safely, efficiently and fairly, the CDR needs to function effectively in conjunction with other frameworks and regulation, including those related to consumer protection, information security, data protection and sectoral regulation. The CDR is not able, and is not designed, to provide a solution to every data-related concern or to eliminate every data-related risk. For this reason, balance and clarity are important for the future development of the CDR.

Balance in approach to safety, efficiency and effectiveness

The Open Banking Review noted that alternative data sharing methods exist, new ones will inevitably emerge and that competing approaches to the sharing of banking data would provide an important test of the design quality of the CDR.[14]

The Inquiry believes it is important for the CDR to be safe, efficient and effective while balancing consumer needs with innovation. While consumer safety is essential, the CDR's design and operation must ensure that innovative services made possible by the CDR are of value to consumers. Without its use by consumers, the CDR will not be effective in achieving its intended outcomes. As an extreme example, if the CDR were so narrow in its application, or so burdensome in its processes, consumers

[14] Open Banking Review, Recommendation 1.1, p. 10.

may use alternatives which provide no safeguards or protections at all. In this case, the CDR would provide no improvement in safety no matter how extensive its control of risks.

At the beach, this would be like lifeguards setting the red-and-yellow flags so close together that no one would choose to swim between them, causing everyone to swim beyond the safety that the flags are supposed to provide. On the other hand, a disregard for safety in implementing the most efficient method of sharing data would be counter-productive. That would be like setting the flags so far apart that even the dangerous surf is between them.

Further, businesses participating in the CDR must provide benefits to consumers to encourage its use. It is important that businesses with which consumers want to share their data are able to participate in the CDR, otherwise consumers may either forgo the benefits of sharing their data or use alternative means of sharing their data with businesses, beyond the safety the CDR provides.[15] The balance required for this is discussed further in 'Development of an inclusive data ecosystem' in Chapter 6.

It is not possible to eliminate all risk associated with consumers sharing their data and this should not be the objective of the CDR's design. The restrictions on choice, flexibility and efficiency required to achieve the elimination of risk would cause consumers and business to use alternative data sharing methods lacking the safeguards of the CDR. The Inquiry believes that a balanced approach to safety, efficiency and effectiveness is preferable for the future directions of the CDR.

Recommendation 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.

Clarity in relation to other laws and regulations

With the continued expansion of Australia's digital economy, the use of data will become increasingly important for consumers and businesses. Through its functionality, infrastructure, safeguards, standards and regulation, the CDR is well-positioned to contribute to making the digital economy work safely, efficiently and effectively for consumers and businesses.

The CDR creates a digital messaging channel (similar to a 'data highway') that consumers can confidently use to share their data for purposes they choose. The greater use of data will enable new activities and behaviours in providing products and services to consumers. Most will be for the benefit of consumers, businesses and society generally. Some may not be. Existing laws and regulations, such as Australia's consumer law and, where relevant, sectoral specific regulation, will apply to these new activities and behaviours. Clarity in the relationship between the CDR regime and other regulation which applies in the relevant circumstances will be important.

[15] An example is third party access to digital banking portals.

Examples of regulation applicable in particular sectors to which the CDR applies are set out throughout this report. Consumers' use of the CDR to apply for, and manage, products and services should not be hindered by unintended consequences of existing applicable laws and regulations. Accordingly, it will be important to consider whether regulatory barriers to use of the CDR are deliberate and necessary. Some laws and regulations may need to be enhanced to ensure an efficient experience for consumers, while maintaining appropriate consumer protections. The CDR already incorporates consumer safeguards and additional protections are recommended in Chapter 7 in the event that the CDR's functionality is expanded. These are intended to protect consumers sharing their data and initiating actions through the CDR, and are not designed, nor intended, to regulate business conduct more generally outside of the CDR.

For example, the CDR has not been designed to regulate the lending of money, even though data shared by consumers through it can be used in applying for or providing loans. Data used by lenders may come from many sources in addition to the CDR, and there are specific laws and regulations designed to protect consumers during the lending process. These laws apply whether or not the CDR, or CDR data, is used. For this reason, the CDR regime should not seek to replicate or replace those safeguards.

It will be important that policy makers and regulators are alive to new possibilities for harmful behaviours or practices that the use of data (whether provided through the CDR or otherwise) and its systems may enable so that the appropriateness of regulatory settings for the protection of consumers can be monitored. This will be particularly important when the application of CDR is proposed in a sector. This would ensure that any required protections are not limited to data which is shared using the CDR and, as a result, protect consumers more broadly.

Recommendation 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.

Consultation process

The Inquiry released its Issues Paper on 6 March 2020, inviting interested stakeholders to provide their views. The closing date for submissions was extended by 4 weeks to 21 May 2020 to allow extra time for stakeholders impacted by the COVID-19 pandemic.

The Inquiry received 73 submissions from a wide range of stakeholders including:

- Banks and other financial service providers
- Energy providers
- Payment systems and service providers
- Fintech businesses
- Data consultants
- Consumer and privacy advocates
- Government bodies
- Legal sector
- Peak bodies and industry groups
- Superannuation sector
- IT services
- Individuals

The Inquiry engaged with interested parties through virtual roundtables, small groups and bilateral discussions. Virtual roundtables were held on 15, 17 and 22 July 2020. The Inquiry met more than 300 representatives from interested organisations and groups. Virtual meetings were also held with a range of overseas parties including policy makers, implementation bodies, regulators and academics, to gain insights into international regimes.

Submissions from a wide range of interested stakeholders resulted in a range of views on key issues being considered. It is noted that given the breadth of issues covered that not all stakeholders responded to every issue. The majority of submissions were positive about the CDR and its potential to improve competition and consumer experiences. Most were positive about further expansion, although there was concern about the timing and the impact of COVID-19 on priorities and implementation. A few submissions called for a faster roll-out while others called for a more measured approach. Others called for a review of the current system and a cost benefit analysis before the CDR is expanded to new sectors. Some submissions expressed concern about expansion into particular sectors.

Numerous submissions strongly supported measures to implement switching. They noted switching services have the potential to overcome behavioural factors and practical barriers that prevent customers from following through to switch to products better suited to their needs with lower fees, better rates or features. Other submissions encouraged a cautious approach to measures which enable automated switching as they considered the level of complexity and risk to be significant, with some submitting it could increase the risk of fraud.

A majority of stakeholders that responded on write access, including payment initiation, supported this expanded functionality for the CDR to varying degrees. Despite this support, submissions also expressed concern about the complexity and risks it could create in the CDR. With these risks in mind, several submissions advocated for a cybersecurity capability as part of the CDR. Most submissions addressing payment initiation raised the need to consider upcoming developments in the payments system, including those relating to the New Payments Platform (NPP), when

considering how best to implement payment initiation in the CDR context. Some other submissions stated that the NPP should not be the only solution for payment initiation in the CDR framework and that the CDR should be agnostic to payment systems.

Some submissions expressed strong support for tiered accreditation, allowing more participants to access the CDR system as it would lower the cost of entry. Others did not see the need for it at this time and considered the current accreditation process appropriate to protect consumers and establish trust in the CDR system. The benefits to the data ecosystem from providing access to specialised intermediaries was noted in several submissions. Many submissions supported measures to increase consistency in consents, noting the potential for this to benefit both consumers and accredited persons. However other submissions expressed concern that further standardisation of consent processes may inhibit the ability to innovate and develop services.

A number of submissions expressed the view that consumer protection should be central to any considerations of expansion of the CDR regime, with several emphasising the importance of appropriate conduct by accredited persons in an action initiation context. Many submissions stated that the CDR should be accessible and beneficial to Australians broadly, and should explicitly consider the needs of vulnerable consumers. Submissions demonstrated a large amount of support for measures to increase awareness of the CDR, as well as to promote financial, digital and data literacy more broadly.

Several submissions cited the benefits of digital identification and its potential to support the CDR infrastructure, including the ability to support greater and frictionless switching. It was also noted that the current approaches to digital identification are fragmented and not widely adopted.

Regarding leveraging the CDR regime, a submission suggested assessing the benefits of consistency in standards across government departments. Others suggested simplifying or centralising the CDR regulatory arrangements. A few submissions suggested that the CDR should leverage existing accreditation in other parts of the economy. Submissions suggested using international and open standards where possible to support international interoperability. A few submissions raised the idea of mutual recognition or passporting regimes. One submission cautioned against prioritising international cooperation and interoperability at the expense of what is best for Australian consumers.

A few submissions called for a roadmap to bring together the different elements needed to successfully expand the CDR and provide some certainty around investment decisions.

The Inquiry considered these wide-ranging and insightful views within its Terms of Reference. These have informed and helped shape the future directions for the CDR that follow in Chapter 2.

Chapter 2: Future Directions for the Consumer Data Right

The CDR strengthens the foundations of Australia's digital economy. It makes it easier for consumers to access and use their data, obtain insights and advice, choose the products and services that suit them best, and to act on those choices. The CDR should continue to have strong privacy and information security safeguards so consumers can be confident in sharing their data. By incorporating features designed to provide flexibility and fairness, the CDR should provide businesses with the clarity, certainty and consistency needed to invest in the future of Australia's digital economy. In these ways, the CDR should deliver benefits for Australia and Australians.

Future Directions

The CDR was originally designed for the safe and efficient transfer of data at a consumer's request. The Inquiry is considering how the CDR could be expanded in four directions:

1. *Beyond data sharing,* ***towards data-empowered consumers*** – Expanding the CDR's functionality to improve consumers' ability to use and benefit from their data so that it can transform the consumer experience
2. *Beyond open banking,* ***towards an economy-wide foundation*** – Growing the CDR throughout our economy purposefully and competitively so that it can become a foundation of Australia's digital economy
3. *Beyond a standalone system,* ***towards an integrated data ecosystem*** – Connecting the CDR with other frameworks and systems so that it can generate a vibrant ecosystem to support a sustainable data future
4. *Beyond Australia's borders,* ***towards international digital opportunities*** – Connecting with overseas data frameworks to promote cross-border consistency, connectivity and community.

Direction 1: Beyond data sharing, towards data-empowered consumers

Since its inception, the CDR has always been consumer-driven. This focus will enable transformative consumer experiences, through simple, secure and convenient digital pathways. These will enable consumers to meaningfully engage with, and benefit from, their data in the digital economy.

Expanding functionality for consumers

While the CDR gives consumers the right to share their data, expanding its core functionality will enable consumers to take insights and recommendations from data sharing and put them into action. Developments in this direction are:

- **Streamlined switching** – supporting consumers to easily and efficiently switch between products or services (refer to 'Expanding the Consumer Data Right to support switching' in Chapter 3)
- **Action initiation** – enabling consumers to conveniently and safely apply for, accept or manage new products and services (refer to 'Action initiation framework' in Chapter 4), and
- **Payment initiation** – empowering consumers to authorise, manage and facilitate payments securely (refer to 'Action initiation in the banking sector' in Chapter 5).

Making data work for consumers as they choose

The CDR should be developed to be inclusive of the needs of all Australians. It should assist those with lower levels of digital and data literacy to confidently engage with the digital economy. It should allow consumers to choose new and innovative products and services suited to their privacy preferences and risk appetite. Developments in this direction are:

- **Clarity in data use** – improving consumer understanding of the proposed use of their data so that their consents are more meaningful (refer to 'Additional consent measures' in Chapter 6)
- **Control over data use** – improving consumer ability to securely view and manage those consents in one location (refer to 'External consent management' in Chapter 6), and
- **Data confidence** – reinforcing consumer protections, including for those with low data literacy or who are otherwise vulnerable, so that they can more confidently engage in the digital economy and, should they choose, use data to their advantage (refer to 'Consumer safeguards' in Chapter 7).

Direction 2: Beyond open banking, towards an economy-wide foundation

Beginning with Open Banking, the CDR is intentionally cast to be economy-wide. This approach will broaden and strengthen the foundations of Australia's digital economy. It promotes competitive dynamics within and across sectors, and supports the growth of start-ups and new business models. Ultimately, this will give consumers greater choice across the economy. Developments in this direction are:

- **Sector-by-sector growth** – continuing to consider the inclusion of more sectors informed by sectoral assessments (refer to 'Integrated CDR Roadmap' in Chapter 9)
- **Enhancing competition between participants** – aligning obligations for data holders and accredited persons that hold consumer data in all sectors (refer to 'Reciprocity' in Chapter 6), and
- **Innovative growth** – facilitating the use of the CDR to share data sets on the initiative of participants and not designated by government, including innovative data sets that could be provided on a chargeable basis (refer to 'Voluntary data sets' in Chapter 6).

Direction 3: Beyond a standalone system, towards an integrated data ecosystem

The CDR encourages a vibrant and competitive environment where innovative businesses can create new products and services. This will promote a thriving data ecosystem where consumers can confidently engage with CDR participants of all sizes. CDR infrastructure will be leveraged to develop strong connections with the rest of the digital economy.

A competitive, creative and accessible data ecosystem

The diverse, efficient and competitive data ecosystem should consist of CDR participants and related service providers who value quality data and seek out new opportunities and innovations. Developments in this direction are:

- **Competitive support services** – providing choice and specialised services to CDR participants supported by other elements of the digital economy (refer to 'Development of an inclusive data ecosystem' in Chapter 6)
- **Inclusion of trusted advisers** – permitting consumers to pass their data to trusted advisers in the broader data and services ecosystem, such as accountants or financial advisers (refer to 'Development of an inclusive data ecosystem' and 'Tiered accreditation' in Chapter 6), and
- **Balance and clarity in developing the CDR** – ensuring that it is safe, efficient and effective in its implementation (refer to 'Broader context of the Consumer Data Right' in Chapter 1).

Leveraging the Consumer Data Right infrastructure

The existing CDR infrastructure includes a rigorous 'data safety licence' through its accreditation regime and data standard setting. These could assist the Australian Government in developing productivity-enhancing initiatives within the digital economy. Developments in this direction are:

- **Support interactions with other regulatory frameworks** – informing and assisting the effectiveness of existing regimes (refer to 'Leveraging standards setting and the Data Standards Body' in Chapter 8)
- **Reduce regulatory burden** – supporting efficient interactions in the regulatory ecosystem through the CDR recognising other regimes (refer to 'Leveraging the accreditation regime' in Chapter 8), and
- **Connecting up the data economy** – linking participants and initiatives of the data ecosystem, including digital identity services (refer to 'Customer authentication in the Consumer Data Right' in Chapter 8).

Direction 4: Beyond Australia's borders, towards international digital opportunities

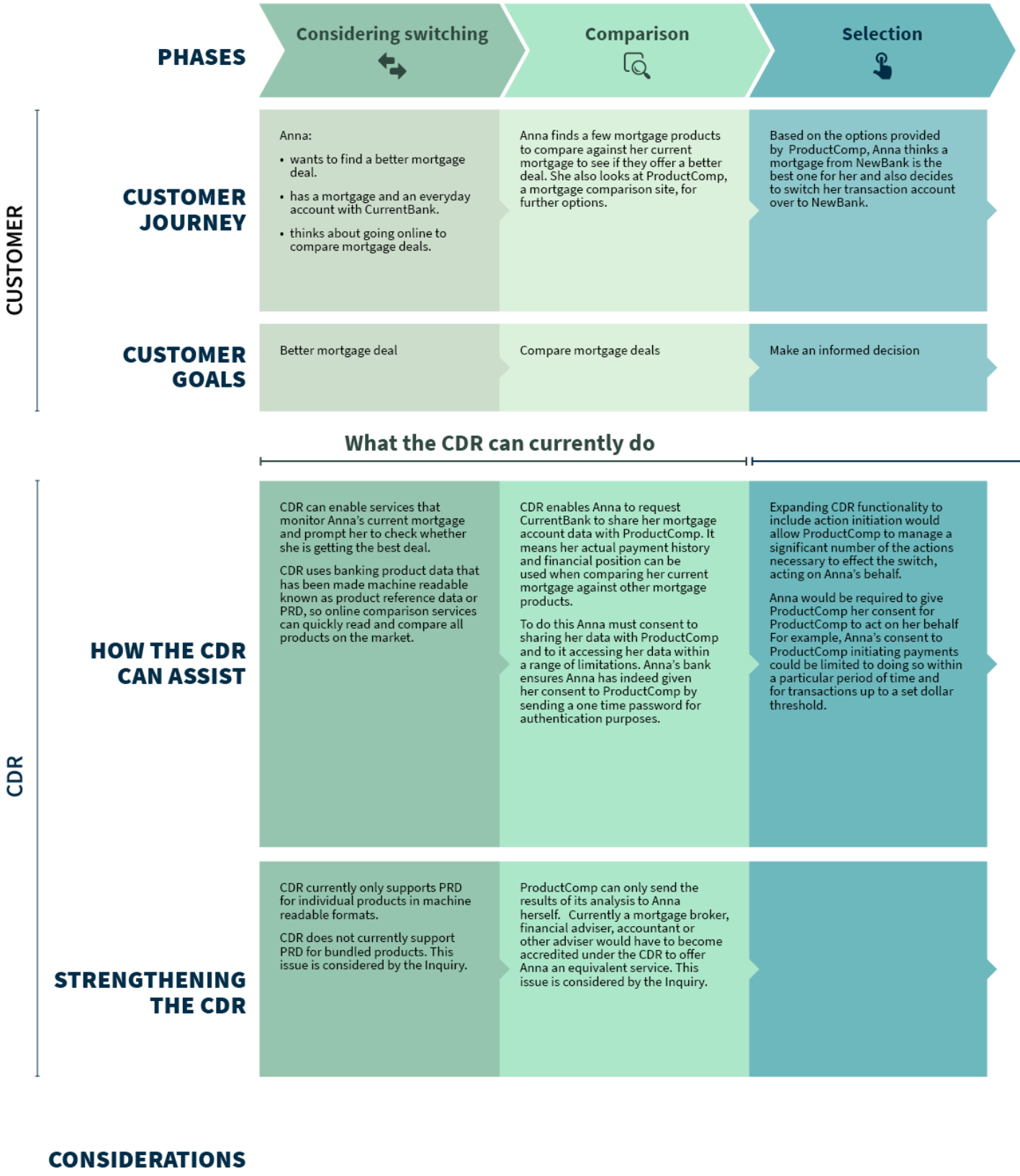
The CDR is one of the leading data frameworks in the world. Connecting with similar regimes overseas will support international trade and a sustainable data future. This should create new

opportunities for providing data-driven services in the global marketplace and more choice for Australian consumers. Developments in this direction are:

- **Cross-border consistency** – supporting consistency in the setting of key standards and principles (refer to 'Common rules and technical standards' in Chapter 8)
- **Cross-border connectivity** – supporting international data portability and interoperability of regimes (refer to 'Streamlined accreditation' in Chapter 8), and
- **Australia as a proactive cross-border contributor** – to the international community of countries with consumer-controlled data regimes (refer to 'International forums' in Chapter 8).

Australia's CDR regime is considered by many to be world leading. Implementation of CDR in the banking sector is advancing and other jurisdictions often look to Australia as a model when developing their systems. The Australian model of an economy-wide data sharing regime has inspired other countries to extend their regimes beyond banking. It is critical that Australia continues to develop a world-leading CDR to support opportunities for Australian data-driven businesses and deliver a world-class digital economy for Australian consumers to enjoy.

Figure 3.1 — Switching mortgages with the CDR



Applying for a new mortgage	Internal bank checks	Approval	Open & close accounts
Anna undertakes all the steps necessary to apply for the new mortgage and submits her application to NewBank. These steps include: • filling out application forms • gathering and providing relevant documents • demonstrating her financial position	NewBank must comply with responsible lending requirements, and other relevant regulatory requirements, in relation to Anna's application. NewBank must also undertake legislatively required Know Your Customer (KYC) checks.	NewBank gets back to Anna – her mortgage is approved! However there is still a number of things that need to be done to finalise the switch.	Anna must: • set up new accounts with NewBank • close out her old accounts with CurrentBank • cancel her existing direct debits and transfer any remaining funds
• Sign up for a new mortgage • Swap transaction account	Provide all necessary documents to NewBank	Approved by NewBank	• Close old accounts and open new ones with NewBank • Transfer funds to new account

What the CDR could do in the future

ProductComp could offer a service that finalises Anna's NewBank mortgage and transaction account applications and electronically send it on Anna's behalf. ProductComp could populate some of Anna's mortgage application, including her personal information (name, address, DOB) and necessary financial information that NewBank requires when considering Anna's mortgage application. ProductComp could also calculate and include analysis of her monthly expenditure to indicate how much she is able to repay each month.	CDR can enable streamlined creditworthiness, lending assessments and pricing analysis.		Action initiation functionality could allow a service like ProductComp to manage the banking elements of Anna's switch: • close her old accounts with CurrentBank • establish her new accounts with NewBank • cancel old direct debits from CurrentBank and re-establish new direct debits with NewBank • make any necessary scheduled payments • pay any outstanding fees It could also support streamlined switching services which could remove the need for Anna to regularly monitor her mortgage to ensure she is on the best mortgage deal.
CDR has capacity to streamline much of the application for a new mortgage however a range of processes and communications will remain outside the CDR. For example, CDR cannot support non-structured data like copies of builders contracts in pdf. In the future it is possible that some services like ProductComp may offer to also manage these aspects of the transactions as part of an integrated service.	Onboarding assessments are not currently able to be processed by non-accredited parties using the CDR. The capability to outsource checks of this nature to other providers accredited to receive CDR data is considered by the Inquiry. CDR could also be used to share KYC outcomes.	Moving data from a consumer's old bank to their new bank under CDR can only happen if the new bank is also an accredited data recipient under the CDR regime. It is anticipated that banks will become accredited data recipients to enable switching between banks, as well as these services being provided by other accredited providers.	

To fully streamline the switching process both banks and service providers like ProductComp will need to be able to send and receive data in standardised machine readable formats. This has been achieved for the first stages of Open Banking however broader work would be required to develop APIs and standards to facilitate switching.

Current legislative safeguards under the AML/CTF Act require banks to verify the identity of their customers. NewBank will need to verify that Anna is in fact Anna before a new account can be established.

Identity verification is different from and requires a higher threshold of proof from customer authentication processes within the CDR framework.

Anna has a number of other processes to complete as part of the switch to NewBank that currently are not digitised or are processes outside the CDR framework.

For example:
- Conveyancing
- Signing the new mortgage documents
- Updating the relevant State or Territory register
- Transfers of real and personal property security interests
- Other transfers (connections, messages to externals/services)

Chapter 3: Expanding the Consumer Data Right to support switching

This chapter discusses how expanding the CDR by building on the current data sharing functionality and including action initiation could increase consumer convenience and ease of engagement, while further encouraging innovative and dynamic data-driven services. The latter half of this chapter looks specifically at how both action initiation and CDR data sharing functions could be used to assist consumers switch products and service providers. It also considers the behavioural and practical barriers to convenient and efficient switching.

To provide an illustration of how an expanded CDR can streamline switching, this chapter is accompanied by a customer journey in Figure 3.1 outlining the normal steps a consumer would take to switch their mortgage and transaction account from one bank to another. It indicates what is possible under the current CDR regime and what could be possible if accredited persons[16] had the power to initiate actions on a consumer's behalf and do more to assist in switching.

Expanding the Consumer Data Right – data sharing and action initiation

Read access and write access

Read access and write access are technical terms used to describe the type of powers given to third parties engaging with data holders.[17] Read access is the ability for a third party to download or view specific information held by the data holder, while write access is the ability for the third party to give the data holder instructions to take actions.

In a general context, a third party with read access to data held by a data holder can potentially use and analyse this information to provide services to a consumer. This provides a form of data sharing, and the read access function will be referred to as 'data sharing' by the Inquiry. In this relationship the accredited person can 'pull' data from the data holder, but cannot interact with them in any other ways.

An accredited person with write access to a data holder can send the data holder instructions. This can enable them to cause the data holder to create or change information they hold, in a sense 'writing' new information. The range of instructions that can be sent are not limited to updating or changing information, making the term 'write access' potentially misleading.[18] Depending on the

[16] For ease of understanding the report will use the existing CDR term 'accredited persons' to include persons who have or will receive data.
[17] For ease of understanding the report will use the existing CDR term 'data holders' to include persons to whom instructions are sent.
[18] That said, record keeping obligations (under the CDR or under other laws such as taxation or corporations laws) are likely to cause record creation even in respect of instructions not primarily directed at altering records.

actions specified, a person with write access could potentially apply for products on another's behalf, update personal details, initiate payments or otherwise use products or open and close accounts.

The Inquiry will use the term 'action initiation' rather than write access.

What the Consumer Data Right currently offers consumers – data sharing

Currently a primary use for CDR data sharing is the provision of an efficient way for consumers to identify the most appropriate product or service that suits their individual needs. However CDR data sharing can also be used to support a range of other services, including financial management and budgeting services.

To share the necessary data with the business offering them these services, a consumer gives their consent to that business (the accredited person) to collect their data from their data holder (for example, a bank or an energy company). The accredited person obtains and analyses the consumer's CDR data, which can include usage and behavioural patterns. A budgeting app could use this information to identify areas of spending that can be reduced and assist the consumer in managing their finances.

A comparator website could access the consumer's CDR data and compare it to information on available products and services. This product information (product reference data or PRD) is in machine readable format and is also made available under the CDR. The comparison can be done electronically and rapidly. The accredited person can then make recommendations on which products or services may best suit the consumer's needs. A consumer can use the accredited person's assessment to make an informed decision on whether or not to switch to a more competitive or suitable product or service.

Data sharing reduces the amount of work and time consumers would otherwise be required to spend in researching and comparing the wide range of potentially complex products in the market. It boosts consumers' power, helping to reduce informational asymmetries and encourage competition. This aligns with the original goals of the Open Banking Review of increasing the control, choice, convenience and confidence of customers. The implementation of data sharing to date has been an important first phase. Looking to the immediate future, expanding both participation in the data sharing ecosystem, the functionality available and the data that resides in that ecosystem will enable growth and innovation in new services. Such services could seek to assist consumers by, for example, providing data analysis, pattern identification and managing their data.

However, data sharing alone does not overcome all the barriers that reduce consumers' ability and willingness to confidently make beneficial choices in a convenient manner. The cost to consumers of overcoming friction when carrying out actions with their providers, as well as behavioural issues such as status quo biases, reduces the ease and convenience with which consumers can make choices and act.

What action initiation could offer

Enabling action initiation would allow third parties to assist consumers in overcoming these issues and reduce the complexity, time and costs to consumers seeking to carry out actions. Action

initiation could support a range of actions that may be undertaken on the consumer's behalf. These may differ depending on each sector but could include enabling accredited person to initiate payments, update personal information, change billing delivery preferences, open and close accounts and assist consumers to switch from one provider to another. Accredited persons may design services that offer to undertake these actions independently, or in combination with, data sharing services.

Finder made the following comments in their submission to the Inquiry:

> *[A] read-only version of the CDR gives consumers powerful insights about the way they spend money, but it is a write-access enabled version of the CDR that gives consumers the power to act on these insights quickly. Without write-access, a consumer would still have to go through the same slow process to change providers or make/cancel a payment. Write-access to the CDR could act as an antidote to the inertia we can see in our research.*[19]

Enabling action initiation could also provide benefits beyond facilitating a consumer's interactions with a single service provider. For instance, allowing an accredited person to initiate an action could assist consumers by allowing them to perform tasks which would otherwise require them to interact with a wide range of dispersed service providers, through a centralised portal of their choice. Further, action initiation could support a service that helps consumers when they are moving house by managing the opening and closing of energy accounts. The same service could also assist by updating the consumer's address with other identified service providers when they move. This could reduce friction and give consumers greater choice in determining their preferred customer experience when dealing with their current and potential service providers. This could result in a competitive market of digital businesses offering these services, potentially lowering costs for service providers who do not want to develop these systems on their own. This ability to 'decouple' the client interface with one or more service providers and have it provided by a third party has the potential to significantly disrupt existing business models to the benefit of consumers.

Action initiation itself is not a product. It is a function that could be offered by service providers to be used by innovative businesses to develop products for and solve problems facing consumers, both now and into the future. The breadth of the use cases and range of benefits that could be enabled by action initiation is dependent on how the framework is designed. In its submission to the Inquiry, Spriggy commented that:

> *Extending the CDR to include write access has tremendous potential to support new and existing businesses to develop innovative offerings that help simplify the lives of Australian families.*[20]

As with most innovations however, action initiation also has the potential to introduce a range of new risks. Without the proper safeguards, action initiation could enable a third party to act in ways contrary to the consumer's express wishes, causing the consumer to come to severe harm. The variety of harms would be dependent upon the sectors designated and the actions permitted.

[19] Finder submission, p. 5.
[20] Spriggy submission, p. 3.

A consumer who uses a regime to allow another to act on their behalf is, therefore, demonstrating strong trust that the system will have measures in place to prevent them being taken advantage of.

Box 3.1 – Account aggregator – an example of action initiation

Data Sharing – If an accredited person can access data from a number of banks, it could view and transform this information to provide services to the consumer. The accredited person could, for instance, offer a service that enables the consumer to view all their financial products in a central location. This service would be limited however, as the consumer would need to contact their individual banks to update their information, close their accounts, open new accounts, or make payments.

Action Initiation – If an accredited person can both access data from a consumer's banks and initiate actions with them, then they could offer consumers a more complete service to manage their finances. The accredited person could now provide the same financial overview as described above, as well as enabling the consumer to centrally initiate actions such as registering for new accounts, closing old accounts and making payments.

Pursuing safe and effective action initiation would be beneficial for the same reasons that data sharing has been enabled. Allowing a consumer to elect how they wish to engage with a service provider increases their control over the products that they use and increases the range and accessibility of choices available to them. This encourages innovative businesses to continue to develop new products that will increase the convenience with which consumers can access services.

Any attempts to enable action initiation functionality must include strong safeguards to provide consumers with confidence when engaging with the system.

The Inquiry has considered the magnitude of this change including where responsibility and liability should most appropriately reside and what protections are necessary for both consumers and data holders.

The Inquiry has also looked closely at the role of consent in this process as robust consent requirements are necessary to ensure consumers are properly informed, clearly understand how their data is being used, and have the ability to set clear parameters within which these action initiation services operate.

Behavioural barriers to consumers engaging with services

It has been observed that consumers do not regularly or frequently engage with or reassess services once they are established and rarely take steps to change, even when a change is likely to provide greater benefits. Examining why this is the case has been the topic of behavioural economic analysis and a number of consumer studies and stems from both behavioural and practical barriers.

In its submission to the Inquiry, Deloitte provided a clear breakdown of six key behavioural biases that affect consumers' willingness to engage, identified from its research in the field as shown in Box 3.2.

Box 3.2 – Behavioural biases as outlined in Deloitte's submission[21]

- **Analysis paralysis*:*** 'There are too many options, I just can't decide.'

  Consumers freeze when too many choices are presented. Decision paralysis brought on by the inability to choose between options is typically the result of cognitive overload and fatigue. This state of choice overload tends to reduce consumers' confidence in a decision they have made and can prevent making one at all.

- **Facing an uncertain future:** 'I know I should… but that can wait.'

  Consumers strongly prefer present payoffs to future rewards. While the potential savings from a lower mortgage rate can be significant over 25 years, they may not create enough of a sense of urgency in people to offset the more immediate transaction costs of gathering information and switching now.

  Cognitive research has shown that people often learn and make decisions using 'case-based reasoning'—solving problems by recalling previous situations and reusing that information. With no personal experience, feedback, or a memory of past reference points, consumers feel ill-equipped to make the right call; even after gathering additional information to supplement their view, they are often left with the sneaking suspicion that important 'unknown unknowns' remain. The behavioural tendency to explicitly or implicitly lean on anchors—trusted reference points—provides our brains with a place to start understanding what good looks like. Without these anchors, and with only tenuous confidence in their own ability to choose wisely, consumers stall and do nothing—sometimes indefinitely—rather than commit to the wrong option.

- **The impact of emotion on behaviour:** 'I worry about failure, and I hate feeling dumb.'

  Consumers are often overcome by fear of failure when presented with an important choice. They hate the idea of being forced to live with a sub-par option, but, just as importantly, they worry about looking silly or stupid for having chosen poorly.

- **Loss aversion effect:** 'I'm worried about what I'll lose… and not certain of the value of what I'll gain.'

  Consumers focus on what they'll lose by changing provider. They put three times as much weight on what they'll lose, compared to what they may gain.

- **Endowment effect:** 'I value what I have more than something new.'

  Consumers value things they've previously made a decision to acquire.

- **Status quo bias:** 'I prefer to stick with what I have … even if there's a better alternative.'

  Consumers value stability, preferring to stick with what they already have.

[21] Extract from the Deloitte submission, pp. 18-19.

Switching using the Consumer Data Right

In its Terms of Reference, the Inquiry was directed to examine how the CDR can be utilised to overcome behavioural and regulatory barriers to convenient and efficient switching between products and providers. This is examined below, with regulatory barriers also discussed in later chapters of this report.

The Inquiry sees broad economic and competition benefits in expanding participation in data sharing and in action initiation to enable and encourage greater switching by consumers. Expanded participation in data sharing would allow other entities (with consent) to access consumer data and assist in the consumer's decision making process. For example, enabling a consumer's financial planner to access CDR banking data would allow that adviser to get a more granular picture of their client's spending and advise their client on switching to better suited products.[22] Action initiation will simplify product switching and provide a framework for switching with less friction over the CDR's secure digital channel. It is also likely to assist in encouraging consumers to engage more with the products and services they already have and those that are available to them.

Encouraging and simplifying switching stimulates competition and innovation in products and services as providers are required to be more responsive to the market demands of consumers in their product offerings and prices, and are incentivised to retain existing customers who may otherwise be inclined to switch.

Risks and costs

Switching can also present risks to consumers. The decision to switch may weigh on the attractiveness of one feature of a new good or service (for example, a better interest rate) while the loss of other features or functionality may not be equally considered.[23]

Switching currently takes time to action and may present hidden costs (for example, exit fees if breaking a 24 month contract when switching mobile phone plans), or additional burdensome tasks such as having to individually cancel and re-establish direct debits if switching transaction accounts.

In the example of fully automated switching – where an accredited person manages the entire switching process on the consumer's behalf and has been granted power to switch the consumer whenever a better deal is identified – there could be a heightened risk of the customer being signed up to a service that does not in fact meet their needs. It is also possible that a consumer could be switched to products more frequently than is in the consumer's best interest but instead serves the interest of the accredited person initiating the switch.[24]

However, by not switching Australian consumers are bearing unnecessary costs. The average Australian household could save up to $1,000 per year on their home loan if they switched to

[22] Financial Planning Association of Australia submission, p. 1.
[23] Detailed examples of this were provided in the Australian Privacy Foundation submission, p. 3.
[24] This issue was explained in the CHOICE submission, p. 4.

another lender – but many do not.[25] Similarly, consumers who switch credit cards could realise savings of $200 a year, however only 17 per cent of credit card holders switch credit cards over a 5 year period.[26] CDR-facilitated switching could help consumers access these savings by making it easier and faster to switch. In its submission to the Inquiry, FinTech Australia stated that the facilitation of switching, 'could be one of the most influential aspects of an expanded CDR.'[27]

Customers choosing to stay with their current provider and paying more are sometimes described as paying a 'loyalty tax'. It describes a situation where loyal customers pay more for services than new customers or customers who are prepared to ask for a better price. The situation has been identified by the ACCC in the banking and electricity sectors.[28] The Australian Government has responded to the ACCC's reports, however the identification of this practice in the ACCC Home Loan Price Inquiry Interim report is a very recent example of the kind of market behaviour that could be mitigated by a consumer base that was willing and empowered to switch providers more often.

Current consumer appetite for switching

Australians tend to stick to their banking providers for a long time. A recent Deloitte consumer study found only 19 per cent of customers have changed providers of at least one of their banking products in the last 3 years. However, the switching rates for individual banking products are estimated at about 10 per cent as consumers may switch providers on a particular banking product, but typically do not change all of their banking products at the same time.[29]

In its submission to the Inquiry, Finder referenced results of its Consumer Sentiment Tracker survey which demonstrated that from September 2019 to April 2020, 17 per cent of consumers surveyed switched mobile plans, 13 per cent switched energy services and 3 per cent switched home loans. Home loans were found to be the most difficult product to switch while being the product with the highest savings potential.[30] The Australian Energy Market Commission (AEMC) 2020 Retail Energy Competition Review reported an average of 19 per cent of customers switching energy retailers across National Energy Market (NEM) States on 2019 data, with many of those taking their business away from the big three retailers to sign-up with energetic smaller players.[31] This figure represents a 5 per cent decrease from 2018 and is a 3 year low.[32]

[25] Based on Productivity Commission data, *Competition in the Australian Financial System Inquiry Report*, 2018 Report no. 89, p. 13.
[26] Based on Silva-Goncalves J, 2015, *Australians' Switching Behaviour in Banking, Insurance Services and Main Utilities*, Queensland University of Technology, Brisbane, pp. 10-11.
[27] FinTech Australia submission, p. 10.
[28] ACCC, 2018, *Retail Electricity Pricing Inquiry final report,* p. 24, ACCC, 2018, *Residential Mortgage Price Inquiry final report*, p. 8, ACCC, 2020, *Home Loan Price Inquiry interim report*, p. 9.
[29] Deloitte *Open banking: switch or stick? Insights into consumer switching behaviour and trust*, October 2019, p. 48. This study was referred to in some submissions to the Inquiry, including that of Westpac.
[30] Finder submission, p 3.
[31] AEMC, 2020, *Retail Energy Competition Review*, p. xiii.
[32] AEMC, 2020, *Retail Energy Competition Review*, p. xiii.

Conversely, the continued presence of a market for budgeting and financial management services that use screen scraping to assist consumers with managing their finances, and innovation in services that assist consumers find and switch to better energy deals,[33] indicates that consumers are willing to switch and to use services which advise on and manage the process for them.

Creating an environment that encourages switching

A range of elements is necessary to create an environment in which consumers feel encouraged to switch. Some of these elements can be addressed within the CDR framework itself and will be enhanced by recommendations made by the Inquiry. However, there are also elements external to the CDR which will have an important impact on how consumers respond to and embrace the potential for CDR driven switching.

Encouraging consumer engagement

In its submission to the Inquiry, Deloitte observed that the majority of bank customers report that they are satisfied with their current provider and generally do not actively seek information about others.[34] Increasing financial literacy and data literacy will encourage consumer engagement with the services they use, the costs they are incurring and how exploring other options facilitated by the CDR may provide them with better outcomes. It is important to note that a person may be financially and digitally literate, or confident in one area and not the other, or neither.

The Open Banking Review recommended a consumer education program for Open Banking, and encouraged industry participants, industry groups and consumer advocacy groups to lead and participate, as appropriate, in consumer awareness and education activities. In its interim report the Senate Select Committee on Financial Technology and Regulatory Technology recommended the Australian Government work with the banking industry to establish and implement targeted campaigns to educate consumers on the Consumer Data Right and the opportunities that Open Banking provides.[35] The Inquiry notes the Government's commitment to support an information and awareness campaign to introduce CDR to consumers and businesses, and drive uptake in this financial year.[36] The Inquiry makes further recommendations in relation to consumer education in Chapter 7.

Access to information on available offerings

Increased consumer engagement is linked to access to information. Consumers need to have access to the information required to compare offerings, including information about how to use the products or services on offer. That information needs to be available in a form that is usable. The data and consumer experience standards, which already form an integral part of the CDR framework,

[33] For example, the bank 86400 offers an energy switching service that assists customers to switch their energy provider.
[34] Deloitte submission, p. 17.
[35] Senate Select Committee on Financial Technology and Regulatory Technology, Interim report, Recommendation 21.
[36] *Economic and Fiscal Update July 2020*, National Consumer Data Right — implementation, p. 170.

contribute to the usability of the information provided within the CDR. Recommendations designed to further enhance the use of CDR standards are made in Chapter 8.

Access to assistance

The volume and complexity of information available about products often results in consumers not being able to properly assess which offering best suits them.[37] Through the CDR, accredited persons could provide services to help consumers better engage with this volume and complexity of information, particularly if broader participation options are available such as tiered accreditation for intermediaries.[38] However, others may be able to assist consumers to make informed decisions about particular products, such as financial advisers and mortgage brokers who would also benefit from access to a consumer's CDR data.[39] Recommendations to enable broader participation by these advisers are contained in Chapter 6.

Switching between products and providers

Once a better offer has been identified, consumers may need assistance to navigate the process of moving to the better offer. Consumers may also not follow through with switching if the process is inconvenient or too complicated, notwithstanding the potential major savings of doing so. This step involves applying for new products, meeting identification requirements for the new provider and enabling the new provider to carry out various assessments. Once a new product has been acquired, a consumer may need to transfer data or, in banking, funds from the old provider (or to pay off outstanding amounts with the old provider). Old accounts may be closed.

As CDR rolls out into new sectors there will be a need to ensure regulatory settings within each sector facilitate the sharing of CDR data with the consumer's consent and do not unnecessarily impede CDR-enabled switching. Examples of sector-specific requirements include anti-money laundering and counter-terrorism financing requirements,[40] or relevant lending standards in banking or explicit informed consent requirements in energy. Recommendations to this effect are contained in Chapter 4.

There are also particular regulatory considerations that must be considered in the implementation of the CDR regime in any sector to ensure that the action initiation functionality that enables switching is safe, secure and efficient.

Appropriate consent requirements

Consumers need to understand and be able to give their informed consent to authorise an accredited person to carry out the identified actions and services they offer to undertake or provide. Recommendations in Chapter 4 have been designed to significantly enhance the understanding and usability of CDR consents for consumers.

---

[37] In its *Comparator website industry in Australia report* (2014), the ACCC observed that complexity and information overload can limit the ability of consumers to fully access the benefits of competition, p. 5.
[38] This is noted in the TrueLayer submission to the Inquiry, p. 6.
[39] This is explained in the Mortgage and Finance Association of Australia submission, pp. 3-4.
[40] Requirements under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

Privacy safeguards and authentication measures

The CDR must ensure that appropriate safeguards are in place to protect consumers from instances of fraud or misuse of their data. Ensuring robust privacy safeguards is essential for consumers to feel secure in granting a third party the ability to use and access their data. There is also a need for robust methods of customer authentication to provide all parties with confidence that only the relevant consumer is providing instructions on access to and use of their data, and initiation of actions. Recommendations to improve privacy safeguards are contained in Chapter 7 with those relevant to authentication in the CDR in Chapters 4 and 8.

Appropriate transfer of data allowed within the Consumer Data Right regime

Currently the CDR regime requires that CDR data can only be transferred to an accredited person. This impacts the switching process. For example, a customer has decided they wish to switch banks. However, the customer's new bank cannot receive the necessary information to process the switch from the customer's current bank unless the new bank becomes an accredited person. Recommendations to address this are made in Chapter 6.

Consumer trust and confidence necessary for switching using the Consumer Data Right

Gaining community trust and confidence in how data is managed and used is one of the broad criteria that informed the Productivity Commission's recommendation to create a consumer data right in Australia.[41]

The CDR has recognised the need for trust in the first of its four guiding principles – that it *be consumer focused, be for the consumer, about the consumer and seen from the consumer's perspective*. This principle has informed the design of a CDR framework that emphasises consumer privacy, consent and security of data.

However, consumers themselves will likely have limited visibility of the backend work of the data transfer infrastructure. They will be more aware of and more focused on their interactions and relationship with the accredited persons and data holders that will handle their data. They will be seeking a particular outcome from these providers that reflects the benefits they understood they were to receive from providing access to their data under the CDR.

The Inquiry recognises how a robust CDR framework and the practices of the entities handling CDR data are fundamentally connected in encouraging consumer take up of CDR based services and stimulating a market that supports future growth and innovation in these services. While the CDR itself is a mechanism which can assist in addressing consumer inertia by reducing effort and mental load on consumers, its benefits cannot be fully realised without both trust in the CDR framework and the services it supports.

[41] PC Data Inquiry Report, p. 13.

The Consumer Policy Research Centre has observed the role responsible business practices and regulation centred around good consumer outcomes can play in enshrining trust and enabling ongoing data sharing for continued innovation and economy-wide benefit.[42]

Switching-related processes

After deciding to switch there is often a range of processes to complete before a new product or service can commence. This section indicates what is now within the scope of the CDR regime to assist with switching, how it could assist with action initiation in the future, and what is outside the scope of the CDR.

Populating the application form

Customers switching products often have to fill out detailed and onerous application forms. Manual completion of forms may lead to inaccuracies, for example, in banking from consumers not having accurate insights into their own expenditure patterns.

Under CDR, it is possible for an accredited person to assist a customer by automatically populating much of their application. For a new bank to be able to do so on behalf of a new customer would require 'pulling' data from their current bank using the CDR. This can only happen if the new bank is also an accredited person under the CDR regime. The Inquiry is aware that one of the first accredited persons, a bank, is currently offering a service to assist customers to switch from identified data holders. Switching will be further enabled when more banks become accredited persons.

The Inquiry considers expanding data sharing to enable CDR driven services – such as those that could support this function for parties not accredited under the CDR regime – in Chapter 6.

Lodging an application

Switching may be greatly streamlined by enabling electronic lodgement of applications in standardised forms by accredited persons on behalf of consumers and could be enabled by action initiation.

Product disclosure obligation

Product disclosure statements set out information about a product's key features – such as fees, commissions, benefits, risks and the complaints handling procedure – and can be important in assisting the consumer to fully understand the product they are signing up to. Generally, product disclosure can occur electronically. Where this is the case, product disclosure could readily be provided through digital channels as part of a streamlined switching process.

[42] Nguyen P & Solomon L, 2018, *Consumer Data and the Digital Economy*, Consumer Policy Research Centre, p. 49: https://cprc.org.au/publications/report-consumer-data-and-the-digital-economy/

There may be cases where regulatory requirements pose barriers to this occurring electronically in a smooth manner.[43] Explicit informed consent (EIC) requirements in the energy sector, for example, are more onerous than provision of key information about a product. As part of detailed EIC requirements the new retailer is required to ensure the customer receives full and transparent disclosure of the product, including being provided the opportunity to ask questions.[44] Some amendments to product disclosure requirements may be necessary, depending on the sector, for consumers to be able to use the CDR for switching.

Providers must process applications, including undertaking regulatory compliance activities

Providers' assessments of applications may be assisted and expedited by CDR assisted analytics. For example, banks may conduct creditworthiness assessments or verify income or expenditure (using information and analysis sourced from to credit bureaux). In addition, banks must comply with applicable lending standards as part of their loan approval processes. Providers may determine pricing on a per customer basis, such as where a bank's decision to offer a consumer a particular interest rate, including whether to offer a discounted rate, is informed by analysis of their financial history, current financial position and an assessment of their future repayment capacity. If these assessments are to use CDR data they currently are unable to be undertaken by non-accredited parties. Expanding the breadth of entities who can participate in data sharing could enable further CDR-driven services. This is discussed in Chapter 6.

Providers may require identity verification of prospective customers

Providers may require customer identity verification to meet regulatory requirements or for commercial reasons. Identity verification of new customers still tends to rely on paper-based proof of identity. Wide adoption of digital identity solutions would assist quick, efficient and convenient switching.

Where identity verification is not required by regulation, and the level of identity assurance required may be relatively low, solutions may be readily available to enable streamlined switching through exclusively digital channels.

Notably *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) compliance obligations pose an impediment to streamlined switching, including switching enabled by CDR. Current legislative safeguards under the AML/CTF Act require banks to verify the identity of their customers before a new account can be established and activated.

[43] For example, the *National Consumer Credit Protection Act* 2009 and the associated regulations facilitate a wide range of interactions involving consumer credit, including certain disclosures, to occur electronically. However, communications are required to be provided physically in relation to a limited number of especially serious matters.

[44] Under EIC obligations energy retailers must also ensure that consent is voluntarily given, free from pressure or duress, and that the customer has the capacity to provide consent.

Making any funds transfers to new providers or payment of outstanding amounts with previous providers

In banking, a bank customer (or a person authorised to act on the account) would need to organise any funds transfers or payments necessary to effect a switch between banks. With action initiation the customer could give an accredited person (which could also be their new bank) authority to manage and make these payments on their behalf.[45]

Transferring across direct debits and scheduled payments

When shifting between bank accounts, a customer may need to transfer direct debits or scheduled payments from an existing account to a new one.[46] Having to individually cancel and re-establish direct debits or scheduled payments can be a significant disincentive to switching accounts or providers. The CDR currently enables accredited persons to access information on existing direct debits and scheduled payments, which would assist them in their transfer upon switching.

CDR action initiation may provide a channel for re-establishing scheduled payments and direct debits with a new provider.

Transferring data across from the old provider

When switching accounts, it can be useful for the customer to transfer across their data, including personal information and service history, directly to their new provider. For example, a person switching electricity providers may want to import all of their contact details and existing bill payment arrangements to their new electricity retailer. It may also be useful in banking when a person wishes all their transaction histories to be transferred to their new bank so they can still access these records through their banking portal.

Currently, if the relevant sector is designated an accredited person could access this data from the consumer's existing provider. However, that accredited person could not transfer it to a new provider unless the new provider was also an accredited person.[47] More consumer control over sharing their data with their service providers could improve the functionality of the CDR and is discussed in Chapter 6.

Closing old accounts

When a customer acquires a new product they may or may not close existing accounts. Action initiation would enable this to be managed on the customer's behalf which would facilitate switching.

[45] The importance of this to enabling switching was noted in the American Express submission, p. 2.
[46] A direct debit is a pre-authorised transfer of money from one account to another. Scheduled payments are payments set up to be paid to another account automatically on a future date. See Chapter 5 for further discussion.
[47] Although, there are mechanisms for banks, with the consumer's consent, to then hold it pursuant to ordinary banking requirements regarding banking data rather than continuing to hold it under the CDR regime.

Sector-specific obstacles to switching

In some cases, there will be specific sectoral or product requirements that present obstacles to streamlined switching. Some may be able to be addressed through the CDR. Some may be capable of being addressed through sector-specific reforms while others may warrant retention for sound policy reasons.

As an example, a major obstacle to switching for some products in the banking sector is the need to create a new security interest or effect transfers of real and personal property security interests when switching between secured lending products. However it is not suggested that this requirement be altered to fit in with the CDR.

In the energy sector, depending on the state or territory, it can take up to three months to functionally switch energy providers as the old energy provider is required to get an accurate reading before they terminate an account, and meter readings generally occur at the end of the 90 day billing cycle. In certain circumstances it may be necessary to have a meter read before switching providers and a consumer may incur an exit fee or a special meter reading charge.

Fees and charges can also present another disincentive to switch as savings from switching would need to cover that cost and still present ongoing cost savings.

The Inquiry accepts that, while the CDR offers a significant streamlining of switching for consumers in most sectors, there is a range of sector-specific requirements that will continue to be friction points where consumers or accredited persons would be required to move off the CDR infrastructure to complete a switch. The sectoral assessment process can be used to identify such friction points and can provide sector-specific CDR responses or identify legislative or regulatory reforms where necessary. Consultation with both industry and sectoral regulators would be important in this process.

Expanded data sharing to assist in removing barriers to engagement

A range of practical barriers that consumers must navigate in order to change their circumstances can act as disincentives to engage or take action. Several of these can be addressed by expansion of CDR data sharing.

Identifying all the relevant offerings in the market

It can be difficult to identify which product among the many on offer best suits the needs and individual circumstances of a consumer looking for the right product. As an example, the comparator website Canstar approximates that there are over 4,000 mortgage products on the market for consumers to choose between.[48]

[48] Canstar website, Home loans, https://www.canstar.com.au/home-loans/ (accessed 19 June 2020).

CDR data sharing provides a mechanism to make the task of comparison and product identification easier, however, PRD information provided through the CDR may not include all the data a consumer considers relevant for comparison purposes. This could result from:

- non-transparent pricing practices[49]
- complexity of plans and their terms and conditions
- product bundling
- the availability of potentially relevant data from other sources (for example, CHOICE, star ratings, customer reviews), and
- possible technical difficulties in mandating relevant data (for example, if that data set is not kept by all data holders).

Furthermore, some PRD data can be quite complex and different at a granular level which makes it difficult to be standardised in a way that an API can compare.

Additionally, what consumers view as benefits or incentives to change services may include factors not strictly considered PRD for the purposes of the CDR. Consumers do not make decisions on price alone and consider other factors such as reward point programs,[50] or a reputation for customer service.[51] The ease of accessing and interacting with a bank may also influence a consumer's decision; for example, the quality of a bank's mobile app, or the availability of a physical or local branch presence and ATMs.[52] These factors can all influence decisions about which provider or product to use. All these factors sit outside of the PRD and the data fields currently included in the CDR for banking, however, additional CDR data fields may be included in PRD in consultation between industry and the DSB.

Transparency of pricing and the practice of 'discounting'

An obstacle to consumers identifying relevant offerings in the banking sector is the practice of 'discounting' mortgages where discretionary discounts are offered to customers after they are assessed for a loan, based on criteria that vary across lenders and over time. The criteria for discretionary discounts is not disclosed to borrowers or made public. The vast majority of borrowers pay substantially less than the relevant headline interest rates.[53]

[49] See discussion of the practice of discounting.
[50] Discussed in the RBA Research Discussion Paper 2018-11 (October 2018): Doyle M-A, 2018, *Consumer credit card choice: costs, benefits and behavioural biases*, RBA.
[51] Customer service has proved to be a point of differentiation in advertising NBN plans in the telecommunications sector.
[52] Branch and ATM locations are included in the UK Open Banking Standard: https://openbankinguk.github.io/opendata-api-docs-pub/v2.4.0/#branch-locator (accessed 19 June 2020).
[53] ACCC, 2018, *Residential Mortgage Price Inquiry final report*, p. 7.

In its Residential Mortgage Price Inquiry Report the ACCC found that headline interest rates advertised by and used by the five major banks to attract residential mortgage borrowers were poor indicators of the interest rate borrowers actually pay.[54]

The ACCC found this lack of transparency in discretionary discounts made it unnecessarily difficult and more costly for borrowers to discover the best price offers. The practice adversely impacted borrowers' willingness to shop around, either for a new residential mortgage or when they are contemplating switching their existing residential mortgage to another lender.[55]

This finding has been reinforced in the ACCC Home Loan Price Inquiry Interim report (the Interim Report). The Interim Report observed that the banks' preference appears to be to increase discounts, rather than reduce headline variable rates, because increasing discounts, in particular discretionary discounts, allows the banks to compete for new loans without needing to extend the reduction in price to all other existing home loan customers.[56] Importantly, the ACCC found that the effectiveness of such a strategy relies on inertia from a large proportion of a bank's customers and that '… banks' profits would be negatively impacted if a sufficiently large number of customers with existing loans demand increased discounts similar to those available on new loans, or switch to another lender to benefit from the larger discounts that may not otherwise be available on existing loans.'[57]

The Interim Report also notes the role of the CDR in improving consumers' ability to compare and switch between home loan products and lenders.[58] The ACCC has indicated that it intends to address switching issues in detail in its final Home Loan Price Inquiry report, due to be presented to the Treasurer by 30 November 2020.

The Inquiry notes that the CDR assists by enabling accredited persons to access information on the actual rates and fees charged by the existing provider to the consumer, with their consent.

Analysis of pros and cons of the offerings

One of the key objectives of the CDR is to remove the complexity and time required to analyse the advantages or disadvantages of the myriad products and services available in the banking and other sectors.

Navigating bundles

Many sectors offer bundled offerings, combining several products and offering some form of incentive to consumers to purchase more services from the same provider. In banking, bundles often involve linked and lower interest rates, and in telecommunications home broadband plans can

[54] ACCC, 2018, *Residential Mortgage Price Inquiry final report*, p. 3.
[55] ACCC, 2018, *Residential Mortgage Price Inquiry final report*, p. 3.
[56] ACCC, 2020, *Home Loan Price Inquiry interim report*, p. 62.
[57] ACCC, 2020, *Home Loan Price Inquiry interim report*, p. 62.
[58] ACCC, 2020, *Home Loan Price Inquiry interim report*, p. 9.

include reduced rates on mobile plans. The Inquiry notes that several providers already offer bundled energy and internet services.[59]

Bundling can offer competitive pricing and convenience for consumers. It can also act as a disincentive for consumers to change any of the individual services in that bundle due to the complexity of calculating costs and potential service disruptions from cancelling or 'unpicking' the bundle.

At present, the CDR only supports APIs for standalone products and comparison of bundles cannot be undertaken.[60] It is anticipated that the CDR will increasingly need to be applied to bundled services within sectors and as bundling services expand across sectors presenting new and attractive competitive offerings to consumers.

Recommendation 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.

Quality of comparison services

Many consumers turn to third parties to assist them in identifying appropriate products. These can include a range of third parties, however, the most visible are comparison websites and brokers.

There have been concerns across a number of sectors in which price comparison services operate regarding the incentives of these businesses. Chapter 7 contains further discussion regarding comparison services.

Non-accredited person advisers cannot access data

At the moment only those entities that have undertaken the accreditation process in the Rules can be granted access to a consumer's data. This impacts trusted advisers who may provide advice to a consumer on switching to new products (for example, accountants, financial advisers or financial counsellors). Chapter 6 of this report examines this issue in greater detail.

Action initiation will be a decision-enabler for consumers interested in identifying and moving to new products and services. Introducing action initiation and expanding data sharing will provide the regime greater capability to deliver data driven services and their benefits to consumers.

[59] Dodo is an internet service provider now offering to bundle NBN internet plans with electricity and gas https://www.dodo.com/bundle and Origin, best known as an energy provider is now offering bundles with NBN internet services. https://www.originenergy.com.au/internet.html

[60] Whether or not a product appears in a bundle is recorded in that product's PRD and bundled products can be identified by APIs in this manner, however comparison of bundles is not yet possible.

Chapter 4: Action initiation framework

A key focus of the Inquiry is how the CDR could be expanded to enable third party action initiation. This chapter identifies how the CDR could be used for this purpose.

Action initiation through the Consumer Data Right

The previous chapter outlined why action initiation is complementary to data sharing in enabling services to help consumers overcome barriers to decision making and participation. This chapter outlines how the processes and infrastructure created to facilitate CDR data sharing could also enable third party action initiation. It also describes what refinements need to be made to the CDR framework for this to be possible.

What is required for action initiation?

To enable a safe and trusted system of economy-wide action initiation, a number of important elements are required. These include:

- A secure communication channel is necessary for ensuring the integrity of any information sent or received.
- A common set of standards is required to enable action initiation requests to be interpreted correctly by a service provider, allowing an interoperable and competitive system to develop.
- A system of accreditation is necessary to provide those receiving instructions with confidence about the legitimacy of the initiator of the request and to ensure adequate protection for consumers.
- Processes for enabling consumers to provide direction and authorisation are needed for the system to operate for the consumers' benefit.
- A clear governance and liability framework would ensure, to the extent possible, that risks are appropriately assigned between participants in the system.

Without these elements, an economy-wide action initiation system would be incomplete.

Why should action initiation be pursued in the Consumer Data Right?

The infrastructure created to enable CDR data sharing arrangements also provides all of the underlying elements required for action initiation. The CDR already includes the following features:

- a secure process for sending encrypted data requests and information between participants
- a process for standardising the format of data requests and responses
- an accreditation regime to regulate those who can send instructions to receive data
- the foundational requirement for consumer consent and authorisation for data sharing to occur, and

- a clear set of legislative boundaries as to what is and is not permissible, including security and privacy protections.

A framework of high-level requirements that could be adapted to enable economy-wide action initiation are therefore provided for, in the context of data sharing, by existing CDR infrastructure. In enabling third party action initiation, it would be more efficient to extend existing digital infrastructure than to create an entirely new system.

There would be additional advantages to leveraging the CDR system after it has become known and trusted by consumers. As stated in Chapter 3, the success of any potential action initiation regime is heavily linked to consumer trust. Leveraging consumer trust in an existing scheme would likely have more success than introducing an entirely new system. However, consumer trust in the CDR will be closely linked to the successful commencement and operation of data sharing. As the Insurance Council of Australia stated:

> *The fundamental findings of the Review of Open Banking report remain relevant in order that customers can feel confident that their data is secure and it is only being used for the purpose for which consent is given under the current 'read' access. It may take some time before customers start feeling comfortable with third parties acting on their behalf and with an extension to 'write' access.*[61]

In light of this, action initiation commencement should be appropriately staggered to allow consumer trust in the regime to grow.

Recommendation 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.

Framework for action initiation

Legislative framework

The CDR regime has a layered regulatory framework. This design was conceptualised in the Open Banking Review and allocates powers and responsibilities between legislation, the Rules and Standards. This allows the CDR to be agile and responsive by enabling the Minister, CDR rule maker and Data Standards Chair to make decisions and implement changes through the Rules and Standards, while enshrining key concepts and protections in the CCA.

To enable action initiation through the CDR, the CCA will need to be amended to provide a firm legal basis for the expansion of the CDR. In drafting these amendments, consideration should be given to how different powers and responsibilities should be delegated to the Rules and Standards to allow

[61] Insurance Council of Australia submission, p. 2.

the CDR regime to remain effective and agile. The Inquiry finds that a similar distribution to the current system would be appropriate.

Box 4.1 – Structure of Consumer Data Right powers

Legislation – The legislation sets out the CDR framework and builds key protections into the regime, including the sector designation process and Privacy Safeguards. CDR provisions set through legislation require Parliamentary approval to change.

Rules – The Rules outline many of the functional requirements for the CDR. These Rules are set by the rule maker, with the consent of the Minister. As the Rules can be more easily amended than legislation, they allow for solutions to be developed iteratively and CDR functionality to be expanded gradually.

Standards – The Standards detail the technical specifications required to engage with the CDR and are set by the Data Standards Chair. As ministerial approval is not required to amend the Standards, they are able to promptly make amendments to solve important technical issues.

Designation process

A key element of the legislation will also be requirements surrounding the designation of action initiation in different sectors.

The CDR designation framework[62] empowers the Minister to designate a sector of the economy as subject to the CDR for data sharing, by specifying:

- the classes of information ('designated information')
- the persons holding the designated information[63]
- the earliest day applicable for beginning to hold designated information
- any classes of designated information for which a fee can be charged, and
- the sectoral gateway or gateways, if applicable.[64]

This same designation framework should be adapted to enable the introduction of action initiation. Alongside designated information, the Minister should also be made able to consider specific classes of actions that should be subject to the CDR, as well as the persons within this sector who should be required or allowed to carry out these actions if instructed through the CDR. Although the same persons required to share designated information may also be required to receive instructions to perform designated actions, these requirements should be considered separately. Consideration

[62] Subdivision B of Division 1 of Part IVD of the CCA.
[63] Under paragraph 56AC(2)(b) the designation instrument may specify the persons who hold one or more specified classes of designated information, or on whose behalf such information is held.
[64] Subsection 56AC(2) of the CCA – an entity through which communications to and from data holders must pass.

should also be given to whether a fee should be chargeable by the designated person for the initiation of some actions.

The Inquiry recommends that the Minister should have expanded powers to designate actions within sectors as being subject to CDR action initiation. When designating a sector, the Minister should be able to determine whether to designate data sharing, action initiation or both, and should be able to vary previous designations to expand or narrow their scope and application. There should also be provisions that allow designated information and actions to be phased in gradually.

Recommendation 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.

Sectoral assessment

The CDR designation framework currently outlines the processes that must take place prior to the designation of a sector. The first requirement is that a sectoral assessment be conducted to inform the Minister of the expected impact of designating a sector.[65] This process is intended to determine whether there would be benefits in requiring certain data sets to be shared, and to determine whether designating this information would impose unreasonable costs on data holders. Specifically, this process must consider:

- the interests of consumers
- the efficiency of relevant markets
- the privacy or confidentiality of consumers' information
- the impact on promoting competition
- the impact on promoting data-driven innovation
- any intellectual property in the information to be covered by the designation, and
- the public interest.[66]

The assessment must also consider a range of other requirements, including the likely regulatory impact of allowing the Rules to impose requirements relating to the information covered by the instrument.[67]

[65] Sections 56AE and 56AG of the CCA.
[66] Paragraph 56AD(1)(a) of the CCA.
[67] Sections 56AD and 56AE of the CCA: The Minister and assessment must also consider the regulatory impact of allowing consumer data Rules to impose requirements, whether those requirements would amount to an

The OAIC is also required to conduct a separate assessment of the potential privacy implications of designating the sector. In this assessment, the OAIC must analyse the likely effect of designating the sector on the privacy or confidentiality of consumers' information. The OAIC then reports to the Minister about that analysis.[68]

Before deciding that action initiation under the CDR be applied in a sector, the Minister should also consider the benefits and costs of designating specific classes of action within the sector. A modified version of the existing criteria in the CCA would capture the same considerations that should be consulted on before designating classes of action within a sector. This should include the consultation of relevant regulators of a sector with ongoing coordination as required.

As with designating a sector to be subject to CDR data sharing requirements, the 'digital maturity' of the sector should be considered. In this context, digital maturity refers to the sophistication of the digital infrastructure already in place within the sector, including the ability for data holders in the sector to digitally authenticate their customers. These considerations have greater importance when considering action initiation due to the range and complexity of actions that may be undertaken, as well as the greater potential for harm from any wrongdoing.

Within many sectors not all providers are equally digitally mature in terms of their ability to engage or transact with customers online. For instance, some providers may operate exclusively online, while others may require consumers to phone their provider to initiate an action. Uneven digital capabilities will impact the costs for different providers to enable action initiation. This could potentially lead to some market participants within a sector being able to more quickly and cheaply implement and take full advantage of action initiation.

The OAIC should be required to separately assess the privacy and confidentiality implications of designating different action classes within the sector.

In addition to considering the likely regulatory impact, the Inquiry recommends that sectoral assessments identify and assess any potential regulatory barriers to enabling action initiation from occurring in a safe, efficient and effective manner. This will assist the Government in identifying regulatory reform needed to enable the CDR to facilitate action initiation in that particular sector. Such regulatory barriers could be at the federal, state or territory level.

acquisition of property, existing fees charged for that information, the impact on the incentives to hold and manage that information, the marginal cost of disclosures of that information, whether any gateways need to be specified and any other matters they consider relevant. The Minister must also consult any person or body prescribed by the regulations, and consult the Australian Information Commissioner on the likely effect of the designation on the privacy or confidentiality of consumers' information.

[68] Section 56AF of the CCA.

Recommendation 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.

Coordination between the Consumer Data Right regime and sector-specific regulation

The sectoral assessment process should identify friction points where change is required to integrate data-driven services provided through the CDR with the existing arrangements in a sector. It is anticipated revision may be required to some regulatory frameworks to ensure that the potential benefits that could be achieved through the CDR are not hindered by existing regulation. Where possible, this should be facilitated by policy agencies and regulators working to integrate the CDR with existing frameworks to find consumer focussed solutions. Depending on the nature of the regulation, solutions may be identified through the CDR designation process, or through review and amendment of the regulatory arrangements in the relevant sector.

Within the banking and energy sectors there are currently regulatory processes which would limit the scope of the CDR to enable action initiation. An example of how these barriers are being negotiated within the energy sector is outlined below.[69]

Explicit informed consent requirements in the energy sector

Prior to the energy sector's designation, the ACCC and the Australian Energy Market Commission (AEMC) considered issues with the explicit informed consent (EIC) requirements under the National Energy Retail Law (NERL) and its impact on switching. EIC's capacity to limit action initiation in the CDR for the energy sector was also raised as an issue in several submissions to the Inquiry.[70]

The National Energy Market (NEM), in which Australian Capital Territory, New South Wales, Queensland, South Australia, Tasmania and Victoria participate, provides a regulatory framework for participating jurisdictions, although regulatory requirements may still differ between jurisdictions. In the absence of a truly national framework, barriers to action initiation and switching in energy may need to be considered on a state or territory basis.

[69] Barriers specific to the banking and payments sectors are discussed in detail in Chapter 5.
[70] Energy Australia submission, p. 5, Red Energy submission, p. 2, and AGL submission, p. 13.

For consumers in the NEM states, the obligation on retailers to obtain EIC in writing, verbally or electronically before transferring a consumer from another retailer or entering into a market retail contract has been identified as a barrier to switching.[71] In its Retail Electricity Pricing Inquiry the ACCC identified that while EIC plays an important role in ensuring that consumers are not switched inadvertently, there is no ability under the NERL or the Victorian Energy Retail Code for third parties to give EIC on behalf of consumers.[72] The consumer must communicate EIC directly to the retailer or their agent. There is a range of existing switching services on the market currently which populate switching applications for consumers and require the customer to provide EIC to the retailer to complete the switch.

The ACCC recommended regulation be changed to clarify the EIC provisions to make clear that consumers can provide their consent to third party intermediaries to give EIC on their behalf. The AEMC has indicated that the most valuable development CDR could bring to the energy sector is action initiation[73] and has committed to work with all agencies with responsibility for CDR to develop CDR in the energy sector.[74] It has additionally committed to developing a proposal to change EIC requirements and allow third parties to provide a consumer's consent to switch services in the energy sector, should action initiation in the CDR not progress.[75]

The Inquiry notes that core changes to the EIC requirements are needed to enable streamlined switching through the CDR channel and is supportive of changes.

Recommendation 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.

[71] This obligation is outlined in both the NERL and the Victorian Energy Retail Code.
[72] ACCC, 2018, *Retail Electricity Pricing Inquiry final report*, p. 285.
[73] Australian Energy Market Commission submission, p. 1.
[74] AEMC, 2020, *Retail Energy Competition Review,* p. x.
[75] AEMC, 2020, *Retail Energy Competition Review*, p. x.

Figure 4.1 Sarah's new home

Sarah is moving out of home for the first time and needs to update her address information. Sarah is dreading needing to wade through all of the separate sites she would need to go through to individually update her address with her banks, mobile phone provider, superannuation fund and who knows who else she's forgotten.

Rather than separately trying to coordinate this process, Sarah decides to use 'UpDets', an app powered by the CDR that offers to help handle this for her. Sarah creates an account with UpDets and gives it permission to send instructions through the CDR to her service providers to update her address. Sarah then enters her new address into UpDets and looks through the list of service providers to find the ones she would like UpDets to contact. (GovAgency! Sarah always forgets about them.) After this, Sarah's providers come to her! Each of the providers Sarah asked UpDets to contact comes back to her to confirm that she has authorised UpDets to request a change to her address and asks her to check the request to make sure all of the details are correct. Once Sarah confirms with each of these providers, the task is done! A process that would have otherwise taken Sarah hours is now solved in minutes, leaving Sarah more time to decorate her new home!

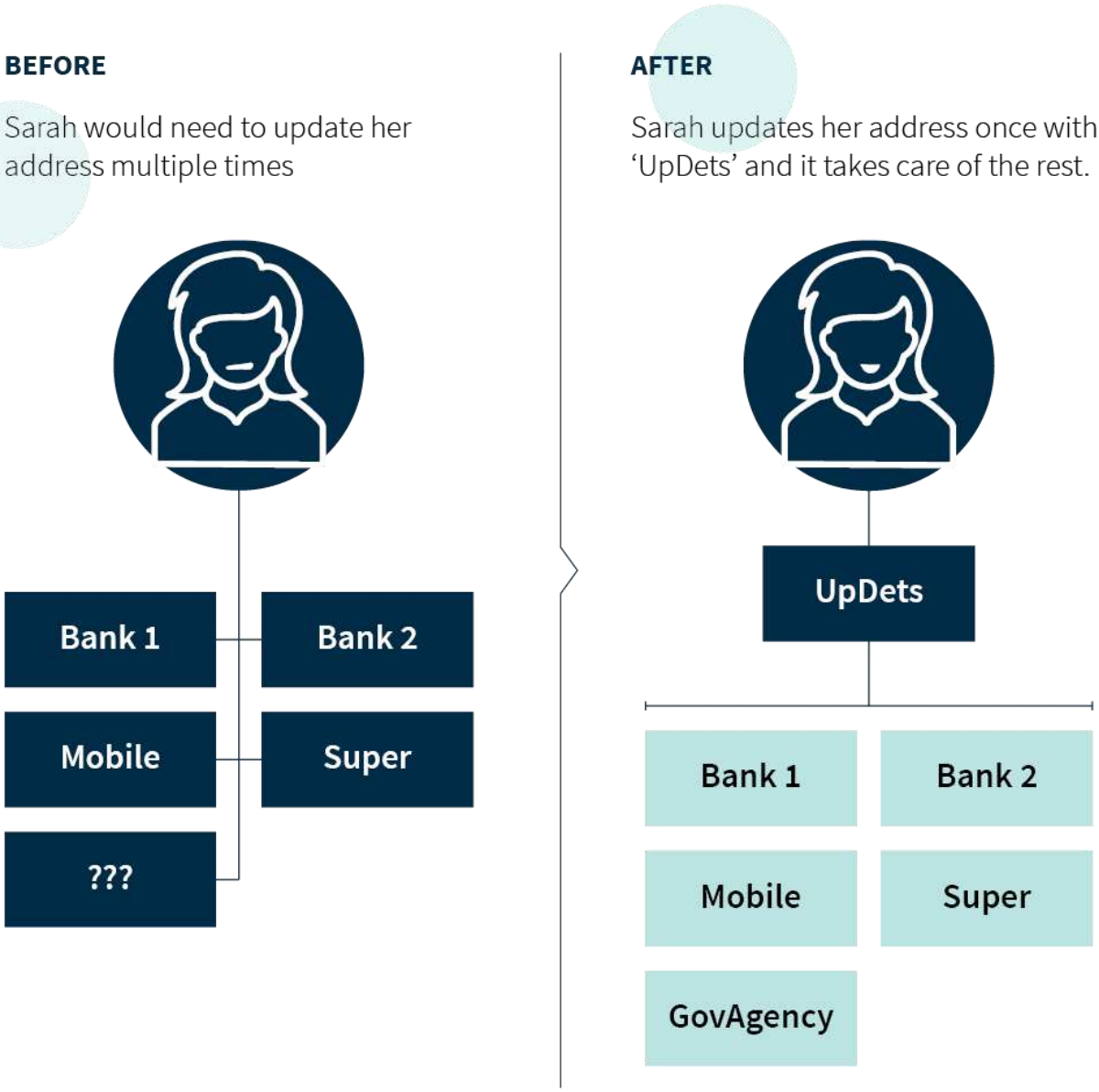
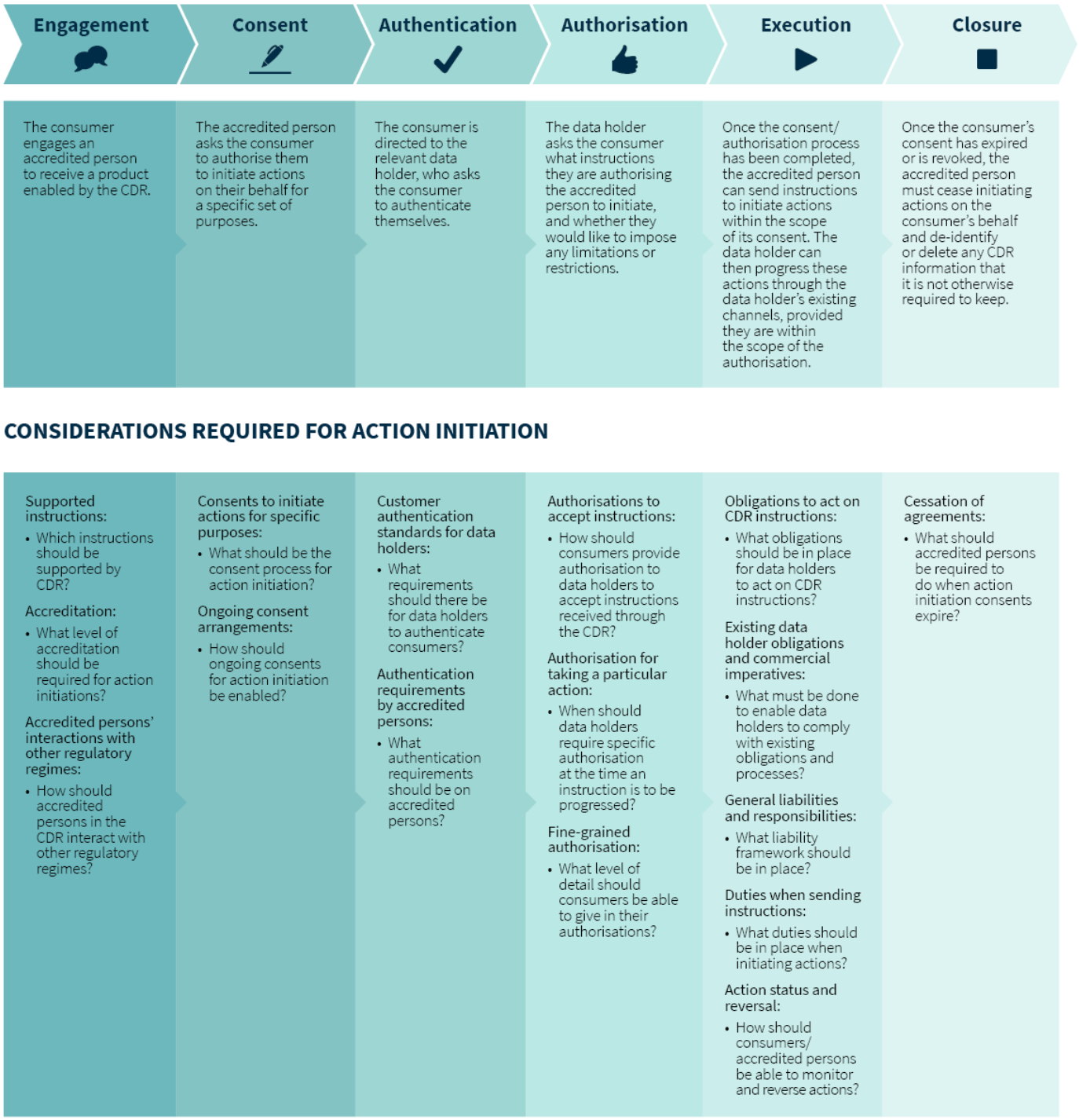


Figure 4.2 Consumer Data Right — Action initiation flow



Action initiation process

The flow diagram outlines the process for a consumer when engaging an accredited person to initiate actions with a data holder on their behalf through the CDR. The process for action initiation should be consistent with the process for data sharing. Accredited persons acting with the consumer's consent should be able to send instructions via the CDR to designated service providers who, after receiving the consumer's authorisation, should be obliged to progress these actions as though they had been received from the consumer. Questions outlined in the diagram about enabling action initiation to be introduced into the existing data sharing consent process are addressed below.

Recommendation 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.

Engagement

Supported instructions

The first points to consider when introducing action initiation in a sector are which classes of actions should be designated, and which data holders should be obliged to accept instructions received through the CDR. This will determine the designated data holders and designated classes of actions.

CDR action initiation should enable an accredited person to do something which the consumer is already able to do, on the consumer's behalf. Action initiation, therefore, should not be used to force a data holder to perform an action which it does not otherwise offer, or which is prohibited under other regulation. This principle should help steer consideration of what actions should be designated for action initiation.

The benefits and risks of designating certain action classes in the context of the specific sector should be considered during sectoral assessment. Actions should also be prioritised within sectors, allowing those actions that are best suited to action initiation and most likely to drive consumer benefits to be delivered first.

Designated classes of actions and designated service providers should usually be determined during the same sectoral assessment process that identifies CDR data sets and data holders for data sharing. This should not preclude implementation in a sector being phased, with more complex functionality brought in after the basic system is established.

The CDR should allow both mandatory and voluntary actions to be initiated. Mandatory actions should be those which designated service providers are required to make available, while voluntary actions are those that a service provider may choose to enable.

Recommendation 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.

There are also some types of actions which should not be able to be permitted using action initiation, even with a consumer's consent, due to the security and privacy risks posed to the consumer. Such actions will likely vary among sectors, and therefore should be determined during the sectoral assessment and subsequent implementation phases. Due to the significant risk posed by enabling a third party to update information such as passwords, this should be explicitly excluded from being actionable through the CDR including as a voluntary data set.

Recommendation 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.

Though the types of actions able to be initiated through the CDR will depend on the specific sector, the Inquiry has identified a number of general classes of action that may be appropriate to designate. These classes of action generically relate to the customer relationship flow within the sector.

Table 4.1 – Potential supported actions

Customer relationship	Product or service	Communication
• Opening a customer relationship • Managing a customer relationship • Closing a customer relationship	• Applying for a product • Managing a product • Closing a product	• Notifications • Complaints

Establishing and managing a customer relationship

Establishing a customer relationship

When a consumer first engages with a service provider they are often asked to establish a 'customer relationship' to identify themselves. This allows the service provider to uniquely identify the customer within their system and enables them to establish arrangements to contact and authenticate the consumer during the period of the customer relationship.

The process of opening a customer relationship differs from most other actions which could be enabled by the CDR, as it would require the accredited person to send a CDR instruction to a data holder with whom the consumer does not have an existing relationship. In such situations, the data

holder will not be able to authenticate that the request has been consented to by the consumer in the same way that they would in data sharing and other action initiation where the parties have an established relationship. To accept that this request is credible, data holders may need to assure themselves of the identity of the consumer and that the request was legitimate.[76]

The level of identity assurance required will differ depending on the relationship that the consumer is entering into. As a basic example, this could be done simply through the provision of an email address that allows the consumer to be identified and contacted in future.[77] Such a relationship could be established entirely through the CDR. This involves minimal assurance of the actual identity of the consumer.

However, some sectors have stricter identification requirements for the creation of these relationships due to the importance of verifying the consumer's identity. The banking sector, for instance, has strict AML/CTF obligations. The process of establishing this relationship is significantly more stringent than most other relationships and, as such, additional steps will be required by the data holder to verify the identity of the consumer. The details required for identity assurance will differ depending on the data holder and potential products in question. It is expected that digital identity solutions will play a role in enabling this in future.[78]

The other limb of assurance is the data holder needing to be assured that the customer has authorised the accredited person to send instructions on their behalf. Data holders may accept different levels of proof depending on the circumstance. In some cases, an assertion by the accredited person that they have been authorised will suffice.[79] In others, the data holder may need to engage directly with the consumer to confirm they are authorised to accept instructions from an accredited person on the consumer's behalf. This may be required due to sectoral regulatory requirements. If there are no existing credentials issued to data holders relating to the prospective customer, this assurance may have to occur outside of CDR processes.

Though the processes and requirements for setting up a customer relationship differ by sector, the CDR should be a useful tool in supporting customers seeking to establish new relationships via accredited persons. The extent to which it would be appropriate for the CDR to assist in establishing a new relationship should be considered as part of the sectoral assessment process and subsequent implementation of the CDR within that sector.

Managing a customer relationship

Action initiation through the CDR could be used to facilitate the correction and maintenance of accurate customer-provided information in a customer relationship. Depending on the data maintained about the customer, the CDR could provide a method for a consumer to instruct third

[76] Customer authentication in the CDR is different to identity verification. Identity verification is the process of proving the identity of a person. Customer authentication is merely confirming that the person seeking to access services is the same customer who is linked to the service. This is discussed in more detail in Chapter 8.
[77] CDR supports anonymous and pseudonymous consumer engagement, unless the Rules otherwise provide.
[78] Digital identity is discussed further in Chapter 8.
[79] Particularly so, given that the accredited person would be subject to sanctions (including loss or restriction of accreditation) for breaches of sections 56BN and 56BO of the CCA (Misleading and deceptive conduct).

parties to update these details. This could extend from the altering of communication preferences, to the maintaining and correcting of personal information. TrueLayer raised this as a desirable feature of action initiation in their submission to the Inquiry.

> *We believe that write access should extend to the ability to change customer identification details, as it is in the interest of consumers to find efficient and secure ways for them to update their details if required. This is also especially important if the CDR expands write access into more use cases, such as account opening and closing, or switching. Where write access is used to change identifying details, we would recommend that changing such details requires additional consent and authentication from the customer, for example two factor authentication.*[80]

Other submissions were also cautious, identifying the significant privacy risks that may be associated with managing a customer relationship. The OAIC's submission stated:

> *[T]he expansion to write access may also raise new privacy and security implications, which will need to be appropriately addressed. In particular, as write access would allow third parties to modify a consumer's financial information, it may increase the motivation for unauthorised actors to target an accredited data recipient's information system.*[81]

The sensitivities of updating the same information also vary across sectors, including due to know your customer (KYC) obligations in place in certain sectors. On this, the Australian Banking Association stated in their submission:

> *The CDR should allow data holders to process any write access requests in line with their existing approach for such requests. Further, personally identifiable information should be excluded due to security, fraud, and privacy risks. In respect to personally identifiable information banks are legislatively obligated to fulfil Know You[r] Client obligations and Verification of Identity obligations. Write access will need to preclude third parties from access to these data elements.*[82]

Given the sensitivity of updating personal information, it is reasonable that data holders should be able to continue taking reasonable measures to mitigate these risks. Therefore, though uniform processes should be in place to allow action initiation to commence the updating of personal information, data holders should be able to continue using existing processes to confirm the correctness of these details where appropriate.[83]

---

[80] TrueLayer submission, p. 12.
[81] The Office of the Australian Information Commissioner submission, p. 3.
[82] Australian Banking Association submission, p. 13.
[83] A data holder may find that receiving authorisation to progress a specific change in details (rather than a broad authorisation to update details generally) is adequate assurance for them to progress an update. This is discussed more in the 'Authorisation for taking a specific action' section.

Due to the potential sensitivity and risks of allowing a third party to alter some customer information, it may also be appropriate to entirely exclude some classes of information from being updated by action initiation within a given sector. As such, detailed privacy impact analysis and information security analysis should occur before determining the scope of information that should be able to be updated through the CDR within a sector, and whether any additional arrangements should be put in place to protect consumers.

Information used to authenticate the consumer, such as passwords and mobile phone numbers, should represent one example of such information. These details should not be able to be modified by accredited persons even with the consumer's consent, due to the significant risks it would pose for identity theft. What information is used for authentication purposes varies across sectors, and as such this should be explicitly considered as part of a sectoral assessment.

Closing a customer relationship

The closure of a customer relationship could also be supported by action initiation through the CDR. Closing a customer relationship is distinct from closing a product. When a customer closes a product, a customer relationship could still exist, even though they may not be receiving any products or services at the time. The closing of a customer relationship would likely also require a customer to stop receiving all ongoing products and services being provided to them by the service provider.

As the relationship is the primary way to identify a customer, the process of closing a relationship may reasonably involve more steps and require the customer's confirmation that they understand the consequences of the action. However, the process to close a customer relationship through the CDR should be no more complex than the process for creating a customer relationship.

Product or service process

Applying for a product

The lodgement of a product application is an important action required for acquiring a new product or switching products.

A general action that may be appropriate to designate is the completing and submitting of applications. Though this action would allow accredited persons to contact a data holder on behalf of the consumer, the consumer may still be required to engage with the data holder to enter into any contracts. The filling of applications could also leverage current data sharing arrangements, whereby the accredited person uses information provided to them through the CDR to fill in details required to lodge applications on the consumer's behalf.

The steps involved in an application process differ between sectors and products. There are also terminology and informational requirements that are specific to a sector. For example, one or more of following steps may occur during a product application process depending on the sector:

- Quote – when specific details are provided to obtain the estimated price or benefit of a product
- Pre-approval – when initial details are provided ahead of a formal product application

- Validation – when certain details are checked for completeness prior to accepting an application
- Order – when the product specifications and quantity are confirmed or approved.

It may be appropriate to offer a status update request as a CDR action when there is a period between the receipt of an application and the product's delivery. When a product needs to be physically delivered or an application takes time to process, the ability for an accredited person to confirm the state of the process could also be of value to a consumer.

Action initiation in the CDR generally requires a data holder to receive authorisation to progress an action before it can be acted on. As discussed earlier, this is not likely to be possible when the action is establishing a new customer relationship, as the potential customer will be unknown to the data holder. As such, a verification process will instead be conducted to provide the data holder with some assurance of the customer's identity and assent to the instruction being given. As many customer relations are expected to be established contemporaneously to when applying for a product, consideration should also be given to how this can best be enabled through the CDR system.

Managing a product

The management of a product differs substantially across product and service types. The ability for a consumer to request that an accredited person alter a product through CDR enabled action initiation would allow easier and more convenient product management.

Digitally accessible products will have varied functionality that could be enabled through action initiation. As stated earlier, the starting point for assessing what functionality could be enabled through the CDR should be the functionality that is accessible to a customer through another channel, such as an online portal. For example, for many banking products, payment initiation would be a primary function. This is further explored in Chapter 5.

Closing a product

It could be convenient to consumers to be able to close a product through CDR action initiation. While a data holder may be incentivised to keep a product open, a customer should be able to send instructions and complete any other actions that are required to close a product through the CDR, and this process should be no more difficult than it is to open the product.

Communication

Notifications

A customer could benefit from being able to request a push notification service through the accredited person. For example, an accredited person could offer a service where it asks a consumer about their interests and then registers them to receive notifications from providers offering services that align with these interests. Such an action would likely be voluntary.

Complaints

A customer complaint general action could give consumers the ability to easily complain about a product or service. There are expected to be behavioural barriers to lodging complaints with data

holders and being able to send complaints through an accredited person may assist consumers in resolving potential issues. This action may also be voluntary.

Accreditation

Those seeking to initiate actions via the CDR should require accreditation. Action initiation accreditation should be tiered, with higher tiers of accreditation required where the accredited person seeks to initiate classes of action with greater potential for harm. The process to gain accreditation to initiate actions should be consistent with the process for accreditation to receive CDR data, though additional criteria for action initiation may be required to reflect the different safeguards necessary.[84] The Australian Banking Association stated in their submission:

> *The ABA supports a robust accreditation process and a tiered accreditation model that reflects the risk profiles associated with expanded read and write activities, without relaxing the existing obligations concerning security, privacy, and consumer consent. The primary consideration of the future CDR regime must be ensuring that consumer trust and confidence in the regime is not reduced through a weakening of the consumer protection mechanisms in the CDR framework.85*

The level of risk associated with an action depends on the action that is being initiated and the authorisation steps taken by the data holder before progressing the action. For instance, lodging a product application via an API is a low risk activity where the receiver is expected to separately assess the customer and application before being able to choose whether to action the application. An action initiation arrangement does not necessarily expose a consumer to greater risk than a data sharing arrangement.

In determining the potential for harm of different actions, a number of factors must be considered. The potential for harm of performing the 'same' action (for instance opening a customer relationship) may differ between sectors, this must be considered when determining the accreditation tiering required to perform that action in each sector. The risks associated with some actions may be mitigated through the introduction of additional restrictions, such as a maximum number of times that an accredited person could initiate a specific action on a consumer's behalf in a month. A full assessment of what requirements are necessary and proportionate for a given action, including information security and insurance requirements, should be conducted after a sector is designated.

Recommendation 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.

[84] Tiered accreditation is discussed in further detail in Chapter 6.
[85] Australian Banking Association submission, p. 11.

Accredited persons' interactions with other regulatory regimes

Though enabling action initiation through the CDR may make it easier for accredited persons to offer innovative services to consumers, it should not circumvent existing consumer protections and licensing requirements for these accredited persons. Accreditation under the CDR will not relieve an accredited person of the need to obtain any other licences they may be required to provide, for example, regulated services. Those intending to use the CDR to initiate actions should also consider the other non-CDR requirements and regulations that they will need to comply with for the services that they intend to offer.

A key example of this would be the need for those previously offering generic financial advice to understand whether the increased specificity and tailored nature of advice possible under the CDR would require them to hold an Australian Financial Services (AFS) licence. Similarly, consideration must be given to how AML/CTF laws may apply to those accredited persons seeking to initiate payments on the consumer's behalf.

Recommendation 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.

Consent – given to the accredited person

Consents to initiate actions for specific purposes

Similar to current CDR data sharing, action initiation made possible through the CDR should be enabled through a consent model, with accredited persons requiring a consumer's active, informed consent to initiate actions on their behalf. In action initiation, accredited persons should require the consumer's consent to initiate specific actions, and their explicit agreement regarding the purposes for which the accredited person is allowed to initiate these actions.[86] Action initiation consents should be voluntary, express, informed, purpose specific, time limited and easily withdrawn.

Consents to initiate actions should allow consumers to select the classes of action that the accredited person can initiate and the data holders to whom the accredited person can send instructions. For instance, a consumer could give an accredited person consent to initiate actions with their service provider for the designated action 'update personal details'. The consumer would then need to agree to the purposes for which the accredited person proposes to initiate these actions. The types of consents and authorisations used for action initiation in the CDR are summarised below, alongside their data sharing equivalents.

[86] As with consents given to ADRs in data sharing arrangements, these are distinct from authorisations given to data holders.

Table 4.2 – Equivalent data sharing and access initiation terminology

	Accredited Person		Data Holder
	Access Consents	Usage Consents	Authorisations
Data Sharing	Consents to collect CDR data	Consents to use data collected	Authorisation to disclose CDR data
Action Initiation	Consent to initiate CDR actions	Consent to purpose for which instructions may be sent	Authorisation to accept CDR instruction

Both an access consent and a usage consent are necessary for a consumer to engage an accredited person under the CDR. By separating these consents, the consumer is able to have greater control over how the accredited person is allowed to act, being able to add additional usage consents easily, as well as being able to revoke specific usage consents without necessarily terminating their entire arrangement.

Box 4.2 – Consents given to and revoked from an accredited person

Sim has signed up to a mobile provider that allows her to vary her call minutes and data amounts on a month-to-month basis. This mobile provider has also decided to voluntarily provide this service through CDR API. Rather than coordinate this herself, Sim subscribes to 'Tele-phorget-about-it' (TFAI), an accredited person who offers to coordinate this service for her. Sim provides TFAI, with an ongoing access consent to receive relevant data from her mobile provider for 6 months and to alter her plan once a month over this period. Sim also authorises her mobile provider to accept such instructions. Sim initially provides TFAI with a usage consent that allows them to edit her data amount each month.

Being happy with this service, Sim provides another usage consent to allow TFAI to also send instructions to edit her monthly call minutes. When 'Tele-me-something-I-don't-know', a competitor accredited person, offers Sim an even more convenient service, she revokes all of her consents with TFAI and terminates her arrangement with them. This prevents TFAI from initiating any further actions on her behalf.

Recommendation 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.

As with the consent process for data sharing under the CDR, the consent process for action initiation should be subject to the DSB's Consumer Experience (CX) Standards and Guidelines to ensure that

processes produce genuine consent in a convenient manner. A significant amount of research has informed the creation of the data sharing consent process to allow a process that is easy to understand and provides for high quality consents. It is also important that the consent process for action initiation provides consumers with an experience which allows them to provide informed, genuine consents. As such, the appropriateness of the Consumer Experience Standards and Guidelines should be reviewed in the context of action initiation.

Recommendation 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.

Ongoing consent arrangements

Consumers should be able to provide ongoing access and usage consents, allowing the accredited person to initiate actions on their behalf on an ongoing basis for the duration of the consent. The ongoing ability to initiate actions on behalf of a customer could have greater potential for harm than ongoing data sharing arrangements, depending on the nature of the instructions. Therefore action initiation should maintain the current limitations on consent and authorisation durations, including the maximum 12 month duration for consents and authorisations and the 90 day notification requirement.

Additional safeguards should also be considered where appropriate. These safeguards must balance the need for security with consumer experience. Requiring accredited persons to authenticate their customers and enabling specificity in authorisations to allow consumers to set additional requirements around what actions the data holder can accept could help to provide this balance.[87]

Recommendation 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.

Restrictions on unnecessary actions

Accredited persons should be limited to only requesting access consents to initiate actions that are directly relevant to the provision of a service to a consumer. This would mirror the current data minimisation principle in the Rules, a requirement under CDR data sharing restricting accredited persons to only collecting and using CDR data that is needed to provide goods or services to the CDR consumer. This means accredited persons cannot request access to CDR data sets that are not linked to the provision of a service. Moreover, any CDR data received which is either not relevant or no longer relevant to the provision of a service must be deleted or de-identified (according to the

[87] Specificity in authorisations is discussed later in this chapter, and authentication requirements by accredited persons are discussed in Chapter 8.

consumer's stated preference). This principle ingrains additional consumer safeguards into the regime by restricting the amount of data that the accredited person can access and hold.

A similar principle should be included for action initiation. Accredited persons should not be able to request access consents for actions which are not directly related to the provision of a service to the consumer. Allowing accredited persons to access actions that are not immediately relevant to their services would needlessly increase risks to consumers by reducing their oversight and control of how the accredited person can act on their behalf. Enabling accredited persons to request access to additional actions could also increase the potential harm to consumers should the accredited person act disreputably or be targeted by a malicious actor. Consistent with the data minimisation principle, this restriction should be incorporated in the Rules.

Recommendation 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.

Authentication

Customer authentication in the CDR provides data holders and accredited persons with sufficient confidence that they are dealing with the data holder's existing customer. This gives them some certainty that any consents or authorisations received are given by persons who are entitled to do so. This also enables them to restrict the availability of CDR driven services to those entitled to access them.

Customer authentication standards for data holders

The current authentication method required for data sharing by data holders is one-time password (OTP) authentication,[88] where a consumer is sent a password through a separate channel to enter into the data holder's customer interface.

OTP was a suitable method to adopt for Open Banking data sharing functions as it met the safety and customer experience needs required of a consumer data sharing system. It was also a method banking consumers were already familiar with as a system used by many banks. However, as the CDR expands, authentication requirements of both data holders and accredited persons must adapt and be proportionate to the risks that misuse of new data sets and functionality could pose to consumers. National Australia Bank (NAB) raised concerns about the adequacy of extending the current authentication process for data sharing to action initiation.

> *NAB believes that the current consent authorisation authentication requirements for the CDR would not provide sufficient security under write access. Currently, consent authorisation does not extend to the authorisation to act on a customer's behalf for use*

[88] Consumer Data Standards V1.5.1, Authentication Flows in the Security Profile.

cases such as payment initiation. If the consent authorisations were not enhanced, NAB believes that CDR activity would face a greater level of cyber security risk.[89]

What should serve as proportionate authentication is discussed in detail in Chapter 8.

Recommendation 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.

Authentication requirements by accredited persons

With the introduction of action initiation functionality, accredited persons may assume responsibility to act on the consumer's behalf in addition to having consents to access and use the consumer's data. Some classes of action initiation functionality can carry a greater risk of fraud or misuse of data which can expose the consumer to potential harm and the accredited person to greater potential liability.

Consequently, if an accredited person has an ongoing relationship with a consumer which enables the consumer to direct the accredited person to perform specific actions through the CDR, the accredited person should be required to have in place a safe and convenient means of authenticating the consumer as a means of managing risk.

Any authentication requirements for accredited persons should provide flexibility on the solutions used and should draw on international standards for assurance levels and rigour of authentication mechanisms.

Recommendation 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.

Authorisation – Given to data holder

Authorisation to accept instructions

To ensure the security of the CDR system in allowing third party action initiation, consumers should be required to give their data holder authorisation to accept instructions sent by an accredited person through the CDR before the data holder can progress the action. This is equivalent to the

[89] National Australia Bank submission, p. 8.

requirement that consumers give data holders authorisation to disclose CDR data to the requesting ADR in the current CDR data sharing arrangements. These authorisations should be readily withdrawable.

Authorisations to accept instructions should outline the classes of action that the CDR consumer is allowing to be progressed, but should not provide details about the purpose for which the consumer has engaged the accredited person.[90] This is consistent with authorisations under data sharing arrangements, where the data holder knows the data sets that the consumer has consented to be disclosed, but not the purpose for using the data sets. Mandating that data holders must be provided a consumer's usage consents without the consumer's explicit agreement would provide data holders with additional insights into the consumer. This would potentially impinge on the consumer's privacy and give the data holder a competitive advantage in seeking to retain the customer. It may be appropriate to enable consumers to voluntarily provide this information to their data holder if they wish.[91]

Authorisation for a taking a particular action

For some actions, data holders should be required to receive more specific authorisations to progress the execution of a particular action.[92] The specificity of the authorisation that the data holder is required to obtain from the consumer should depend on the nature of the action requested and other factors, such as the potential impact on the consumer and existing practices and processes in the sector. With higher risk actions, such as updating of personal details, it would likely be appropriate for the consumer to review and authorise that specific action being executed (rather than provide a broadly expressed authorisation to act on action initiation requests falling within particular bounds).

Though consumers should generally be able to provide data holders with ongoing authorisations, for actions where they are required to provide specific authorisations to the data holder to taking a specific action, these would likely need to be provided at the time the accredited person seeks to initiate an action. By requiring authorisation at the point of the request, the consumer would be made aware by the data holder of the action that has been requested, and is given the opportunity to assess whether it is in their interests at that point and therefore whether they should authorise it. It should be an opportunity for a data holder to confirm the consumer's understanding that the action has been requested, and not a chance to influence the consumer's decision.

Box 4.3 – Specificity of Authorisations

An action where it may be appropriate to require a specific authorisation, due to its sensitivity, could be the updating of a consumer's personal details. A number of submissions noted the sensitivity of enabling such information to be updated by a third party. For this example, it would also be appropriate for a consumer to need to authorise a specific change to this information, rather than generally allow this information to be changed. To enable the consumer to review

[90] These additional details are contained in the consent to initiate actions provided to the accredited person.
[91] This point is discussed in greater detail in the consent management section in Chapter 6.
[92] Rather than, for example, an ongoing authorisation for a class of actions.

the proposed change, this would require them to grant authorisation at the time the action initiation instruction was sent to the data holder. As noted previously, the sensitivity of particular personal information will vary depending on the sector in question, and so consideration should be given during the sectoral assessment to which information should be subject to this requirement.

Another action which could require a specific authorisation, due to its substantial impact on a consumer's relationship with their data holder, may be a request to open certain kinds of new products or close a consumer's product or relationship. A customer may need to provide a specific authorisation to accept applications for new products that could impose substantial obligations or risks on the consumer, such as a share trading account, but may be able to give ongoing authorisations to accept applications for lower risk products, such as savings accounts.

Recommendation 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.

Fine-grained authorisation

In instances where it is not necessary for the consumer to authorise the specific action itself, it may still be appropriate for consumers to be able to impose restrictions when authorising their data holder to accept action initiation instructions. For instance, this could include the ability for the consumers to impose a maximum limit on amounts for transactions initiated by accredited persons. This process, known as fine-grained authorisation, would enable consumers to have greater control over how accredited persons act on their behalf, embedding additional consumer protection measures into the regime. A data holder should be required not to progress any actions which lie outside the scope of the data holder's fine-grained authorisation.

Recommendation 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.

Execution

Obligations to act on instructions received through the Consumer Data Right

After receiving a consumer's authorisation to initiate actions in response to requests from a specific accredited person, data holders should be obliged to progress actions that fall within the parameters set by the consumer to the same extent as if the requests had been initiated by the consumer.

This is not the same as obliging the recipient of the instruction to always act on these requests.[93] For example, if a back could refuse to act on a payment instruction through another channel, such as in instances of suspected fraud or abuse, they should similarly be entitled to refuse to act on a similar instruction through the CDR channel.

This will enable ordinary commercial and regulatory considerations to apply without the CDR having to create a new framework for when actions can be refused.

However, data holders should not be able to discriminate against instructions sent to it through the CDR channel. For example, if a bank can act with discretion to not progress an action but only exercises this discretion in relation to the CDR channel, this should be a breach of their CDR obligations.

It should be in data holders' interests to not obstruct use of the CDR channels as:

- they will be obliged to invest in making the channel available for mandatory actions
- it will be possible for action initiation under the CDR to jointly benefit consumers and data holders, and
- the CDR will enable enhanced consumer experience, creating demand and support for the regime.

A data holder should be able to refuse to progress the requested action if it considers this necessary to prevent physical or financial harm or abuse, if it reasonably suspects that the request could threaten their information and communication technology systems, or in other circumstances laid out in the Standards. This is consistent with the exemptions in place for data holders who would otherwise be required to share CDR data.[94]

Data holders should only be required to progress actions that the data holder otherwise offers or supports through another channel. Data holders should not be required to facilitate entirely new actions.

Data holders should be able to choose to voluntarily make additional actions available to be initiated through the CDR.

[93] There may of course be circumstances where the law may compel a service provider to perform an act when instructed directly by the consumer.
[94] These circumstances are outlined in Division 4.2 of Part 1 of the Rules (Rule 4.7).

Recommendation 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.

Existing data holder legal obligations and commercial imperatives

Under the CDR, data holders will still need to abide by all existing legal obligations placed on them by other regulatory regimes. Action initiation through the CDR is not intended to change the regulatory requirements imposed on data holders, but is intended to provide another channel through which they can receive instructions.

Therefore, data holders must still be able to continue to fulfil these requirements, and measures may need to be built into the CDR to facilitate this. Such measures could include ensuring appropriate information is provided as part of instructions from the accredited person, or enabling additional authentication processes (step-up authentication) so the consumer can confirm the legitimacy of potentially suspicious requests. For example, data holders should still be able to monitor and mitigate the risk of fraud. As such, data holders must be able to continue to perform step-up authentication requests to mitigate against fraudulent actions being initiated through the CDR.

Data holders currently use a variety of techniques to confirm the validity of a requested action. Enabling action initiation by accredited persons may alter the way in which these traditional techniques are used, requiring the data holder to exercise greater diligence in assessing these requests. NAB raised this in their submission, stating:

> *NAB currently relies heavily on an in-depth understanding of the user and their device through tools embedded in the way that customers choose to interact with NAB (such as internet banking, mobile applications). This understanding determines the fraud and financial crime risk that a user possesses. If third-party providers can make applications on behalf of a consumer, financial institutions lose this ability. As a result, banks may need to be more conservative in approving applications lodged with Open Banking.*[95]

The way these processes are conducted should be commensurate to the risk associated with the action being requested, acknowledging that action initiation by third parties may increase the level of uncertainty around the legitimacy of specific action requests.

Providing additional information about when and how a customer has directed the accredited person to facilitate actions may assist data holders in performing this role. A customer should be able to share this information with their data holder if they choose.

[95] National Australia Bank submission, p. 8.

Recommendation 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.

General liability and responsibilities

To support the efficient and reliable operation of the CDR, the CCA protects data holders from liability when carrying out data sharing requests where the data holder has complied with the requirements of the CDR regime.[96]

The expansion of instructions in action initiation beyond data sharing means that the liability of the data holder needs examination. As the data holder is obliged to receive the instruction, the principle-based approach that underpins the current provisions should be extended to action initiation instructions. This will allow protection from liability to be applied to wider action initiation in a way that is consistent with the current arrangements in place for data sharing. Therefore, when an accredited person makes an action initiation request and the data holder receives and progresses this request in a way that is consistent with their requirements to do so under the CDR regime, the data holder should be protected from liability for doing so. If the customer suffers a loss for reasons other than the data holder complying with the requirements of the CDR, the CDR should not displace ordinary rules of liability and allocation of loss.

A data holder, in carrying out an instruction in good faith, continues to be subject to other regulatory obligations, such as compliance with AML/CTF sanctions screening obligations that would otherwise apply if the instruction had come directly from the customer.

Further discussion of how liabilities apply to payment initiation is included in Chapter 5.

Recommendation 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.

[96] Section 56GC of the CCA.

Duties when sending instructions

As discussed above, accredited persons should require the express consent of a customer to initiate actions on their behalf. This includes the sending of instructions and in respect to the purposes for which instructions can be sent. Additionally, when seeking consent to initiate actions, or initiating actions, on behalf of a consumer, accredited persons should be subject to specific obligations in carrying out those functions. As discussed in Chapter 7, at a minimum, accredited persons should be obliged to act efficiently, honestly and fairly in doing so.

This duty should only apply to exercising the power to initiate actions under the CDR on behalf of a consumer, and not more broadly to the entirety of the services being offered by the accredited person to that customer. To do this would place the CDR in the position of regulating goods or services merely because they were CDR enabled. This is the role of sectoral regulatory frameworks, including consumer laws. Regulation of this nature could result in a far more limited variety of products being available to consumers through the CDR compared to outside the system.[97]

Accredited persons are already bound by other legal obligations that prevent them from engaging in misleading, deceptive or unconscionable conduct and additional restrictions on the accredited person's usage of the CDR are already applied through the Rules.

Action status and reversals

Consideration must be given to how a consumer monitors actions initiated by an accredited person, and what safeguards there should be to allow consumers to reverse actions they did not intend to authorise. To allow consumers to track actions performed on their behalf, accredited persons should be required to record any actions they have initiated. This record should be available at the consumer's request. Additionally, there should be a requirement that accredited persons notify consumers when an action is initiated, similar to Privacy Safeguard 10.

The Inquiry acknowledges that it may not be possible for data holders to reverse some actions initiated through the CDR. For instance, if a consumer agrees to have their account closed with a specific data holder, it would not always be possible for the same account to be simply reopened. Other actions may similarly be difficult to reverse. The ability to reverse specific actions should be assessed through the sectoral assessment process.[98]

Positive frictions should be included in the consent and authorisation process to help prevent consumers accidentally enabling actions. As discussed, this should include the ability to give fine-grained authorisations, the ability for data holders to have step-up authentication, and the requirement for some actions to be specifically authorised at the time of action initiation.

[97] This is discussed further in Chapter 7.
[98] The ability to reverse payments along with other instructional functionality is discussed in Chapter 5.

Recommendation 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.

Closure

Cessation of agreements

Accredited persons should only have the ability to initiate actions on a consumer's behalf when they have a current consent from the consumer to do so. Once a consumer's consent expires or is revoked, the accredited person must cease initiating actions on the consumer's behalf through the CDR and delete or de-identify any CDR data that they received about the consumer.

Recommendation 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.

Additional considerations

Record keeping

When a consumer has engaged an accredited person to initiate actions on their behalf, the accredited person should be required to maintain ongoing records. These records should detail the actions they initiated, as well as the consents they had received from the consumer. These records should be able to be used during dispute resolution processes, by regulators or by the consumer themselves to determine whether the accredited person acted within the scope of their remit.

This record keeping requirement may result in the accredited person being required to keep CDR data beyond the duration of the consumer's consent. This should be permitted, as is the case with records kept for read access under the CDR. This would similarly apply where there is a legal obligation to retain records, such for certain income tax purposes.

Recommendation 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.

Dashboards

As with data sharing, accredited persons and data holders should be required to maintain consumer dashboards from which consumers can easily track and manage their action initiation consents and authorisations. Consumers should also be able to revoke or amend consents and authorisations provided to accredited persons and data holders from these dashboards, either revoking specific

usage consents, withdrawing access consent for specific actions, or withdrawing their consents all together.

Privacy safeguards

In enabling action initiation through the CDR, consideration must be given to the adequacy of current CDR protections provided through the privacy safeguards. This is discussed in detail in Chapter 7.

Consumer Data Right and the ability for an accredited person to contract on behalf of a consumer

The CDR regime provides a communication channel through which accredited persons can send instructions to data holders. The CDR also provides a means to establish that this communication is with the authority of the consumer.

The CDR is not designed to fulfil all legal requirements for a consumer to grant an accredited person permission to enter into contracts on their behalf. Ensuring any such requirements are met is the responsibility of any accredited person seeking to offer services to the consumer which require them to have authority to contract on the customer's behalf.

It is currently possible under a number of arrangements for a consumer to enter into an agreement with a business which allows the business to make financial decisions on the consumer's behalf. An investment manager, for example, may be able to buy and sell shares on behalf of the consumer without the consumer's ongoing participation in the process.

If an accredited person is (outside of the CDR regime) granted the right to contract on behalf of a consumer, the CDR may provide the means of communicating an assertion of that fact and other supporting information to other parties. For example, Tim agrees to ComparisonServiceX acting as his agent to enter into new internet service provider (ISP) contracts. This occurs outside the CDR. Tim then allows ComparisonServiceX to lodge product applications on his behalf through the CDR. He allows them to communicate as part of those applications that they are legally binding offers to enter into a service contract on his behalf. This occurs through the CDR channels. The prospective ISP may voluntarily choose to accept that assertion that ComparisonServiceX has the capacity to enter into contracts on Tim's behalf.[99]

Therefore, working together with existing legal frameworks, the CDR should support a range of services such as more streamlined or automated switching.

[99] In such a situation, the onus would be on the internet service provider as to how they wish to verify the consumer and confirm their agreement that the ADR was acting at their direction. This choice may be influenced by knowledge that the ADR may be subject to sanctions if they communicate false and misleading information through the CDR.

Box 4.4 – Streamlined switching versus automated switching

[The Inquiry notes that the EIC requirements in the Energy Sector may mean that the following examples are currently not possible, however such services may become possible in future.]

D'Arcy signed up to 'Energ-Easy', a fee-free energy switching service that is accredited to use the CDR. Energ-Easy promises to swap D'Arcy between energy accounts to save him money on his energy bill. D'Arcy gives Energ-Easy consent to access his energy data and send applications to energy companies to give him a better deal through the CDR. D'Arcy also gives his current energy provider authorisation to share his energy usage data with Energ-Easy.

Energ-Easy assesses D'Arcy's energy bill and finds him a cheaper deal. Energ-Easy presents D'Arcy with this information and then sends an application to the potential new provider. On receiving this application, the new provider approaches D'Arcy to verify his identity and confirm that he agrees to sign up to their deal. D'Arcy agrees and also gives consent and authorisation to Energ-Easy accessing energy data from this new provider, allowing them to continue providing their service.

D'Arcy later decides, on the recommendation of a friend, that he would rather try a different service. He goes to 'Best Energy Deals' (BED), a CDR accredited person who charges a yearly fee. BED promises to assess all market options through analyses of CDR product reference data and only recommend the best deal for their clients. Additionally, BED offers a legal arrangement where they can cancel and enter into contracts on their clients' behalf. This authority to contract on the customer's behalf is facilitated externally to their capacity as a CDR accredited person.

D'Arcy agrees to sign up with BED, and opts into their additional arrangement. He gives BED consent to receive energy usage data from his current provider and gives his current energy provider authorisation to share data with BED. BED then goes looking for deals. As BED has an arrangement that allows them to enter into new contracts on D'Arcy's behalf providers no longer approach D'Arcy directly to sign him up. Additionally, as BED is an accredited person, they can send applications via the CDR rather than via email as they would have otherwise have done. D'Arcy now only needs to periodically go to the BED portal to allow them to access energy data from his latest provider.

Chapter 5: Action initiation in the banking sector

The Inquiry has been asked to examine how action initiation could enable consumers to apply for and manage products, including initiating payments, in the banking sector through the CDR.

This chapter builds on the foundation of the action initiation framework in the previous chapter. It begins by examining the case for extending Open Banking to include action initiation. Then it outlines how payment initiation and non-payment action initiation in the banking sector – such as product applications and management – could be implemented through the CDR.

Extending Open Banking to include action initiation

What is 'payment initiation' and what is 'general action initiation'?

As discussed in Chapter 4, action initiation involves an accredited person sending instructions on behalf of a consumer to a data holder to perform actions. In the banking sector, the Inquiry distinguishes between instructions that are 'payment initiation' and 'general action initiation' as classes of actions.

Payment initiation refers to a payment instruction sent through the CDR that requests the transfer of money. General action initiation refers to all other non-payment initiation instructions. These may include applying for, managing and closing products. Examples of these which can be observed in the current functions a customer can initiate through a digital banking portal, include requesting an update to customer details, changing account settings on existing products and altering other preferences.

It is important that payment initiation is considered separately to general action initiation,[100] because payment instructions are facilitated through the existing payments system infrastructure. The inter-bank payment systems that connects up individual bank systems are subject to robust security and payment system specific standardised arrangements. In contrast, general action initiation instructions do not have sector-wide standards although there are common product features and proprietary standards developed for many products.

Assessment and designation for action initiation in the banking sector

Chapter 4 outlined how the sector assessment process should apply in new sectors where CDR action initiation is under consideration. In this section, the Inquiry examines the likely impacts of enabling both payment initiation and general action initiation in the banking sector.

[100] National Australia Bank submission, p. 7.

Interests of consumers

Action initiation functionality would build on and enhance benefits provided to banking consumers by the CDR. The ability for an accredited person to initiate actions on behalf of a consumer has the potential to improve consumer convenience and reduce the time and costs of interacting with service providers. Data sharing enables the customer to gain valuable insights from their banking data shared with an accredited person, but action initiation would enable the application of the insights to assist consumers in manage their finances.

The benefits of integrating payment initiation with data sharing have been observed overseas, primarily in the UK.[101] The examples below show the potential for innovative consumer solutions which include:

- an app that moves funds to optimise interest earnings among a consumer's bank accounts[102]
- a single aggregated view across accounts at different banks with the ability to manage those accounts including initiating payments, and
- a service to monitor cash flow and automate payments towards a savings or investment goal.[103]

The delivery of such benefits is dependent on appropriately managing the risk of unauthorised or unsuccessful payments, and maintaining trust in the integrity and efficacy of the payments system.

General action initiation could help overcome consumer 'stickiness' by making it easier to take the next step of applying for a banking product and switching to a new product.[104] An application programming interface (API) enabled approach could provide substantial benefits to consumers or, as Finder stated, enable consumers 'to turn their CDR data into real life savings.'[105] The Switching Journey in Chapter 3 shows how the CDR, with enhanced functionality, could assist in the process of switching to a better value home loan, including by:

- enabling easier product comparisons across the market, supported with product application capability, and
- providing support to switch accounts, including funds transfers, paying out account liabilities and closing accounts.

While the potential benefits are compelling, it is important to ensure that there are adequate safeguards to protect consumers from harm and financial abuse, particularly if action initiation has the potential to exacerbate existing problems.[106] There is encouraging evidence from UK Open Banking that uses beneficial to disadvantaged people will emerge. For example, use cases that support greater financial inclusion, support for legal aid and welfare support advice have been

[101] On 28 September 2020, UK Open Banking announced that it had reached two million customers: https://www.openbanking.org.uk/about-us/latest-news/real-demand-for-open-banking-as-user-numbers-grow-to-more-than-two-million/
[102] An example of this is included further below at Figure 5.1 – 'Cedric's finances'.
[103] Some of these examples are based on propositions in the Deloitte submission, p. 26.
[104] Switching using the CDR is discussed in further detail in Chapter 3.
[105] Finder submission, p. 1.
[106] Financial Rights Legal Centre submission, pp. 19-20.

developed.[107] Many potential use cases would require payment or general action initiation functionality.

Promoting competition

An important aim of Open Banking is encouraging competition in the banking sector. In its 2018 Inquiry into Competition in the Australian Financial System, the Productivity Commission found, '[t]he banks, and particularly the major banks, exhibit substantial pricing power. The major banks' market power has allowed them to set interest rates to borrowers and depositors that enable them to remain highly profitable – without significant loss of market share.'[108]

Payment initiation and general action initiation would further promote competition by enabling accredited persons to improve the quality and customer suitability of banking services. Accredited persons would provide competitive pressure to banks through enhanced customer experiences and greater responsiveness to customer needs. For example, increased competition could lead to better outcomes for customers by enabling more switching among higher margin products. As consumers become more mobile in search of better deals and savings, banks and non-bank competitors should respond with better services, new and improved product offerings and more competitive pricing. The accredited person would also be able to more efficiently deal with actions such as closing accounts and take actions based on pre-set parameters.

Efficiency of relevant markets

The CDR is designed to address market inefficiencies[109] by reducing information asymmetries through data sharing, overcoming behavioural biases to rational decision making and addressing practical difficulties that consumers face[110] by providing access to third party advice. The implementation of general action initiation to complement data sharing could provide consumers with a more effective price signal in banking product markets. While standardised data sharing can efficiently transfer information about banking products and customers, action initiation could reduce the transaction costs associated with switching products. For example, it could increase demand for lower interest rate loan products to apply pressure on incumbent providers to offer more competitive pricing.

The payment services market should become more efficient as third party payment initiation provides easier access to lower cost payment services and more convenient ways of managing bills and payments.[111] The use cases above show that payment initiation could save consumers time and money. Businesses could better manage their cash flows. Business running costs could be reduced by having more competitive payment services to choose from. New types of payment services could particularly assist small businesses with constrained resources to invest in their technological infrastructure. Business customers with the technological capacity could substantially benefit from

[107] United Kingdom's Financial Conduct Authority, *Call for Input: Open Finance*, December 2019, p. 8.
[108] Productivity Commission, 2018, *Competition in the Australian Financial System Inquiry Report*, p. 10.
[109] For example, a lack of price transparency in the home loan market can make it unnecessarily difficult to find the best price offers: ACCC, 2020, *Home Loan Price Inquiry interim report*, p. 9.
[110] For example, to deal with increased complexity and volumes in products and services.
[111] An example of this is included further below at Figure 5.1 – 'Cedric's finances'.

standardised APIs through the CDR as it would enable an end-to-end digitisation of the business banking relationship.[112]

Promoting data-driven innovation

Introducing payment initiation and general action initiation should encourage further innovation in payment and product acquisition processes. Payment initiation could enable accredited persons to provide payment services, such as merchant payments, that are more customer-focused using CDR data. It should allow the facilitation and management of payments while maintaining the safety and security consumers expect.

UK Open Banking has over 200 third party service providers (equivalent to accredited persons in CDR) providing a diverse range of services. About a quarter of these third party service providers are able to offer payment initiation services. Extending Open Banking to include action initiation would help expand the CDR data ecosystem with a greater range of innovative services. This should be supported by an increasing demand for specialised services assisting accredited persons in the value chain. For example, in Australia, it is notable that the first two accredited persons to join the CDR are using it to provide a personal finance management app and to streamline loan applications.

Privacy or confidentiality of consumers' information

The CDR has featured strong privacy and security protections to safeguard the interests of consumers. Action initiation has many potential benefits, but they are accompanied by risks. The information contained in an instruction to act could be sensitive – for example, product applications would contain personal information. In the case of payment initiation, it could contain personal information of other parties, including the person receiving the payment.

The payments industry has strong information security practices and strict requirements due to its critical core function of moving money. These include the security and proper use of data and personal information and contracts to meet industry standards.[113] However, the information security arrangements that apply to CDR participants would need to be reviewed for action initiation, and particularly for payment initiation.

To protect customers, enabling changes to a customer's information in general action initiation should, for example, attract stronger protections for personal information contained in consents, authorisations and instructions data.[114] Allowing such changes present heightened risk to customers through increased risk of harm or loss through cyber-attacks, identity theft or other fraudulent activities. The CDR regime would require robust regulatory settings to mitigate and manage these risks to have the confidence of CDR participants and consumers. A privacy impact assessment would be an important part of identifying privacy risks in detail in the broader context of action initiation.[115]

[112] Deloitte submission, p. 27.
[113] Cuscal submission, p. 4.
[114] If adequate protections cannot be put in place, certain data sets should be excluded.
[115] Privacy issues are addressed further in 'Privacy and information security safeguards' in Chapter 7.

Sector-specific and digital maturity issues

One of the most cited regulatory issues in submissions relating to the banking sector was the current settings of Know Your Customer (KYC) requirements under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). These are important customer identification and verification procedures that apply when a new customer opens a bank account. Addressing the transferability of the outcome of these procedures could improve the efficiency of switching accounts, which could be a widely applicable use case for action initiation. This sector-specific issue is discussed in detail below and addressed at Recommendation 5.21.

Concerns regarding digital maturity are less relevant for the banking sector as it is largely digitally-based sector and already implementing CDR data sharing. Larger financial institutions have built sophisticated IT infrastructure to deliver banking services, although various legacy systems are being maintained. Smaller financial institutions generally use specialist core banking solution suppliers to provide their IT needs in a secure and flexible way. Building on the IT of CDR data sharing should result in efficiencies in implementation and regulatory costs. Further analysis in a regulatory impact assessment would be an important part of implementing action initiation effectively.[116] This is particularly important for smaller financial institutions where regulatory costs may divert resources away from other initiatives.[117]

Implementation in the banking sector

With Open Banking already in operation, special consideration is needed for how action initiation, including payment initiation, should be implemented in the banking system. While banking sector submissions generally did not object to enabling action initiation, there was a common thread about payment initiation, to ensure the Inquiry was aware of the industry's work to implement the Mandated Payments Service (MPS) of the New Payments Platform (NPP).

The Inquiry considers that the banking sector designation should be extended to enable CDR action initiation once legislative amendments are in place. Accordingly, a full sectoral assessment to look at whether the banking sector should be designated for action initiation should not be required. However, thorough regulatory and privacy impact assessments and detailed consultation on the content of the designation instrument will need to be undertaken prior to a final decision by the Minister. This will ensure the design of action initiation can learn from the development of CDR data sharing and deliver benefits for the consumers.

Recommendation 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.

[116] Including the AML/CTF implications of implementing action initiation, including payment initiation.
[117] Customer Owned Banking Association submission, p. 2.

Figure 5.1 Cedric's finances

Cedric is sorting out his bills and knows he has been putting things off. He is worried that his payments are going to be overdue again and that his money has been sitting in his low interest transactions account rather than his high interest savings account.

To sort out his finances, Cedric signed up for 'MoniMoova', an app that can help manage money and has payment functionality. Cedric gives MoniMoova permission to receive CDR data from his utilities providers, and also authorises those utilities providers to send it to MoniMoova. Cedric can now see on the app that he is not late paying his bills this quarter.

He then gives MoniMoova permission to receive CDR data so that it can read his bank account balances and also gives permission to move money between his accounts to maximise interest earnings but ensures that he has $300 spending money in the transactions account. He also gives permission to MoniMoova to arrange payments from his transactions account to his utilities providers, and authorises his bank to accept these instructions. He limits the payment at one payment of up to $300 a quarter to each utility provider, as he doesn't expect his bills to be too high.

A week later Cedric's bills are due and MoniMoova pays his utilities providers from his transactions account. MoniMoova sends Cedric a notification that the bills have been paid and shows his account balances.

BEFORE

Cedric would miss bills and his money is earning less interest than it could.

AFTER

Cedric has his bills taken care of and his money is earning a higher amount of interest.

Consumer Data Right payment initiation

This section outlines the functionality and features required for CDR payment initiation and considers how these outcomes could best be achieved.

The Australian payments landscape

Payment methods

A 'payment method' is a way of facilitating the movement of money between different parties. These are crucial to the successful operation of Australia's economy. Table 5.1 outlines the main payment methods used in Australia.

Different payment methods are appropriate in different situations. For instance, the most appropriate payment method may depend on factors such as:

- the payment's destination
- the availability of the relevant parties
- what is most convenient
- the purpose for which the payment is being made
- the timing in which the payment must be settled, and
- the amount of the payment and currency of the payment.

More specific requirements and costs may also apply to certain payment methods. For example, specific file types need to be used to make a bulk payment.

Table 5.1 – Main payment methods used in Australia

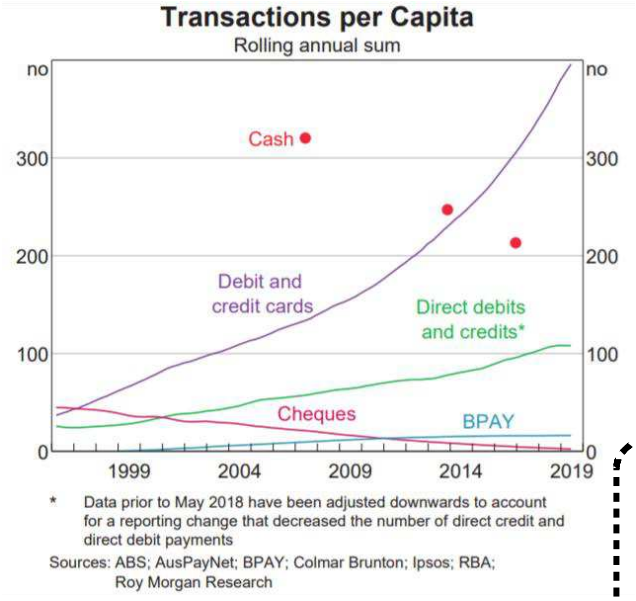
Payment methods	Description
Physical payments	Cash and cheque
Digital bank payments	Intra-bank transfers and inter-bank account-to-account transfers for direct debits or credits using the Bulk Electronic Clearing System (BECS) or the New Payments Platform (NPP)
Third party bill payments	Payments through a third party network specifically to pay bills – eg BPAY and Post BillPay
Card payments	Debit, credit and charge card payments – eg international card schemes and domestic card scheme (such as eftpos)
International payments	Payments to an overseas financial institution via international protocols and networks – eg SWIFT and Continuous Linked Settlement
Proprietary network payments	Other networks to transfer funds – eg Ripple and Alipay

One of a bank's primary functions is to make payments. These payment methods are available through a number of different channels, including:

- physical bank channels, such as at bank branches and ATMs
- merchant point-of-sale
- online channels, such as internet banking, e-commerce websites or apps on a mobile device, and
- corporate banking channels.

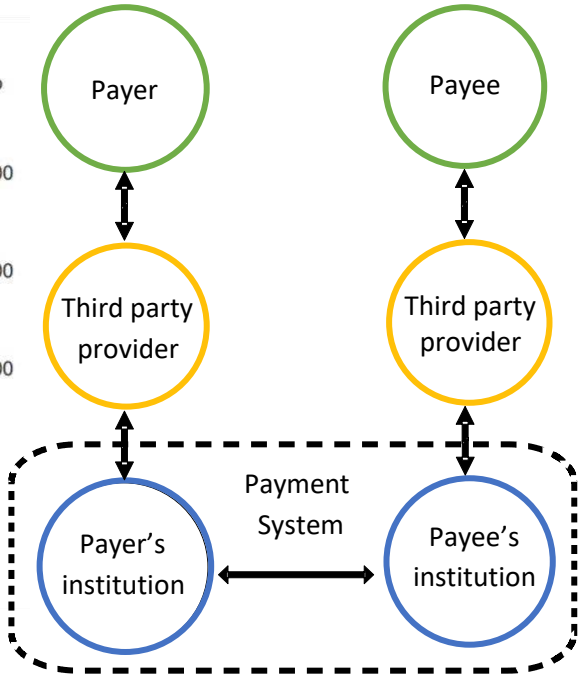
The growth of debit and credit card transactions compared with other payment methods over 23 years to 2018-19 is shown in Figure 5.2. This growth has been supported by consumer demand for the convenience of card payments.[118] Within that category, the strongest growth has been in debit cards with an average annual transaction growth rate of 14.2 per cent over the decade to 2018-19.[119] This indicates a continued consumer demand for payment methods that are digital, cross-channel and move money directly from their accounts. The uptake of digital payments has accelerated since the impact of COVID-19 with evidence of increased use of online shopping and reduced use of cash. Some of these shifts to digital payments are likely to be permanent changes in behaviour.[120]

Figure 5.2 – Payment methods in Australia over 23 years to 2018-19



Source: RBA Payments System Board Annual Report 2019, Graph 1

Figure 5.3 – Parties in a generic payment system



[118] RBA,2019, *Payments System Board Annual Report 2019*, p. 25.
[119] RBA, 2019, *Payments System Board Annual Report 2019*, p. 21.
[120] Bullock M, Panic, Pandemic and Payment Preferences, RBA, Speech on 3 June 2020, https://www.rba.gov.au/speeches/2020/sp-ag-2020-06-03.html

There are several parties who play a specific role in facilitating inter-bank payments. As shown in Figure 5.3, these are:

- the payer and payee – the people sending or receiving money, such as a consumer or merchant
- the institution(s) – the participant(s) (usually banks) who provide the payer and payee with their accounts
- the payment system – the mechanism and organisations that facilitates the execution of the payment, such as the NPP, and
- any third party provider – a party who acts on another's behalf in providing a payment service.

Sometimes only a subset of these roles are required, or multiple roles may be performed by the same party. For example, a payment system is not required when the payer and payee are customers of the same institution, resulting in an 'on us' or intra-bank transfer. This similarly occurs when a person transfers money between their own accounts at the same institution. In comparison, proprietary networks that do not use bank accounts, such as American Express, essentially operate the payment system as an intermediary between a payer and payee.

The stages of payment initiation

The payments process can be broken down into three stages:

- payment initiation
- payment authorisation, and
- payment clearing and settlement.

Payment initiation is the start of the payment process, where a payment initiation instruction is sent to a bank. Once this payment initiation instruction is received by the relevant bank, the bank primarily:

- records the details of the payment instruction
- checks the format of the payment instruction for compliance, and
- checks the details of the person giving the payment instruction to determine whether it is authorised to make the instruction for a payment from the account.

Once this has been completed, the bank moves to the second stage, payment authorisation. Before a bank progresses a payment initiation instruction, it needs to have a reasonable level of certainty the payment being requested has been authorised by its customer. This is to prevent fraudulent transactions being made from its customer's account. A bank may therefore request the customer to authorise a payment before progressing it through a step-up authentication measure, such as a one-time passcode.

Whether or not a bank seeks further authentication is subject to its assessment of the risk profile of the payment initiation instruction. For instance, payment instructions comprising large amounts, payments instructions directing money be transferred to unknown payees, and payment instructions initiated from unusual locations may all prompt a bank to seek further authorisation from its customer before progressing the payment.

After a payment has been initiated and the bank is comfortable progressing it, the payment clearing and settlement process occurs through the central payment infrastructure.

For clarity, payment initiation does not include the payment's authorisation or the payments clearing and settlement which are required to complete the payments process. Therefore, CDR payment initiation should only enable:

- the establishing of the CDR consent for an accredited person to give a payment instruction
- the setting up of the CDR authorisation for an institution to accept that instruction
- the sending by an accredited person of payment initiation instructions pursuant to that CDR consent, and
- the permitting of the receipt of that payment initiation instruction by the institution.

Payment initiation methods

Payment initiation messages can be sent by either a payer or a payee, or by authorising a third party.

A payer initiated payment describes a situation where the payer requests that a bank move money from one of their accounts to another account. A customer choosing to move money from their spending account to their savings account or directing that they pay a bill through BPAY are both examples of payer initiated payments. These can be normally managed through a customer's digital banking portal.

A payee initiated payment describes a situation where a payee asks a bank to move money to their account from another account.[121] For such a payment to go ahead, the payer's authorisation will be required. A direct debit payment initiated by a gym to collect a member's monthly fee is an example of a payee initiated payment. The gym would need pre-authorisation enabling the bank to progress the payment with certainty of the payer's authority.[122] However, this is not an entirely digitised process and so it can be difficult for a customer to manage or cancel a pre-authorisation once it is given.

A third party payment initiation arises where a payer or payee does not contact their bank themselves, but instead asks a payment facilitator to initiate a payment from a payer's account to the payee's account. An accounting software provider that prepares and initiates a payroll run for their client (or payer) is an example of this type of payment. This is also the way open API-based payment initiation models have been developed by banks to allow third party access on a secure platform.

[121] Payer payments are sometimes equated to 'push payments', as they appear to push money out of a consumer's account, while payee payments are sometimes equated to 'pull payments'. As both payer and payee functionality can technically be provided to a consumer through either push or pull payments, the Inquiry will only use the terms payer and payee initiated payments.
[122] This is a BECS direct debit request where a merchant seeks the authorisation of a customer to direct debit their bank account in the future under the terms and conditions of a standardised direct debit service agreement.

The use of third party access to digital banking portals ('screen scraping') to make payments directly from a consumer's account to a merchant's account is another form of third party payment initiation. This is discouraged by banks as it puts a customer's digital banking credentials at risk and can affect protections provided under the ePayments Code if an unauthorised or mistaken payment is made.[123] Further discussion is included below with Recommendation 5.14.

A significant domestic development in enabling third parties to initiate payments is the proposed expanded capability of the NPP through the MPS. The MPS seeks to enable consumers to provide ongoing authorisation for payments within specific terms to be made from their account in a secure and flexible way (refer to Box 5.1 for further details).

Through this, the MPS should increase customer control over how they make payments. The NPPA also publicly indicated that they intend to align, where possible, with standards for consent under CDR data sharing.[124] NPP participating financial institutions are bound to implement processes to support MPS functionality to enable payment initiation with payment agreement management by December 2021. NPPA has noted the uncertainty associated with the impact of COVID-19 and that these financial institutions should begin to roll out MPS services in early 2022.

Submissions to the Inquiry raised the importance of enhancing the functionality of initiating bank account-to-account payments by third parties. This was cited as a potential way to reduce the cost and complexity of delivering payment services.[125] Other submissions identified a lack of standardised APIs across industry and the importance of a consistent consumer experience across third party payment initiation processes.[126] Addressing these issues could increase consumer trust and confidence, and support competition in the payments system.

Given the focus and weight of submissions on payment initiation functionality, the Inquiry recommends that bank account-to-account payments should be prioritised in coordination with developments in the Australian payments industry. Expediting the delivery of greater customer benefits should be a core focus of payment initiation through the CDR. While the possibility of other payment methods (for example, cards) were considered, usage levels did not show a need for it to be prioritised.

Recommendation 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.

[123] Reserve Bank of Australia submission, pp. 2-3.
[124] New Payments Platform Australia submission, p. 4.
[125] Spriggy submission, p. 3.
[126] Deloitte submission, p. 27 and p. 33.

Box 5.1 – New Payments Platform – Mandated Payments Service[127]

In October 2019, New Payments Platform Australia (NPPA) published its first NPP Roadmap that included plans to develop a Mandated Payments Service (MPS) to support payers pre-authorising payments within certain parameters to be made from their account to another specified account. This is designed to enable recurring and 'debit-like' payments, and facilitate third party payment initiation solutions more broadly.

What is NPP?

Launched in 2018, the NPP is payments infrastructure that enables real-time, data-rich payments between bank accounts connected to the NPP, 24 hours a day, 365 days a year. While there are more than 72 million accounts that can send or receive payments via the NPP, NPPA estimates that about 95 per cent of all accounts will be reachable. Currently, more than 20 per cent of all account-to-account credit payments are transferred on the NPP.

NPPA states that the NPP operates as a non-profit maximising utility with 13 shareholders that are primarily financial institutions, including the RBA. There are over 90 participating financial institutions (including banks and non-banks) that are directly or indirectly connected to provide NPP-enabled services.

Planned features of the MPS

While NPPA has not yet released all the details of MPS's planned functionality, it has announced:

- **Digital payment agreements**[128] – Payment agreements will act as pre-authorisations for payments, as a digital alternative to direct debit today. These payment agreements will provide greater flexibility, however, as they have the ability to specify more payment parameters (such as number of payments per month or limitations on transaction amounts) than is possible with direct debit. Payment agreements in the MPS will be created by the institution seeking to initiate the payments via their financial institution and will require the payer's authorisation through their bank.
- **Centralised store of payment agreements** – Payment agreements will be stored in a secured, access-controlled central database as a record of the customer's agreements. This database will be accessible to all NPP participating financial institutions, allowing them to ensure that any initiated payments are indeed authorised. Consumers will be able to access and manage their payment agreements through their NPP participating financial institutions.
- **Single third party access point** – Those seeking to use the MPS will be able to choose from four direct or indirect access options.[129]

NPPA states that the MPS's flexible, extendable capabilities should support use cases such as:

- scheduled, recurring payments and subscription services
- payments initiated by third party service providers (eg payroll, accounting)
- event or trigger based payments (eg e-invoicing or smart contracts), and
- e-commerce, in-app, in-store and one-off payments.

[127] NPPA, *Mandated Payments Service – Enabling third party payment initiation on the NPP,* 30 April 2020.
[128] These digital payment agreements were previously referred to as mandates, and the centralised store of payment agreements was referred to as the Mandate Management Service (MMS).
[129] Further details on these access options are provided in the NPPA's submission attachment, pp. 8-10.

Required design features for Consumer Data Right payment initiation

CDR payment initiation should enable a customer to authorise an appropriately accredited person to use the CDR to initiate a bank account-to-account payment on their behalf, provided the customer could otherwise authorise their bank to initiate such a payment. The Inquiry recommends the following design features for CDR payment initiation.

- **Broad obligation and scope:** Banks, that are subject to CDR data sharing obligations, should be obliged to make third party payment initiation widely available. Banks should enable a broad and extensible functionality on accounts that are subject to CDR data sharing obligations, consistent with bank account-to-account payments a customer can initiate. Payment initiation should allow for competition among payment systems and leverage future developments.
- **Accessibility and standardisation:** Only appropriately accredited persons should be able to engage in CDR payment initiation. Standardised payment initiation APIs should apply to the CDR. Banks should be able to charge for access, however, consumers should expect costs of making a payment to be comparable to other digital channels.
- **Integrated consumer experience:** CDR payment initiation should have a consumer consent-driven approach, appropriate authentication settings and provide fine-grained authorisations. The consumer experience should integrate with, and complement, CDR data sharing and other action initiation functionality.

Each of these design features is discussed in detail over the next 11 recommendations (5.3 to 5.13). A summary of the required design features for CDR payment initiation is included in Table 5.2A. Further to these design features, there should be a clear allocation of liabilities for third party payment initiation and the CDR should support fraud mitigation processes (Recommendation 5.14).

In the context of developments in the Australian payments industry, later in this section there is a discussion of a CDR payment initiation roadmap (Recommendation 5.15) and opportunities for alignment of payment industry developments in third party payment initiation and these design features (Recommendation 5.16). This is aimed at providing a clear path forward for implementation.

A comparison of United Kingdom's (UK's) Open Banking and the NPPA's NPP with MPS proposal has been included in Table 5.2B. In part, this is to highlight the design features and payment functionalities that these systems have identified as necessary to meet the needs of consumers and businesses. UK Open Banking is a useful comparison as the design of CDR data sharing has drawn on elements of the regime and its payment initiation regime has been in active operation. While CDR payment initiation should learn from the ongoing implementation of UK Open Banking, CDR payment initiation needs to be designed for Australian consumers and the Australian payments environment.

Table 5.2A – CDR payment initiation design features Table 5.2B – Comparison

Required Design Features	Description	UK Open Banking	NPP with MPS proposal
Bank obligation to support CDR payment initiation (Rec 5.3)	Banks under CDR mandatory data sharing should provide access to third party payment initiation and be obliged to process instructions received from an appropriately accredited person as though they had been received from their customer.	9 mandated banks & other banks voluntarily	NPP participating financial institutions
Broad and extensible payment instruction functionality (Rec 5.4)	Banks should support broad and extensible payment instruction functionality, including where an accredited person initiates a payment on behalf of a payer or payee. (Refer to payment functionality in Table 5.3A)	Payer-based model	Payee and payment facilitator based model
Coverage of accounts (Rec 5.5)	Banks should enable third party payments on all account types covered by CDR data sharing that ordinarily support payment functionality.	Payment accounts accessible online	NPP-enabled accounts
Competition in the payments system (Rec 5.6)	CDR payment initiation should allow competition among payment systems and leverage future developments in the payments system to improve consumer outcomes.	Multiple payment systems	Only NPP
Accreditation for payment initiation (Rec 5.7)	The unrestricted tier should be the assumed starting point for accreditation for CDR payment initiation. An assessment should determine where lower tiered accreditation may be appropriate.	Via payment initiation service providers	Four NPP access options for third parties, but no accreditation system
Standardised payment initiation APIs (Rec 5.8)	Banks should be obliged to receive a CDR payment initiation instruction from an appropriately accredited person through a standardised API.	UK Open Banking standards	Sample APIs in NPP Framework
Cost of providing payment initiation (Rec 5.9)	Banks should be able to charge reasonable fees for providing access to third party payment initiators. ACCC should be empowered to intervene if unreasonable fees are charged.	Free for consumers, chargeable APIs	Commercial agreement for MPS
Consent-driven payment initiation (Rec 5.10)	An accredited person 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.	Consent-driven approach	Customer-authorised MPS payment agreement
Authentication requirements for payment initiation (Rec 5.11)	Authentication requirements for banks and accredited persons should be determined based on the risks inherent to payment initiation, as well as the need for consistency in the consumer experience.	Specific requirements including PSD2	For financial institutions and third parties
Fine-grained payment initiation authorisation (Rec 5.12)	Consumers should be able to specify a level of detail to their banks when authorising them to accept a payment initiation instruction from an accredited person.	Yes	Flexibility in the detail in a MPS payment agreement
Consistent and integrated consumer experience (Rec 5.13)	CDR payment initiation should be designed to integrate into the rest of the CDR to provide a consistent experience for consumers.	Read/write standards implemented together	Intended alignment with CDR noted in submission

Broad obligation and scope

Bank obligation for CDR payment initiation

In implementing CDR payment initiation, clear obligations must be placed on what banks are required to provide. The Government should impose, through the CDR, an obligation on banks to support access to third party payment initiation through accredited persons with the customer's authority, to the extent that the customer could otherwise initiate payments themselves.

Obligations to facilitate CDR payment initiation should be imposed on those authorised deposit-taking institutions (ADIs) that are subject to mandatory data sharing obligations under Open Banking.[130] As such, foreign ADIs, foreign branches of domestic ADIs and restricted ADIs should be excluded from this obligation. As with data sharing obligations under Open Banking, it may be appropriate for CDR payment initiation to be phased in gradually, having regard to the banks to which obligations would apply, the features which must be enabled and the order of account phasing by type under data sharing. This phasing should also have regard to other obligations placed on banks, such as those relating to the implementation of the NPP's MPS.

While maintaining the commitment to the obligation of third party payment initiation, regulators should be able to appropriately deal with ADIs on a case-by-case basis, allowing for specific or time-limited exceptions to the obligation.

Under CDR payment initiation, banks should be obliged to process, on a non-discriminatory basis, valid payment initiation instructions received from appropriately accredited persons as though they had been directly received from their customer through another digital channel. Banks should continue to be bound to all existing obligations placed on them by other regulatory regimes, such as the AML/CTF regime. For example, the bank should continue to be able to mitigate the risk of fraud and manage commercial risks through processes that correspond to the risk profile of the payment.[131] In addition, the rights and obligations under the existing banker-customer relationships between banks and consumers should continue to apply.

Recommendation 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. Authorised deposit-taking institutions should continue to be subject to existing obligations placed on them by other regulatory regimes.

[130] For ease of reference in text, a reference to 'banks' and 'ADIs' in this chapter is an ADI subject to a mandatory CDR data sharing obligation. A register of ADIs is available on the APRA website: https://www.apra.gov.au/register-of-authorised-deposit-taking-institutions

[131] Applying the approach in Recommendations 4.13 and 4.14.

Broad and extensible payment instruction functionality

CDR payment initiation functionality should be broad and develop over time. This functionality should seek to allow accredited persons to undertake the payment initiation actions that a customer can undertake themselves through other channels.

The payment instruction functionality should enable an accredited person to initiate a payment on behalf of a payer or payee, provided it has their authority. Its functions should provide flexibility in the frequency, amount, timing, customer involvement, direction and volume of payments. CDR payment initiation should allow for functional extensibility to incorporate future capabilities that develop from innovation in the payments system. The functionality for CDR payment initiation should align with the CDR's consumer goals and be complementary with the rest of the CDR. A description of the required payment functionality is included in Table 5.3A.

The payment instruction functionality has drawn on the experience of UK Open Banking payment functionality described in Box 5.2. A comparison of UK Open Banking and the NPPA's NPP with MPS proposal has been included in Table 5.3B to provide an indication of the functionalities provided.

Box 5.2 – UK Open Banking – Payment functionality

The UK Open Banking regime completed their initial implementation of UK Open Banking Standards in September 2019, mandated for the nine largest banks. The UK had implemented both account information and payment initiation services to meet the EU Payment Services Directive 2 (PSD2) requirements. The UK Open Banking Standards are payment type agnostic and include a range of payment-related functionality. UK Open Banking payment initiation standards were limited to single use consents so a customer must consent to the initiation of each payment or creation of a standing order. The UK Open Banking regime supports a range of payment functionality including:

- confirmation of funds (ie data sharing functionality)
- initiation of a single domestic payment
- initiation of a single international payment
- creation of a scheduled payment
- creation of a standing order (ie set of scheduled payments), and
- registration of a payment file (ie bulk payments).

In May 2020, the UK's Competition and Markets Authority (CMA), published a final approved roadmap for the implementation of UK Open Banking. [132] In addition to the above, the following payment functionalities are being implemented in this final phase:

- reversal of payments (ie refunds), and
- variable recurring payments (which extends the functionality beyond a single use consent).

[132] Open Banking Limited (UK), CMA publishes approved Roadmap for the final stages of Open Banking implementation, 15 May 2020: https://www.openbanking.org.uk/about-us/latest-news/cma-publishes-approved-roadmap-for-the-final-stages-of-open-banking-implementation/

Table 5.3A – CDR payment initiation functionality

Table 5.3B – Comparison

Required Payment Functionality	Description	UK Open Banking	NPP with MPS proposal
Both payer and payee initiated payments	Accredited persons being able to initiate payment either at the payer or payee's direction.	✓ Payer-based model	✓ Payee/payment facilitator-based model
Domestic payments	Accredited persons being able initiate a domestic payment on behalf of a payer or payee.	✓ Consent each time	✓* With pre-authorisation
International payments	Accredited persons being able to initiate an international payment on behalf of a payer.	✓	✗ Only inward domestic-leg
Flexibility in frequency, amount and timing	Accredited persons being able to initiate one-off or recurring payments with variable or fixed amounts. This includes scheduled payments.	Scheduled payments & developing variable recurring payments	✓*
Flexibility in enabling in-person and unattended payments	Accredited persons being able to initiate payments either at the consumer's direction (in-person) or in line with pre-authorised terms (unattended) to enable both payer and payee initiated payments.	In-person only	✓
Intra and inter-bank payments	Accredited persons being able to initiate a payment from a customer's account to accounts with either the same bank ('on us' payment) or a different bank (through a payment system).	✓	✓**
Bulk payments	Accredited persons being able to initiate a bulk payment.	✓	✓
Reversal of payments	Accredited persons being able to initiate a refund of a payment back to the consumer from a merchant.	Developing reversals	✓
Flexibility in payees	Consumers being able to consent to an accredited person to initiate payments without specifying the accounts to which payments can be made.	✓	Limited by the scope of pre-authorisation
Long-lived consents	Accredited persons having the ability to initiate payments on an ongoing basis, provided the payments align with a consent provided by the consumer.	Developing variable recurring payments	Limited as there is no usage consents

* Requires the setup of a pre-authorised MPS payment agreement

** Noting that banks do not process intra-bank payments through the NPP

The payment initiation functionality above should be complemented by payment-related action functionality, such as management of scheduled payments, registered payees' address books and authorisations (for example, direct debits). These payment-related actions should be considered as part of the general action initiation. Other actions which are undertaken less frequently, such as term deposit roll overs and credit card balance transfers, could also be considered with these payment-related actions. These should be supported by other fraud mitigation measures such as allowing step-up authentication, enabling banks reasonable access to data to detect and manage fraud risk and providing reasonable flexibility to not action suspicious instructions.

Recommendation 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.

Coverage of accounts

Submissions to the Inquiry have focused on bank account-to-account third payment initiation as a missing link in payment functionality, but did not specifically comment on account coverage. Given the implementation of CDR data sharing, the Inquiry considers the extension to payment initiation should apply to those accounts covered by the Rules shown in Table 5.4 below.

CDR payment initiation would only be a new instructional channel. The CDR would only require the support of payment functionality that is provided by the bank for a given account. This should in most cases align with the payment functionality available in a customer's digital banking portal. On this basis, accounts such as residential home loans for example should not be required to provide the same level of payment initiation functionality as a transaction account. Similarly, credit card payments that are made through the card payment systems would not be expected to be facilitated.

If there is a change of account coverage for CDR data sharing, it should be expected that this would similarly apply to CDR payment initiation, provided there is corresponding payment functionality.

Table 5.4 – Account coverage for CDR data sharing

Phase 1 product	Phase 2 product	Phase 3 product
Savings account	Residential home loan	Business finance
Call account	Home loan for an investment property	Loan for an investment
Term deposit	Mortgage offset account	Line of credit (personal)
Current account	Personal loan	Line of credit (business)
Cheque account		Overdraft (personal)
Debit card account		Overdraft (business)
Transaction account		Asset finance (including leases)
Personal basic account		Cash management account
GST or tax account		Farm management account
Personal credit or charge card account		Pensioner deeming account
Business credit or charge card account		Retirement savings account
		Trust account
		Foreign currency account
		Consumer lease

Recommendation 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.

Competition in the payments system

A single payment may be able to be processed through a number of different payment systems. For example, BECS and the NPP are both payment systems that provide transfers between bank accounts, although they provide different service offerings.

Payment initiation through the CDR should be implemented in a payment system agnostic manner to enable competition among, and innovation in, payment systems. There should be flexibility in the implementation and the CDR should not mandate that any one specific payment system be used.

In distinguishing the payment initiation from any particular payment system, TrueLayer stated in its submission that:

> *Payment initiation services should sit in an 'instructing' layer above the underlying inter-bank payment infrastructure.*[133]

Allowing competition should facilitate improved consumer outcomes. This is particularly important in a dynamic environment where there may be changes in payment methods and systems. When a new payment system emerges in the future, it will be important that the CDR regime remains open to its use to process payments initiated through the CDR. It follows that the Rules and Standards to support payment initiation should not be payment system specific as far as is possible.

Importantly, requiring that CDR payment initiation allows payments to be processed through a variety of payment systems does not mean that this choice should be given to consumers, if this choice is not otherwise available to the consumer.

Recommendation 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.

[133] TrueLayer submission, p. 11.

Accessibility and standardisation

Accreditation for payment initiation

Accreditation should be required for a third party to send a payment initiation instruction through the CDR. As payments risk the loss of money, possibly in real-time, the potential level of risk associated with initiating this action is considered to be high. Even a business model based on small individual payment amounts could be considered higher risk, due to the frequency and scalability of transactions.

Accreditation does not only provide a level of assurance to consumers but also to those banks receiving instructions through the CDR – that is, assurance as to the third party's information security arrangements, whether they and their management are fit and proper, and whether they hold adequate insurance against breaches of the CDR regime.

The 'unrestricted' tier should be the assumed starting point, however, the CDR rule maker should undertake detailed information security and insurance assessments to determine what additional requirements may be appropriate. Such a review should have regard to the special obligations and requirements placed on banks, and should involve consultation with industry, consumer groups and the relevant regulators. This review should also examine whether lower tiers of accreditation could or should be enabled for accredited persons seeking to initiate lower risk payments, such as payments with maximum thresholds over a given period or payments restricted to registered payees.

The process to be accredited for payment initiation should be consistent with the rest of the CDR accreditation process. The reviews and processes described here are consistent with Recommendation 4.8 on accreditation for action initiation more broadly.

Accredited persons would continue to be subject to existing regulatory obligations, such as licensing requirements. Some potential licensing obligations are discussed in 'Interactions with other regulatory regimes' further below.

Recommendation 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.

Standardised payment initiation application programming interfaces

CDR payment initiation instructions should be sent to a bank through an API channel. These APIs should be consistent across industry.

The benefit of a standardised approach is well-appreciated as consistency of requirements lowers cost for access by accredited persons. Standardisation allows accredited persons to 'plug and play' with different institutions. They can reuse their existing information technology and systems without significant amendments, use off-the-shelf software, or engage external service providers providing standardised services.

Currently, there is no standardisation of sector-wide APIs for payment initiation. Notably some banks, such as Macquarie Bank and National Australia Bank, have made APIs available for their customers and third parties. The NPPA has also published sample APIs in their NPP API Framework as guidance for interested participants to enable third party service providers and software developers to design NPP payment services.[134] While it is not mandatory for NPP participants to develop their APIs in alignment with these sample APIs, there are indications that participants would adhere for consistency.[135]

The Inquiry recommends that in applying payment initiation as a CDR action, standardised industry-wide payment initiation APIs should be made mandatory. These standardised APIs should be designed by the DSB in close consultation with banks, payment system operators, consumer groups, accredited persons and other stakeholders. This collaboration will ensure that the mandated APIs leverage the existing work undertaken by banks and payment systems and are able to interoperate with services beyond CDR payment initiation.

The CDR payment initiation APIs should use the NPP API Framework and the UK Open Banking standards as reference points. These align with the international standard ISO 20022 that assures data consistency and interoperability along the value chain which, amongst other things, assists with AML/CTF compliance.[136] As the CDR looks toward developing APIs with a broad payment functionality, these international payment standards should be referred to as an important reference point as it will promote the interoperability of messages and the ability for accredited persons to expand activities overseas.

[134] New Payments Platform Australia, 2019, New Payments Platform API Framework – Publication Version 3.0: https://nppa.com.au/wp-content/uploads/2019/11/NPP-API-Framework-v3.0_28-Nov-2019-1.pdf
[135] New Payments Platform Australia submission attachment, p. 12.
[136] SWIFT submission, p. 5.

Recommendation 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.

Cost of providing payment initiation

Banks should be entitled to charge fees for providing access to third party payment initiators. This is reasonable given the risks they take on as a participant in a payment system and the cost of providing any value-adding services they might provide.

However, any fees charged should be reasonable and proportionate to the risks involved.

Use of payment initiation APIs should be *chargeable* in a similar way to voluntary sharing of CDR data is currently allowed to be chargeable. The existing powers for the ACCC to intervene when charges are not reasonable should similarly apply.[137]

It would be reasonable for consumers to expect any charges to be comparable to those imposed for their use of other digital banking channels.

Recommendation 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.

Integrated consumer experience

CDR payment initiation should be interoperable with the rest of the CDR regime. An accredited person should require the consumer's explicit consent to send payment initiation instructions through the CDR, and the consumer's bank should require authorisation to act on these instructions. This process should be integrated with CDR data sharing and the rest of CDR action initiation. As with the rest of the CDR, the consent process for CDR payment initiation should be easily accessible, while still including intentional frictions where appropriate to promote active consumer participation and enable necessary banking security measures.

[137] For example, under section 56BV of the CCA for chargeable CDR data.

It is important to reiterate that the CDR itself is only seeking to enable a third party to send payment initiation instructions, and will not enable them to progress payments past this point. The NPPA stated in its submission that:

> *Payment initiation messages, which are essentially only instructions for a payment to be made, are inherently less risky than a payment clearing message, which entails the actual movement of money.*[138]

Consents

When enabling an accredited person to send payment initiation instructions on their behalf, the consumer should outline the kinds of payments they are allowing the accredited person to initiate, as well as the purposes for which they are permitting the accredited person to make these payments. These should be treated as access and usage consents. As is the case under existing CDR data sharing arrangements, banks should not automatically be provided with the information contained in a CDR usage consent, and should not be required to determine whether a requested payment complies with a usage consent.[139]

Consents for payment initiation should reflect the requirements set out in the rules and standards and be voluntary, express, informed, specific to purpose, time limited and easily withdrawn. The process for giving payment initiation consents should be integrated into the broader CDR consent process in a way that best facilitates consumer engagement.

The DSB should undertake consumer experience testing to determine whether any particular arrangements are required to ensure that payment initiation consents are properly understood by consumers. Such arrangements could include a requirement that payment initiation consents be displayed at a separate point to other consents during an accredited person's consent flow process.

Ongoing consents

A consumer should be able to grant ongoing consents to accredited persons to initiate varied (by amount or payee) payments on their behalf. For an accredited person acting on behalf of the payer, this would allow them to initiate varied payments from the payer's account. For an accredited person acting as a payee (or on behalf of a payee), this would allow them to instruct that varied payments be made from predetermined payer accounts to their own account (or the payee's account). Requiring a consumer to go through the consent process each time their accredited person seeks to initiate a new payment on their behalf, regardless of how similar that payment may be to previous payments, may result in the CDR consumer experience not meeting the consumer's expectations and limiting the range of services that could be facilitated. Though consumers should be able to provide ongoing consents, banks should still be able to request step-up authentication or recommend pre-authorisation where appropriate.

---

[138] New Payments Platform Australia submission attachment, p. 10.

[139] A consumer may be able to direct an accredited person to share information about their usage consent with their bank, should the accredited person offer such a service and the consumer see benefit in doing so. The sharing of consent information is discussed further at Chapter 6.

Enabling an accredited person to send varied payment initiation instructions to a consumer's bank on an ongoing basis is likely to be one of the CDR actions with the highest propensity for risk if not implemented in a careful and considered way. As such, it is important that privacy and security protection safeguards be implemented alongside the enablement of this functionality to protect consumers.

One key concern is the level of customer authentication required by third parties through whom a person can instruct variable payments be initiated. For instance, consider an accredited person who offers a service that, after receiving the consumer's express consent, enables the consumer to initiate variable payments from their accounts at multiple banks using a single application. In this situation, if this application has insufficient consumer authentication requirements in place to ensure that the consumer initiating payments through the application is authorised to do so, then the consumer could be placed at significant risk. The authentication processes required should be determined by the DSB as part of the Standards.

Authentication

After the customer provides its consent to the accredited person, the bank should be required to authenticate the consumer, and the consumer must then provide the bank with an authorisation of the kinds of payment initiation instructions they are authorising be received.

Authentication requirements are discussed in detail in Chapter 8. The level of authentication required by data holders and accredited persons to be engaged in payment initiation should be determined via the minimum data assurance standard and risk assessment processes recommended in Recommendations 8.2 and 8.3.

Authorisations

Subject to the finding of the DSB's consumer experience research, a consumer should be able to authorise multiple different CDR actions and data sharing agreements as part of the same authorisation process.

The consumer should be able to provide fine-grained payment authorisations, specifying a range of additional criteria about the only kinds of payment instructions that they are authorising the data holder to progress.

Though banks may have regard to these payment initiation authorisations when determining whether to immediately progress a payment request received by the accredited person or whether to conduct step-up authentication, the existence of a payment initiation authorisation itself should not necessarily result in a transaction automatically being processed. Banks should still be able to conduct due diligence to protect consumers from fraud. Providing greater detail to a bank about the kinds of payments that the consumer is authorising be progressed through fine-grained authorisation may provide a bank with greater assurance that a payment requested by an accredited person does not require step-up authentication. Alternatively, instructions requesting payments that have been preauthorised by the consumer through processes like direct debit agreements or MPS payment agreements could also increase bank confidence that a CDR payment initiation request is legitimate.

A bank will also be able to refuse to action a payment for which there is a valid authorisation in accordance with its usual processes. This could include if it considers this to be necessary to prevent physical or financial harm or abuse, if the bank has reasonable grounds to believe that the payment would adversely impact security, integrity or stability of the bank's systems.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Clear liabilities and responsibilities

Clarity in the allocation of liability and responsibility for CDR payment initiation is critical to building and maintaining consumer confidence in the CDR. Many submissions have raised concerns about how liabilities for payments would be allocated when they are initiated by a third party. Some raised how the liabilities could shift to payment initiators[140] and referenced other possible models to draw

[140] Including AusPayNet submission, p. 5; National Australia Bank submission p. 5; Commonwealth Bank of Australia submission, p. 9.

on, including the EU's approach in PSD2[141] and the card payments liability framework,[142] others noted the need to consider carefully the interaction with other regimes, such as the ePayments Code.[143]

Payment initiation under CDR is not a comprehensive payment system or scheme. Instead, it is a new channel for communicating instructions to make payments from a customer's bank account on behalf of the customer. The CDR does not govern the creation of the customer's bank account, or the legal relationship between the customer and its bank. Nor does the CDR govern the making of the payments using existing payment systems and schemes. The allocation of liability for CDR payment initiation needs to be considered in this context, as complementing the legal and regulatory arrangements which are already in place between the bank and its customer, and under the governance of the relevant payment system or scheme. The CDR should not seek to replace those arrangements and their regulation is properly a matter for the regulators of banking and payment services and all of the relevant stakeholders.

The allocation of liability and responsibility discussed in this section is only part of the protections which are offered to consumers in connection with CDR payment initiation. The more general consumer safeguards in the CDR, and the recommended enhancements in Chapter 7, offer consumers further protections in addition to those described below.

Existing allocation arrangements

The Inquiry considers that the approach taken to allocating liability needs to use, as a foundation, the arrangements which already apply to protect a customer with respect to unauthorised payments from their account. Unauthorised payments are payments which are made from the customer's bank account without the customer's permission. Examples include payments which are made from the customer's account due to fraud or system error. They are referred to as 'unauthorised' because the bank does not have the customer's authority to make the payment. This is different from the CDR authorisation for a bank to receive an instruction from an accredited person in payment initiation.

The existing allocation of liability for unauthorised payments from a customer's bank account differs depending on the type of customer, type of account, the terms and conditions of the account and the bank involved. For example, the ePayments Code has provisions which allocate liability for unauthorised payments.[144] However, it is a voluntary code and does not apply to all payments which are made from bank accounts in Australia.[145] Despite these differences in allocation, it is common for the arrangements to address responsibility for the conduct of persons that the customer appoints to operate their account on their behalf (such as supplemental card holders and employees). For example, under the ePayments Code, the holder of an account takes some responsibility for the misconduct of a person that they have agreed with the bank can perform transactions on their

[141] Article 74 of PSD2 (Payer's liability for unauthorised payment transactions).
[142] Tyro submission, p. 6.
[143] ANZ submission, p. 6.
[144] The ePayments Code refers to these as 'unauthorised transactions'.
[145] Clause 2.1 to 2.5 of the ePayments Code. For example the ePayments Code applies only to banks that are subscribers to it and it does not apply to business accounts.

account. The account holder is liable, subject to certain limitations, for losses from an unauthorised transaction which were contributed by such a person's fraud.[146]

Principles for allocating payment liabilities

The Inquiry considers that the following four principles should underpin the allocation of liability for unauthorised payments which involve a payment initiated by an accredited person through the CDR.

- An accredited person should be responsible for its own conduct with respect to unauthorised payments. This is consistent with the principle applicable to sharing of data under the CDR and is also consistent with the recommendations made in Chapter 4 on action initiation more generally.
- The existing compensation arrangements for unauthorised payments which apply to the relevant account, including the ePayments Code where relevant, should continue to apply between the bank and its customer. Consistency with these existing frameworks is important to avoid uncertainty about the rights of consumers in relation to their bank accounts.
- For the purposes of applying those existing compensation arrangements between bank and customer, the conduct of the accredited person should be taken to be the conduct of someone who the bank and the customer have agreed can operate the account on the customer's behalf. The accredited person should not be treated as an unauthorised person when it gives payment initiation instructions and they should be treated like others that the customer properly authorises to give payment instructions on their account.[147]
- If the bank or customer suffers loss because of this conduct (taking into account the compensation arrangements between the bank and its customer) then they should be compensated by the accredited person for that loss and have a direct right of action to support this. For consumers, this should be supported by the dispute resolution protections available to them under the CDR. As is the case in the CDR currently, CDR participants should be able to take action for breaches of CDR obligations by other participants in relation to losses they suffer.[148]

This allocation distinguishes the customer's right of compensation from its bank (which arises from the existing account arrangements) and the ultimate responsibility of the accredited person for their misconduct (which is created by the direct right of compensation for the bank and customer for the loss suffered). It results in the accredited person being responsible for their misconduct and having to compensate the bank (if the bank has compensated the customer), the customer or both. The application of the existing allocation arrangements for the account means that the customer continues to take some responsibility for the conduct of the person (the accredited person) they have chosen and consented to acting on their behalf. This is reasonable because the bank would have had no role in the decision to engage an accredited person. However, the bank continues to

[146] Clause 11.2 of the ePayments Code.
[147] In some cases adaptation will be required, for example if the compensation arrangements provide only for individuals to operate an account on behalf of the holder.
[148] Sections 56EY (Actions for damages), 56FD (Legal effect of data standards) or 82 (Actions for damages) of the CCA.

have obligations to compensate the customer for unauthorised payments consistently with existing compensation arrangements with the right to recover from an accredited person if the unauthorised payment was caused by their conduct.

Some examples applying the four principles to the ePayments Code are set out below.

- There is an unauthorised payment from the customer's account but the accredited person has complied with its CDR obligations and neither the customer nor the accredited person have contributed to the loss through fraud. The bank should be liable to compensate the customer for the loss in accordance with the ePayments Code.
- There is an unauthorised payment due to a security breach of the accredited person's IT environment caused by the accredited person failing to comply with their CDR information security obligations. Assuming that neither the accredited person nor the customer has contributed to this loss through fraud, then the bank should be liable to compensate the customer for the unauthorised payment and the bank should have a direct right to recover this from the accredited person.
- There is an unauthorised payment due to the fraud of the accredited person. The bank should not be obliged to compensate the customer for the unauthorised payment (subject to the limits of the customer's responsibility under the ePayments Code) and the customer has a right to compensation from the accredited person. To the extent that the bank does compensate the customer then it has a direct right to recover this from the accredited person.

Where customers have a right to compensation from accredited persons, they would have access to CDR internal dispute resolution, external dispute resolution and direct rights of action with any compensation awards backed by mandatory insurance coverage.

The application of these principles should incentivise banks to continue to manage fraud risk to protect their customers and invest in the technology for a safe and efficient payment system as they continue to bear similar responsibility for their customers' accounts, without bearing ultimate responsibility for the conduct of the accredited person.

ePayments Code changes

The ePayments Code has been the subject of several reviews. The Government agreed with the recommendation in the 2014 Financial System Inquiry that the ePayments Code should be mandated to strengthen consumer protections.[149] The 2018 Productivity Commission Inquiry into the Competition in the Australian Financial System also recommended that:

> *… ASIC should review the ePayments Code and update it to reflect changes in technology, innovative business models and developments in Open Banking. ASIC should more clearly define the liability provisions for unauthorised transactions*

[149] 2014 Financial System Inquiry Final Report, Recommendation 16, p. 161.

when third parties are involved, including participation in financial dispute resolution schemes.

ASIC should update the ePayments Code by end-2019 and commit to 3-yearly reviews.[150]

ASIC is currently reviewing the ePayments Code and expressed support for the above PC recommendation in their consultation paper.[151]

The Inquiry supports updating of the ePayments Code so that it further clarifies how liability provisions apply when payments are initiated through a third party, such as an accredited person.[152]

Fraud mitigation and cyber security

Customers rightly expect banks to protect their money. As such, the CDR should facilitate the provision of data to banks to help them manage privacy, fraud and cybersecurity risks.

The ANZ submission observed that, 'as new tools and solutions are developed in the payments system, the nature of fraud will change. This will require further monitoring and consideration of the sufficiency of technical security controls will be required.'[153] An example of these security controls is the information security data an accredited person would have indicating a compromised device from their direct interactions with the consumer.[154]

Banks should continue to commit to enabling Australians to safely transact online and should protect consumers from unauthorised transactions being made on their accounts. As recommended above, they will continue to be subject to their existing obligations under other regimes, such as transaction monitoring for high-risk and suspicious transactions under the AML/CTF laws.

The CDR should support the banks' efforts to detect and manage fraud, including:

- through an updating of the CDR information security requirements for payment initiation;
- by ensuring appropriate provision of information by accredited persons to banks in relation to payments, to support assessment of fraud risk; and
- by permitting banks to request step-up customer authentication where there is a reasonable suspicion of unauthorised payments.

[150] Productivity Commission,2018, *Competition in the Australian Financial System Inquiry Report*, Recommendation 17.6, p. 504.
[151] ASIC, 2019, CP 310 Review of the ePayments Code: Scope of the review, paragraph 139, p. 32.
[152] Particularly noting that the current ePayments Code does not specifically apply to NPP Payments, although industry arrangements ensure their coverage in practice.
[153] ANZ submission, p. 6.
[154] Commonwealth Bank of Australia submission, p. 8.

Recommendation 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.

Developments in the payments industry

The Australian payments landscape is undergoing a significant period of change as initiatives to simplify and modernise payment systems are progressing in the payments industry. These include with the implementation of the NPP's MPS, the potential consolidation of the NPP, BPAY and eftpos Payments Australia[155] and planning for BECS's eventual retirement.[156] The NPP is currently processing around one-in-five direct credit account-to-account transfers.[157] Over time this is expected to grow as payments migrate from BECS and overall payment volumes increase. The implementation of CDR payment initiation will need to take account of concrete plans and changes.

The Inquiry is cognisant of the various payments system processes that are currently underway or announced, including the RBA's Review of Retail Payment Regulation and the Review of the Australian Payments System.[158] The NPPA has released two NPP Roadmaps in response to a recommendation of the RBA's 2019 consultation on the NPP's functionality and access.[159] These have provided the Australian payment industry with a level of transparency on the plans of the NPPA and have assisted industry participants in making the commitments needed to support the development

[155] Hendry, J, IT News, NPP, BPAY and eftpos merger advances to study phase, 5 June 2020, https://www.itnews.com.au/news/npp-bpay-and-eftpos-merger-advances-to-study-phase-548989
[156] AusPayNet, *Future State of Payments Action Plan – Conclusions from AusPayNet's Consultation*, 18 August 2020, p. 15.
[157] New Payments Platform Australia submission, p. 1. (as at April 2020).
[158] Treasurer, the Hon Josh Frydenberg MP, released the Terms of Reference for this review on 21 October 2020. Mr Scott Farrell is leading the review.
[159] RBA,2019, *NPP Functionality and Access Consultation: Conclusions Paper*, p. 4.

of the payments industry. It is noted that the RBA, with the assistance of the ACCC, will conduct another review of NPP functionality and access issues commencing no later than July 2021.[160]

The Inquiry recommends that the Government should publicly consult with the payments industry and interested stakeholders in setting clear expectations for the implementation of CDR payment initiation. This should indicate the expected timing of CDR legislation for action initiation framework, which would include rule making and standard setting powers for payment initiation.

Recommendation 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.

Implementation of CDR payment initiation

Opportunities for alignment

Throughout the Inquiry's consultations on payment initiation, a range of stakeholders raised their concern that the CDR would require banks to build duplicative systems and infrastructure to that needed to meet their other obligations outlined above, including the NPP's expanded capabilities.

The Inquiry agrees that this would be highly undesirable. The objective of CDR payment initiation is to ensure that the functionality and features outlined in this chapter are provided. If a bank manages to comply with these requirements by leveraging existing or planned payments infrastructure, then this should be supported.

There is currently an opportunity for the Government and the NPPA to work together to align NPP and CDR requirements,[161] so that systems and processes established by NPP participating financial institutions to comply with the NPP's MPS can also be used to meet CDR requirements.

The Inquiry's recommended CDR payment initiation design features outline what is required to meet the needs of Australian consumers and businesses. Some of these features are provided by the proposed expansions to the NPP, while others go beyond this. The Inquiry notes that the arrangements needed to support the proposed NPP functionality[162] may also be able to be leveraged to support those CDR payment initiation recommendations that are not to be covered by the NPPA.

[160] RBA, *NPP Functionality and Access Consultation: Conclusions Paper*, p. 35: The RBA notes that this review could take place earlier if it becomes aware of significant issues or concerns regarding NPP access or functionality.
[161] For example, payment instruction content and formats, third party to bank API design, banks' customer authentication processes, banks' customer approval processes for MPS payment agreements/authorisation, consumer experience guidelines, accreditation requirements.
[162] Such as the ability for instructions for MPS payment agreement creation requests to be sent to any NPP participating financial institution, but then to be routed to the payer's bank.

Allowing banks to design their systems to adhere to both sets of requirements could also speed up implementation and reduce investment costs.

Given the proposed timing for NPP's MPS implementation, there is a relatively short window for alignment to occur. The CDR rule makers and standard setters could engage with the NPPA in advance of any legislative changes to the CDR regime being made, subject to the Government's response to the Inquiry. As part of this process, it may be necessary for the DSB to develop voluntary CDR standards for payment initiation in advance of legislation being passed, with a view to those voluntary standards becoming mandatory APIs in the future.

Recommendation 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.

Payments through a third party access to digital banking portal

Screen scraping can include processes under which consumers hand over their banking credentials to enable third parties to access otherwise restricted interfaces. This can then allow the third party to access data or initiate actions that are directly accessible to the consumer themselves.

The Open Banking Review considered how screen scraping should be approached and stated that:

> *Open Banking should not prohibit or endorse 'screen scraping', but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism.*[163]

More recently, the Senate Select Committee on Financial Technology and Regulatory Technology made the following interim recommendation in relation to screen scraping (also known as digital data capture).

> *The committee recommends the Australian Government maintain existing regulatory arrangements in relation to digital data capture.*[164]

[163] Open Banking Review, p. x.
[164] Senate Select Committee on Financial Technology and Regulatory Technology Interim report, Recommendation 22, p. 255.

Some data-driven businesses, such as illion and Finder, have advocated for the retention of the practice as a technological option at least while CDR is still being rolled out across the economy.[165]

However, the Commonwealth Bank of Australia recommended that a sunset clause be introduced to prohibit the use of unsafe methods of data sharing, namely screen scraping.[166] Similarly, the RBA stated in its submission that it:

> *… supports the CDR reducing the reliance of the financial sector on screen scraping and suggests that the Inquiry examine if a ban on screen scraping for data available under the CDR – as has been introduced in the United Kingdom – would support the financial sector's transition away from the practice.*[167]

Given the risks of consumers handing over their banking credentials to third parties, the EU has prohibited screen scraping in relation to payment services, subject to transitional arrangements.[168]

The Inquiry considers that, due to the risk involved, the eventual prohibition of the practice of screen scraping for payment initiation would be in the interests of consumers. However, this should only occur once CDR payment initiation is fully implemented as a viable alternative. This will only be when CDR payment initiation has a broad coverage (of banks and accounts) and functionality in place. Accredited persons will also have to have an appropriate level of access at acceptable costs.

Recommendation 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.

General action initiation in the banking sector

This section considers how action initiation in the CDR could enable consumers to apply for and manage products through APIs. As defined above, 'general action initiation' refers to banking actions apart from payment initiation.

The Inquiry has focused on common existing actions taken by consumers as part of their banking relationship. The CDR is not intended to require new types of actions that are not available through current channels, although the CDR should support participants voluntarily offering new types of actions.

[165] illion submission, p. 5, Finder submission, p. 10.
[166] Commonwealth Bank of Australia submission, p. 7.
[167] Reserve Bank of Australia submission, p. 3.
[168] EU PSD2.

The Inquiry observes that general action initiation requires strong consideration of potential security, privacy and fraud risks. The risks associated with action initiation may be higher than those associated with data sharing. While the CDR infrastructure is designed with technical specifications to deal with these types of risks, as addressed in the action initiation framework in Chapter 4, further privacy and information security assessment will be required.

Which general initiation instructions should be supported by the CDR?

The principle for CDR action initiation is that it should enable an accredited person to do something which the consumer is already able to do, with the consumer's authorisation through a digital channel. Action initiation therefore cannot be used to force a bank (or other person subject to an action initiation requirement) to do something which it would not do in response to a request from the customer itself. With this in mind, several submissions provided examples of potential action initiation use cases in banking.[169] These, along with other examples, have been broadly summarised in Table 5.5.

Table 5.5 – Main action categories

Instruction type	Examples
Product applications and establishing a new customer relationship	Applying for a deposit account, credit card or home loan pre-approval
Managing customer information and products	Changing an email address of the customer Changing details of stored payees Requesting a credit limit increase or imposing a transaction value cap
Closing a product or ending a customer relationship	Closing a dormant bank account

Product application and establishing new customer relationships

A product application is a process under which a bank receives a request for a banking product. The CDR can provide a new channel for those applications to be provided to a bank, with the consent of the customer. In line with the previously stated principle, the CDR would not regulate how the bank then chose to process that application, with that being left to existing sectoral regulations and practices.

Having standardised CDR APIs to receive product applications would have a range of benefits for consumers and businesses, such as enabling efficient and convenient product switching. Leveraging

[169] ANZ, Australian Banking Association, Financial Rights Legal Centre, National Australia Bank and Westpac submissions.

CDR data sharing – for example to pre-fill applications – could further simplify this experience for consumers.

The information required for a specific application will be dependent on the product's eligibility requirements and features. While it is expected that it should be possible to fully standardise application initiations for relatively simple products, such as deposit and transaction accounts, more complex accounts may require specialised information or may have varied application processes across banks. For instance, credit products such as credit cards or loans require a credit assessment. On this, Lixi stated that:

> *Credit products are unusual in that they are not available to be offered or sold to everyone. There are many legal requirements that restrict the way in which credit products can be suggested or sold to potential customers. The ability of a customer to access a particular credit product depends upon an assessment process to ensure that the lender is certain that the product is affordable for, and not unsuitable for the customer.*[170]

Standardisation in product application APIs would not preclude a bank from requiring any additional documents necessary for assessing the suitability of the client for some specific products, where this information would be required were the application received through another channel.[171] These additional documents could be provided through traditional channels or through proprietary APIs.

In designing the relevant CDR data standards for enabling applications to be lodged, the DSB should seek to include as many relevant fields as appropriate, to allow accredited persons and data holders to maximise the efficiency gains from standardisation. However, the CDR should support banks specifying additional fields to meet their own individual needs, provided this is done in a way that is compliant with CDR requirements and that is transparent to accredited persons. The DSB should collaborate with existing proprietary standard setters, such as Lixi, and leverage the experiences of overseas jurisdictions.[172]

Application processes will also need to differ between those consumers who have a relationship with the relevant bank and those who do not. Customer verification will be necessary for those applying for products with banks with whom they do not have an existing relationship.[173] Verification processes in banking are strict due to the Know Your Customer (KYC) requirements imposed on banks under the AML/CTF Act. The establishment of digital identity processes[174] and the enabling of KYC outcomes to be transferred could assist in making this process simpler for consumers, without reducing necessary safeguards. This is discussed further below with Recommendation 5.21. As discussed in Chapter 4, new consumers should be able to authorise a bank to accept an instruction to

[170] Lixi submission, p. 3. Noting that this was provided prior to the Australian Government's announcement on 25 September 2020 of its intention to change the circumstances in which responsible lending obligations apply with the exception of small amount credit contracts and consumer leases.
[171] For example, evidence of a building contract would need to be provided to support the application for a loan to fund construction. Similarly, business loans would require financial statements and business plans.
[172] For example, Hong Kong has prioritised product application APIs early in its Open API rollout.
[173] This is discussed further in Chapter 4.
[174] This is discussed further in Chapter 8.

enter them into a new product during the verification process, rather than being required to provide this authorisation separately. Such a process should still be compliant with the Rules surrounding authorisation.

Updating customer information

Customers need to update their details from time to time and manage their products. Enabling this could potentially require a broad range of actions. The Rules for the banking sector categorise information that could reasonably be subject to change in the following ways:

- customer data – in relation to information that identifies or is about the person and includes:
  - the person's name, contact details, including telephone number, email address and physical address
  - information provided by the person relating to the eligibility for a product at the time of acquisition, and
  - information on the operation of a business, including the business name, Australian Business Number (ABN), Australian Company Number (ACN), type of business, date the business was established, registration date, organisation type, country of registration and whether the business is a charitable or not-for-profit organisation.
- account data – in relation to a particular account includes:
  - authorisations on the account (including direct debits), scheduled payments and details of payees.[175]

Being able to have an accredited person update a consumer's information could enable a variety of use cases, such as requesting that multiple institutions be informed simultaneously of a change of address.[176] Many submissions from the financial sector however, expressed that the protection of the consumer should be paramount should such an action be enabled.[177]

Further, the Financial Right Legal Centre submitted that for joint accounts, in particular this could increase potential for financial abuse and other forms of domestic violence.[178]

The Inquiry notes that it is common for existing online banking channels to support variation of some personal information (for example, addresses and contact details), while commonly others cannot be changed through those channels (for example, names). Practices vary between banks.

It is clear that some core personal information carries higher risks of harm if unauthorised changes were to occur. For example information that may be used in identity theft such as contact information commonly used in customer authentication processes. Though digital identity frameworks could provide a safe way of dealing with this issue in the future, such frameworks are as

[175] Selected data from Clause 1.3 of Schedule 3 (Provisions relevant to the banking sector) to the Rules.
[176] National Australia Bank submission, p. 7.
[177] Including Commonwealth Bank of Australia submission, p. 9, Australian Banking Association submission, p. 13.
[178] Financial Rights Legal Centre submission, p. 22.

of yet immature.[179] Without adequate security measures in place – such as those verifying identity, it would be difficult to manage the security risks to third parties, consumers and banks.[180]

In the banking sector therefore, if these risks cannot be adequately managed, it may be appropriate for certain core personal information to be excluded from being updated through the CDR. Possible options to manage the risks associated with changing high risk information is to require that banks seek re-authorisation directly from the customer at the time that the updating action is sought to be taken. Another is to provide for fine-grained authorisations that are particular to the sensitive data that the customer wishes to allow to be changed.

As stated in Chapter 4, an assessment of the range and degree of the risks posed by allowing changes to high risk data sets and the potential mitigation measures that may be put in place should occur through formal information security and privacy impact assessments.

Managing a product

A consumer should also be able to manage variable features of a product through an accredited person via a CDR API. This would ensure that products continue to meet the consumer's needs. An example of this could be requesting an increase in the credit limit on a credit card. Product management action requests may result in the bank requiring additional information to be provided by the consumer to ensure that the requested change is appropriate.

An example of an account management action that should be enabled is the updating of a consumers payee address book. As the payee address book is essential for providing additional assurance that a certain payment instruction is legitimate, this should be treated as a high risk action. As such, at a minimum, banks should seek reauthorisation directly from the customer at the time that the updating action is sought to be taken.

As stated in Chapter 4, due to the potential sensitivity of altering some customer information, detailed privacy impact analysis and information security analysis should occur before determining the full scope of information that should be able to be updated through the CDR. Where appropriate, these assessments should also identify further risk mitigations.

Closing a product or ending a banking relationship

The closing of an account or ending of a customer's relationship with a bank should also be CDR actions. This is a necessary step to support streamlined switching of accounts. The consequences associated with closing a product or ending a relationship differ between products and providers. As it will be burdensome, if not impossible, to re-open a closed account or re-establish an ended relationship, the bank should be able to request the consumer's authorisation at the time that such an instruction is received from an accredited person. Such a request should provide an opportunity for the consumer to be made aware of the proposed action, but should not be used to unreasonably

[179] Digital identity frameworks are discussed further in Chapter 8.
[180] Australian Business Software Industry Association, p. 4.

dissuade the consumer from continuing and should be no more complex than the process for entering into the product or relationship.[181]

Voluntary actions

Other APIs should be able to be provided voluntarily, for example, a complaints or general enquiries function. This, for example, could enable an accredited person who has analysed a customer's transaction data and discovered an incorrectly calculated interest charge to request that this be rectified.

Such a function would support improved customer experiences while also potentially giving rise to efficiencies in complaint/enquiry handling by the bank.

In relation to the accessing of banking functions in third party applications, ANZ had suggested conducting consumer research to explore consumer appetite to access this functionality.[182] The Inquiry notes that this could help inform decision making on the prioritisation of general actions.

CDR support for general action initiation in relation to banking products should be carefully phased in. The current order in which accounts have been phased in for CDR data sharing reflects an assessment of the benefits and complexities associated with different account types. It may therefore be a useful starting point for the ordering of action initiation by account type. In relation to prioritisation by action type, applying to establish a new customer relationship and to acquire a new product should be prioritised, given their role in enabling streamlined switching.

Recommendation 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.

Recommendation 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.

[181] This is discussed further in Chapter 4.
[182] ANZ submission, p. 5.

Interactions with other regulatory regimes

Australian Financial Services and Australian Credit licensing regimes

Financial services, such as those in relation to banking products, are regulated by ASIC under the *Corporations Act 2001* (Corporations Act). Persons who carry out financial services are generally required to hold Australian Financial Services (AFS) licences.

Circumstances in which a person may carry out a financial service include where they provide financial product advice or deal in a financial product.[183] Broadly, a financial product is a facility through which a person makes a financial investment, manages financial risk or makes non-cash payments[184] and there a range of products specifically included as financial products.[185] Financial product advice is a recommendation or a statement of opinion that is intended to influence a person in making a decision about a financial product.[186] The AFS licensing requirements and exemptions that could apply depend on the business model that is undertaken. Therefore, accredited persons should determine how the licensing requirements apply to their business activities alongside their CDR obligations.

In the specific case of action initiation in relation to a credit product, an accredited person could also be required to have an Australian Credit Licence under the *National Consumer Credit Protection Act 2009* (NCCPA) due to their acting as an intermediary between a credit provider and a consumer (for a credit contract) or between a lessor and a consumer (for a consumer lease).[187] The Inquiry notes the Government's announcement to simplify access to credit for consumers and small business, including the removal of responsible lending obligations from the NCCPA, with the exception of small amount credit contracts and consumer leases where heightened obligations will be introduced.[188]

Given the range of services that could be enabled by data sharing or action initiation in the banking sector, it would be beneficial if ASIC provided guidance as to the circumstances under which an accredited person would also be required to hold an AFS or Australian credit licence. This includes in respect of the roles that accredited persons could play if they were to apply for a product, vary a product or initiate a payment on behalf of another party. It would be important to manage the regulatory burden, for example by coordinating government processes, to avoid unnecessary delay or costs for entrants.[189]

[183] Section 766A of the Corporations Act.
[184] Section 763A of the Corporations Act.
[185] Section 764A of the Corporations Act.
[186] Section 766B of the Corporations Act.
[187] Section 9 of the NCCPA.
[188] The Hon Josh Frydenberg MP, Treasurer, Simplifying access to credit for consumers and small business, 25 September 2020.
[189] Visa submission, p. 5.

Recommendation 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.

Identification verification assessments

Expansion of CDR functionality to include action initiation will be impacted by the current Know Your Customer (KYC) obligations required of banks under the AML/CTF Act. KYC obligations require that banks verify the identity of their customers, including their full name and either their date of birth or residential address against identity documents.[190] Customers switching to new products within their existing bank are often required to verify their identity again.

As is the case in other jurisdictions, banks should not be required to conduct AML/CTF checks on accredited persons in addition to checks on their own account signatories.[191]

The Open Banking Review found KYC identity verification processes in banking were slow and cumbersome and involved significant duplication. The Review supported implementation work being undertaken by the Attorney-General's Department to amend the AML/CTF Act to allow data holders to share the outcome of an identity verification assessment performed on the customer with ADRs as a means to improve efficiencies in the system.[192]

The Australian Government has introduced legislation to the Parliament to amend the AML/CTF Act to expand the circumstances where regulated businesses may rely upon customer due diligence conducted by a third party. These amendments seek to increase reliance on shared outcomes of identity verification assessments.

The degree to which the proposed KYC amendments facilitate action initiation and switching in banking should be observed closely once implemented. The Inquiry notes concerns expressed by stakeholders about the proposed reforms to the AML/CTF Act and specifically whether those reforms will offer an efficient and workable identification mechanism that could assist accredited persons in providing streamlined and convenient switching in the banking sector.

[190] In banking, identity is verified by application of the '100 point test' - the provision of a range of key identifying documents including passport, driver's licence, birth certificate, Medicare card, bank card etc. Different providers may request that the documents are presented in person or may accept digital or hard copies, certified or otherwise.
[191] The definition of signatory in section 5 of the AML/CTF Act was amended in *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017*, noting the discussion in the associated Explanatory Memorandum to the Bill at paragraphs 196 to 198 relating to instructions to account providers.
[192] Block8 submission also submitted that 'portable KYC' was an appropriate extension for CDR.

Recommendation 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.

Chapter 6: Read access enhancements

This chapter discusses ways the CDR can be enhanced to support different business models, encourage participation, promote fairness in the exchange of consumer data and increase the range of data available in the CDR system. This chapter also examines a number of additional measures that could increase consistency in consent terminology and bolster comprehension.

Development of an inclusive data ecosystem

Benefits of a sophisticated data ecosystem

As the CDR matures, it will connect more customers, data holders and data recipients, linked by their participation in a system with set rules and standards. Customers will develop relationships with both data holders and data recipients. Sometimes these connections will be strengthened by some parties performing more than one role. The connections and network effects should increase as other sectors are added to the CDR. As the connections increase, a data ecosystem should naturally grow in a similar way to the ecosystems in other markets where unique functions may be performed by specialist service providers, enabling a wider range of higher quality and more cost effective services. Specialisation may manifest in the regime in a number of different ways including through the presence of software providers, software-as-a-service, outsourced service providers, arm's length businesses working cooperatively and arm's length businesses operating independently but in complementary ways.

The CDR will ideally become a key channel in the Australian data economy acting as an enabling framework that supports a diverse range of business models. The CDR should not discourage new entrants and should not place further costs on participants where additional compliance requirements provide no benefit to the consumer. As submissions from specialised service providers have noted, excluding some preferred methods of data transfer (such as those discussed below) will often be detrimental to small and medium sized organisations.[193] The CDR also needs to allow users to connect to each other in a variety of ways to enable efficiency gains from specialisation and to foster innovation, enabling all productive transfers between service providers that do not unreasonably weaken the safeguards built into the CDR framework. Enabling the use of specialised service providers has the potential to reduce the time and costs required for data recipients to access the CDR.

The ability to pool data from multiple sectors will enable an entirely new field of services and products to offer enhanced customer choice and convenience. This new source of information from customers will enable data holders and data recipients to tailor product design to meet customer needs. The more successful the ecosystem, the more people will rely on it and prefer it to services available outside the CDR. All support functions allowed should generally follow the principle that transfers should not occur without express and informed consumer consent. Rather than operating as a closed system, the CDR should be the central part of a broader system where a customer's data

[193] Experian submission, p. 14, Data Republic submission, p. 10.

can be utilised by businesses outside the system, where appropriate, in a manner which complies with appropriate safeguards and maintains security and confidence in the system.

Recommendation 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.

Enabling a sophisticated data ecosystem

There is a range of possible ways that CDR data could be transferred to grow participation, develop business models and enhance the products and services in the CDR ecosystem. The following possibilities are discussed below:

- use of outsourced service providers (OSP) for specialised services
- accredited data recipient (ADR) to ADR transfers
- authorised representatives
- provision of data and information products outside the CDR system, and
- flexibility in business models in relation to the above.

The ACCC is currently consulting on a number of proposed rule changes that cover some of the recommendations below. The Inquiry is proposing what a future version of the CDR should include to achieve the outcomes articulated, and is not commenting on the rules proposed by the ACCC.

Use of outsourced service providers for specialised services

To benefit from specialisation and allow sophisticated supply chains to develop, ADRs should be able to outsource functions, but retain responsibility and liability. This outsourcing should be subject to proportionate arrangements to ensure an outsourced service provider (OSP) operates within their mandate. Restrictions preventing the use of non-accredited specialist third parties would have the potential to place the CDR at a competitive disadvantage to data access services used outside the CDR, such as screen scraping, where the ability to use third parties for data collection is not hindered by the same level of regulation.

The CDR will only improve consumer safety if people are willing to use it. The policy settings for the CDR must be directed at improving overall safety, which is a function of it both being safer and attractive, and therefore extensively used. Overly restrictive requirements that result in people continuing to use unregulated methods will result in a greater risk of harm being suffered by those the CDR is intended to empower and protect.

OSPs that do not collect data are already able to act on behalf of the ADR who holds ultimate liability to the consumer for any breaches, with any liability between ADR and the OSP then determined by contractual arrangements. Preventing OSPs from providing services under the same liability framework in relation to data collection, or requiring OSPs to become accredited themselves, will act

as an undue barrier to the provision of their specialised services. Such barriers would require ADRs to instead develop their own capability, or defer functions to more sophisticated ADRs (should the ability to transfer between ADRs eventuate).

With appropriate safeguards, use of specialised providers to transmit data should result in safer data sharing, while also enabling lower cost and quicker establishment of systems by ADRs (and lower ongoing costs).

When acting on behalf of accredited persons, OSPs would consequentially need to comply with existing standards, which include information security controls and API standards. An amendment to the Rules defining OSPs and CDR outsourcing arrangements to include both the collection of CDR data by an OSP, and disclosure to an ADR, would be required. Consent to transmit data would still be provided by the customer to the ADR, reflecting the liability ultimately held by the ADR under the outsourcing arrangement. This would operate in addition to the rule changes that let service providers perform the same functions by becoming accredited intermediaries, if they choose that path.

Recommendation 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.

Accredited data recipient to accredited data recipient transfers

An ADR should, with consumer consent, be able to transfer CDR data to other ADRs, functioning as voluntary disclosures. This will enable the transfer of CDR data, including value-added data products, to other businesses with services to offer the consumer.

Were the CDR to limit this capability, it would prevent one ADR from using another ADR to provide the consumer with a complementary or perhaps completely different service. For example, an ADR may want to provide ongoing access to enhanced CDR data to other ADR businesses for a unique consumer-facing application that they have designed, or to filter and process raw CDR data for easier integration with an ADR's ultimate use case.

Data set standardisation by data holders has been mandated to improve consistency, accessibility and interoperability across the data economy; this does not necessarily require government to mandate the formats in which ADRs then transfer information between themselves. An image or graph displaying insights generated from raw CDR data is one example of a possible output.

Transfers of responsibility for data within the regime should only occur with a consumer's consent, but special arrangements should be considered when an ADR is only acting as a conduit (perhaps with value adding or filtering). Given that the transferring data holder or ADR must have consent to disclose and the receiving ADR must have consent to collect, it may be that disclosure to the consumer of the presence of this kind of intermediary would be sufficient. Separate consents should

always be required if the intermediary retained or otherwise sought to use the data for any other purpose.

Recommendation 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.

Authorised representative model

Some stakeholders have suggested that the CDR should enable a data sharing intermediation model akin to the Australian financial services (AFS) licensing regime's authorised representative model. The AFS licence authorised representative model is a long-standing regime directed at balancing the need to ensure financial services are provided in a safe way, while seeking to ensure that regulatory burden does not unduly restrict supply of such services to those who need them. Under this model, an AFS licence holder may authorise others to provide financial services under its licence, subject to appropriate controls and acceptance of joint liability for breaches of licensing laws.

Some stakeholders have suggested that the CDR could adopt a similar model, where a CDR authorised representative would not need to hold CDR accreditation, while others have suggested a significantly lower level of accreditation. Under the proposal, the authorised representative would rely on the primary ADR for its feed of CDR data (which would allow the primary ADR to act as a gatekeeper to the CDR system), and the primary ADR would be responsible for determining other arrangements to ensure compliance by the authorised representative. An authorised representative would differ from a client facing OSP as it would be operating a legally distinct business from the perspective of the consumer.

Recommendation 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.

Provision of CDR data to data holders

Data holder activities are currently restricted to the provision of data to ADRs. This means that a data holder would need to receive CDR accreditation before receiving CDR data from another data holder or ADR. Currently, a bank that is an ADR that receives CDR data can take on a new customer, and then receive consent from that customer for the data they receive to be treated as CDR data no longer. A data holder will naturally hold CDR data for consumers relating to their activities in a

particular sector, subject to existing regulations and controls, so an extension of their capabilities to receive the same data in relation to their own sector from ADRs or other data holders would not increase risk to customers.

Giving data holders the capability to receive CDR data from their sector would lead to wider use of consumer data, enhancing competition, and enable the transfer of data for new customers from their old to their new provider. Customer switching is one activity where giving data holders a data recipient capability would allow stronger competition and better record keeping. For example, an ADR product comparison provider may download and want to transfer CDR data to a new bank, if the customer has approved the switch recommended by the ADR. That new provider could not currently receive this data if they remain just a data holder with no ability to receive data.

Currently, data holders that are Authorised Deposit-taking Institutions (ADIs) are eligible to apply for streamlined accreditation as set out in the Rules, which permits them to receive CDR data at the unrestricted level. To be eligible for streamlined accreditation, participants in newly designated sectors would need to be subject to adequate existing regulation and controls. Sectors dealing with lower risk data may not be subject to adequate existing regulation and controls for streamlined accreditation to apply, or may be suitable for streamlined accreditation at a lower tier. A data holder could simply be eligible to receive data relating only to activities in their own sector at the direction of the consumer, including derived data. To be eligible to receive this data, data holders for a newly designated sector would need to be assessed to confirm their ability to protect and manage CDR data. Individual data holders would need to ensure that their policy covers how they will manage CDR data, should they wish to receive it.

Recommendation 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.

Provision of data and information products outside the Consumer Data Right system

Where it is appropriately safe to do so, CDR data should be able to leave the system for use by trusted parties. Consumers should be able to access services provided by persons within the CDR regulatory perimeter, but also by persons outside the perimeter who are supported or assisted by those within the perimeter.

The Open Banking Review noted that the CDR regulators might also conclude that participants in a particular sector may be eligible to receive CDR data without requiring accreditation. There are circumstances where accreditation may not reduce the risk involved to the customer. In some use cases, CDR data would be substituting data that would be accessed elsewhere less efficiently, or CDR data would be covered by regulation or controls over customer information that already exist in a particular industry.[194] This needs to be subject to appropriate restrictions that are proportionate to

[194] Mortgage and Finance Association of Australia submission, p. 2.

the risks associated with data leaving the regime, guided by common principles governing data security and confidentiality. Any restrictions need to be crafted considering the regulatory arrangements already in place and other circumstances or arrangements that otherwise manage these risks.

Provision of data and information products to non-accredited persons: Regulated persons

There are a number of scenarios where consumers are likely to benefit from the transfer of some CDR data to recipients that already use similar information provided outside the CDR. These recipients may already comply with their own industry regulations covering limitations on use and disclosure of information for professional purposes, including consequences for misuse of information provided by customers.

Examples of such data products and regulated, non-accredited recipients could include:

- An accredited CDR-driven accounting software provider supplying financial data directly to a financial adviser or lawyer
- An accredited CDR-driven accounting software provider providing a consumer's accountant with access to accounting information, including accounting records at a transaction level
- Mortgage brokers receiving data feeds from an accredited provider to their own software systems that generate analysis and pre-fill forms, and
- An ADR providing CDR-driven product applications, income and expense verifications, creditworthiness assessments to a non-ADR lender.

The opportunity for the consumer to direct CDR data to these regulated third parties could save both the consumer and the recipient time and money spent managing raw data. If they cannot use the CDR to access data then they may use unregulated data access methods, exposing them to greater risks.

Requiring entities, who are subject to existing regulations and accountable for the use of consumer's data under those regulations, to obtain accreditation (even at a lower tier) would be disproportionate. For example, an accountant can be trusted with accounting data – whether it is CDR derived or not. If they cannot be trusted then it should be the role of the frameworks regulating accountants to address this, and it is not a role for the CDR, unless there is risk inherent in the CDR data transfer mechanism.

Appropriate restrictions may be required to ensure data is shared only with persons for the purposes of regulated activities. Consideration should be given to ensuring that a non-accredited recipient has given appropriate undertakings, or is subject to appropriate duties and obligations, regarding their conduct in relation to data.

The CDR should support, with consumer consent, an ADR producing and providing regulators or other government bodies with CDR data or information products derived from CDR data. The regime currently enables CDR derived data to be provided to the ACCC and OAIC for CDR regulatory compliance. Further examples could include the use of CDR data to complete forms for lodgement to

meet regulatory requirements or use of CDR for completion of taxation documents for lodgement with revenue authorities.

Recommendation 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.

Provision of data and information products to non-accredited persons: Low risk and high public benefit

The CDR should also in rare circumstances provide greater access to low risk persons, especially where there is a significant public benefit to be gained. For example, financial counsellors are not required to hold AFS licences due to the low risk nature of their services. Where entities providing a service for the public good have been excluded from existing regulatory or licensing regimes due to their activities being considered lower risk, the CDR regulator should be able to recognise them as suitable recipients of CDR data. Disadvantaged and distressed people may potentially benefit greatly from counsellors being able to access prefilled financial summaries or detailed financial analysis provided (with their consent) by an ADR. The CDR has significant potential to assist people suffering financial hardships, including due to the impact of COVID-19, as has been shown by the use of Open Banking in the UK to support those affected.[195]

Recommendation 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.

Provision of information products to non-accredited persons: Mere insights

The regime should allow an ADR to transfer 'mere' insights based on CDR data to someone outside the CDR, with consumer consent. Under the CDR, it is possible that an ADR could provide insights derived from CDR data to fulfil a sole purpose for a consumer. This could include outcomes of income and expense verification or information confirming cash flows and prior rental history that real estate agents require before renting a property to new tenants. For example, intermediaries are developing an online way for applicants to use their employer's Single Touch Payroll data to safely and accurately prove their income.[196]

[195] Open Banking Limited (UK), #PoweroftheNetwork website, https://www.openbanking.org.uk/insights/power-of-the-network
[196] Verifier, Proof of Income website, https://www.verifier.me/income-verification

This information is already provided by customers in a less refined form, so allowing a more accurate version of the same information to be provided through the CDR would make the existing process more efficient. Existing regulation of this information outside of the CDR would still apply. The ACCC is currently consulting on how the scope of insights data would be defined in the Rules. A principles-based test is one approach that could avoid an overly prescriptive process for allowing these insights.

Recommendation 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.

Flexibility in business models

The CDR regime should facilitate, rather than restrict, the development of diverse and innovative business models that meet the objectives and principles of the CDR regime. The regime should not dictate particular business models or seek to exclude any solely on the basis that another supported model is sufficient. Business models should generally only be prohibited or restricted if a case is made that this is necessary to protect consumers or the system.

Example business model - Algorithm-to-data

One example of a model that requires specialist service providers and unique data transfers is an algorithm-to-data model. Instead of raw data flowing to an ADR, the algorithm is transferred to the data. This avoids raw data flowing from a higher security environment to a lower security environment. The holder of the data processes the data and provides the potentially lower risk output, such as a confirmed credit reference check,[197] to the ADR. The data might be held and processed by an OSP, an arm's length ADR or voluntarily by a data holder. This model could allow ADRs, under a lower tier of accreditation, to apply new algorithms to consumer data without being required to securely collect and store higher risk data themselves.

Example business model – Arm's length intermediaries

The CDR currently requires ADRs to request and collect data from each of their customer's data holders directly. There are other models available in the ecosystem that use specialist arm's length intermediaries to provide the same service.

While use of an OSP to collect data would be akin to a grocery store using a contractor to order produce *direct from the farm*, use of arm's length intermediaries would be akin to the grocery store accessing produce through one or more *wholesalers*. The ADR would generally not be liable for the actions of the 'wholesaler'.[198] The 'wholesaler' may not just enable more rapid and efficient access to

[197] Data Republic submission, p. 9.
[198] Although arguably there may be exceptions to this if an intermediary does not obtain separate consents to collect or use data provided to the receiving ADR, instead relying upon disclosure.

a broader range of 'produce', they would be able to provide 'packaging' services of the raw produce (filtering and value adding of data).

The emergence of arm's length intermediaries will have positive and negative effects on competition (as will the emergence of OSPs for data collection and disclosure) which must be monitored. This model could remove the need to enter into separate outsourcing contracts with multiple collecting OSPs as well as avoid other complexities and inefficiencies with doing so.

An example of an arm's length intermediary is a 'data wallet' that a consumer has previously chosen to manage access to their data. When using an ADR service provider, the consumer would instead consent to them accessing the wallet provider. The data wallet might provide cleansed, filtered or enhanced data sets to ADRs in a manner or format preferable to sourcing raw data from the data holder directly. The data wallet might hold the data sourced from original data holders, or may merely manage access to those data holders. While the former could reduce the burden on data holders who will not need to complete every request for data themselves, the potential centralisation of a consumer's data means that risks of pooled data would have to be appropriately managed.

Reciprocity

Obligations for both data holders and data recipients should be calibrated to enable consumers to have a broad choice of the data that they can choose to share, and to encourage the growth of the CDR. These obligations should also avoid unduly discouraging participation by persons who can provide services to the benefit of consumers. As the Open Banking Review noted, a consumer-focused CDR should not prevent consumers from sharing data between trusted parties, nor should any obligations placed on ADRs extend the scope of the system by stealth.

Background to reciprocity in the Consumer Data Right

The Open Banking Review considered that in the interest of balancing obligations, an ADR should also be obliged to provide *equivalent* data to other ADRs in response to a direction from a customer. It contemplated that equivalent data could relate to sectors beyond banking. The adoption of reciprocity was to 'provide that those who wish to become accredited and receive designated data at a consumer's request must be willing to share equivalent data, in response to a consumer's request.'[199] This concept of equivalent data is intended to grow the scope of data available for consumers, and to ensure that those that join the system also contribute to the system, which is ultimately for the benefit of all consumers.

The CDR legislation incorporates a principle of reciprocity, allowing reciprocity arrangements to be put in place in relation to data of the kind specified in the sectoral designation. This means that distinctly different kinds of data to those already covered by the CDR cannot become subject to the CDR under reciprocity, until a normal sectoral assessment and ministerial designation process has been completed. On its own, this is a potential constraint on cross-sector data sharing through

[199] The Treasury,2019, *Consumer Data Right Overview* p. 4.

reciprocity, until further sectors have been designated.[200] For example, a non-bank lender ADR holding data covered by the banking sector designation could be required, with the customer's consent, to provide the same types of data as a data holder.[201] However, an established data-driven business that receives banking data under the CDR but does not itself hold any in scope banking-like data would not be obliged to share any consumer data they may hold.

Issues arising from limited cross-sector reciprocity

The Government has stated that the CDR is to ultimately apply economy-wide.[202] Cross-sector sharing of data between sectors is a key feature of CDR. As the CDR expands to cover more sectors, then cross-sector reciprocity in sharing data under the CDR will naturally increase, as data specified in the relevant designation instruments will be shared by accredited entities at consumers' request. However, during the initial phases of the CDR, there is an opportunity for some ADRs to enter the CDR, and then access data held by designated data holders without having to comply with a consumer's request to provide consumer related data they hold in return. Those able to benefit from this could include start-ups seeking to provide new products using CDR data. However, they may also include established and data-rich companies seeking to use the CDR to expand their service offering before the CDR applies directly to them. For example, businesses may compete with designated providers of financial services by combining data they obtain under the CDR with data they hold in relation to a customer's shopping patterns and product choices, their travel history or their web browsing history and social interactions.[203]

In its analysis of the market impacts of the dominant digital platforms, the Government's response to the Digital Platforms Inquiry, noted that consumer data:

> *is being created and collated at an unprecedented scale. The capacity to process this data is also improving, providing us with greater insights and information than ever before.*
>
> *While the benefits of digital services and technology are vast and will continue to grow, we must also be aware of, and respond appropriately to, the risks that are presented so that consumers and businesses have the confidence and capacity to engage in the digital world.*
>
> *These changing dynamics require new approaches to regulation.*[204]

From the consumer's perspective, determinations as to whether data relates to one sector or another may have little meaning. For example, information which the consumer shares about themselves may be the same in the banking, energy, telecommunication or other sectors. Given the purpose of reciprocity to empower consumers by giving them a means of requiring that data held for

[200] This constraint implied for the need for designation was recognised by the Open Banking Review, as was the difficulty in determining what is equivalent data for sectors not yet included in the CDR: Open Banking Review, p. 44.
[201] Section 56AJ of the CCA.
[202] The Treasury, *Consumer Data Right Overview,* p. iv.
[203] Deloitte submission, p. 44.
[204] The Treasury, 2019, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry,* p. 4.

them be shared, it is important that the implementation of reciprocity to data about a consumer or their transactions from a sector which is not yet included in the CDR should be clarified.

Impact of clarifying cross-sector reciprocity obligations

Consumers

The CDR enables a customer of a data holder to share their data with a trusted ADR in order for the consumer to receive a service. If an ADR holds data that would be useful for other CDR participants offering services, enabling earlier sharing of that data under reciprocal data holder obligations, with appropriate consents, would benefit their customers.

Where an ADR is able to get their customer a better deal by combining information accessed via the CDR with information relating to the customer held by the ADR, then it follows that the customer's original provider may also be able to offer a better deal if access to the ADR's information is available to them. Enabling customer information to flow in both directions, at the customer's discretion, opens up further possibilities for value to flow to consumers through competition within the CDR.

The Consumer Data Right ecosystem

The CDR is a data sharing ecosystem designed to allow consumers to derive the most value out of data they provide, one way this is achieved is by encouraging competition in the data economy. As the Institute of International Finance noted, 'Data gathered from the provision of one service has value in other markets, and increasingly so with more advanced data analytics based on artificial intelligence.'[205] Reciprocity obligations for all ADRs holding consumer data are one way of encouraging competition and fairness in the short term before all relevant sectors included in the CDR and the relevant CDR data is defined in designation instruments.

Sharing of 'equivalent' data

The Open Banking Review considered that the accreditation regulator should determine what constitutes equivalent data for persons seeking accreditation who are from outside of the already designated sectors. The Inquiry believes that this remains an important function to be performed. Materially enhanced data, and voluntary data sets, should be excluded from the scope of the equivalent data which is required to be shared at a consumer's request. A guide to the type of customer data the ADR may be obliged to provide is what data would be required for provision when their sector is covered by a sectoral assessment.

Relevant data standards would also need to be developed for new data sets which are determined to be equivalent data. Unless appropriate and relevant data standards are already in existence, or could be easily established from those already used in the relevant industry, this would slow down accreditation processes for affected firms. This could also divert government resources, potentially including those used for the rollout of prioritised designated sectors. Such work may however

[205] Carr B, Pujazon D & Urbiola P, 2018, *Reciprocity in Customer Data Sharing Frameworks*, Institute of International Finance (July 2018). https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf

provide the regulator with an understanding of what data sets exist in sectors eligible for future designation.

A requirement to comply with reciprocity obligations may encourage prospective ADRs to bypass the CDR in favour of less onerous data access methods, potentially undermining the CDR model before a sector is designated.[206] Such arrangements could also add to the compliance costs of new ADRs, as they will have to set up infrastructure for both the supply and receipt of data. To lessen the potential for these obligations to discourage new entrants to the CDR, exemptions should apply to smaller ADRs.[207] Allowing exemptions under a certain threshold may distort business activity when these thresholds are approached.

However, clarity in the application of reciprocity obligations may also encourage ADRs to participate in CDR, particularly if such participation is being withheld due to concerns that value-added data would be included.

As payment and action initiation capabilities are introduced to the CDR, the potential benefits of joining the CDR will increase. It will similarly increase as the CDR ecosystem develops and provides access to more data and markets for ADRs. Consequentially, any marginal deterrent effect caused by reciprocity obligations will decrease.

On balance, clear guidelines for implementation of reciprocity obligations, and measures to exempt smaller entities, should empower consumers to share more of their data during the early stages of the CDR rollout without excessive disruption to the accreditation process.

Recommendation 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.

Recommendation 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.

[206] AGL submission, p. 7.
[207] For example, the existing definition of a small proprietary company in the *Corporations Act 2001* or small business entity in the *Income Tax Assessment Act 1997* could be considered.

Recommendation 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.

Tiered accreditation

The unrestricted accreditation model

The Open Banking Review recommended a tiered risk-based accreditation model that accounts for the risks of data sets, ADR activities and existing risk mitigants. Tiered accreditation is directed at ensuring that the regulatory burden is proportionate to the risks being addressed, and to reduce undue barriers to entry by potential ADRs.

Currently the Rules only provide for a single tier of accreditation – 'unrestricted accreditation'. It is designed to be suitable for full access to all banking sector designated data sets and all operating models with their associated potentially high levels of risk.

While streamlined accreditation is allowed for banks participating in the CDR, this process does not involve compliance with a lower level of accreditation; it is a process for recognising the existing information security arrangements that banks are subject to under their sectoral regulation.

Benefits and costs of tiered accreditation

To encourage broad participation in the CDR, it remains desirable for the accreditation process to avoid requiring unnecessarily intensive or costly levels of accreditation. It follows that lower tiers of accreditation must be available to ADRs, where the risk of harm and potential levels of harm that given data sets or activities could cause is lower than others. Sectoral analysis, and in particular associated Privacy Impact Assessments, of both the banking and energy sectors have already revealed different risk profiles for consumer data held in different sectors or within a sector.

Newly introduced sectors, data sets, and different business models will carry unique risks that may make them suitable for different information security requirements. Aligning these requirements with unique levels of accreditation is one way of calibrating risk management across an increasingly complex ecosystem. Once tiers are established, there is greater potential to link these identified levels with recognised risk management and compliance regimes outside the CDR.

Excessive numbers of tiers would introduce undesirable levels of complexity and costs into the regime. Some estimates have placed a high financial cost on the process of seeking CDR accreditations. Lower tiers of accreditation would involve a reduced burden of time and money on the party seeking accreditation, both initially and ongoing.

If barriers to obtaining accreditation are reduced where appropriate, entities currently providing services using data accessed outside the CDR (for example, those sourcing data through screen scraping) should be incentivised to adopt the CDR regime, with attendant safety benefits for consumers. It will therefore reduce the overall risk of data misuse in the economy.

Tiering of obligations

The accreditation criteria must set out any minimum level of insurance coverage required by those eligible for lower tiers of accreditation, to provide assurance that losses from data breaches can be recovered. Allowing lower tiers of accreditation will also provide insurers greater clarity regarding the limitations of various users of the CDR, so insurers can match their coverage to the specific risks faced by an ADR.

A detailed segregation or delineation of the roles, responsibilities and protections required for each tier will also provide a clear scope for auditors to address when providing assurance services, such as what levels of information security safeguards are applicable.

The level of assurance (and associated costs of providing that assurance) for different tiers of accreditation may be adjusted by either lowering the obligations imposed under the tier or by relaxing the process for establishing compliance with those obligations. For example, lower tier ADRs may not need an independent auditor to provide an assurance report. Alternatives to this could be either the provision of an attestation statement, or a check by the CDR regulator that compliance reporting undertaken outside the CDR covers the necessary criteria.

Scaling obligations

Even within a given tier, accreditation requirements may be designed to scale with levels of risk or types of activity. This could involve an avoidance of prescriptive regulatory requirements in favour of principle-based regulation.

For example, an ADR that does not intend to connect directly to a data holder, but instead rely upon an accredited OSP for collection or an arm's length intermediary may not be required to pass the Conformance Test Suite requirements prior to accreditation. Irrespective of the tier of accreditation of such an ADR, the Register would need to record that they were not entitled to connect directly to a data holder.

Recommendation 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.

Basis and application of tiered accreditation

Risk of data sets

Particular data sets or data relating to an entire sector could be assessed as being of a higher or lower level of risk based on the likelihood and level of harm that may arise if there were to be unauthorised use or access to the data. In considering this harm, the regulator should consider factors including the degree of personal insight that may be revealed by the data. This consideration should take into account that seemingly innocuous data sets, when combined, may pose greater

risks than the sum of the risks associated with them individually.[208] Account balances or other summary data products are one set of data within a designated sector that could be considered a lower risk data set, as opposed to detailed transaction data for the same accounts.

Applying a limit to the CDR data an ADR can access at a particular accreditation level could stifle the development of new products. If the cost of accreditation required to access higher risk data sets is prohibitive then the use of these riskier data sets outside the CDR system may be encouraged.

Risk of activities undertaken

Another method of assessing risk from data access could be based on the way an accredited party seeks to receive, use or hold consumer data.

Not all ADRs seek to hold data after providing a service to their customer – data storage and security requirements may be less relevant to these data recipients. The use of specialist service providers in the data supply chain may result in ADRs carrying out less risky activities resulting in a lower tier of accreditation being proportionate with that residual risk.

One risk of an approach that recognises ways of using and retaining data is that by calibrating accreditation specific to certain data supply chain models, alternative models may be prevented from emerging in the regulated ecosystem should the trade-offs discourage an extension of capability.

Various submissions have called for those performing action initiation functions to receive the highest tier of accreditation as a default requirement. While unrestricted access for payment initiation may warrant this, the level of accreditation for action initiation should be set with regard to the risks associated with the subject matter of the action initiation and the activities that the applicant for accreditation is undertaking.

For example, a limited ability to move funds between a customer's own accounts would pose significantly less risk to consumers than the ability to transfer funds to a third party account.

Detailed design of action initiation (including payment initiation) should identify mechanisms to provide consumers with control over the level of risk to which they are exposing themselves. For example, the potential for action initiation API settings to restrict certain actions, such as payment amount limits or length of authorisation.

An assessment of the adequacy of information security requirements for different types of action initiation, including payment initiation, should be determined by rigorous information security assessments with the input of interested stakeholders. Input from regulators, including the RBA and APRA, would be required to assess the risks posed by payment initiation capability.[209]

---

[208] Australian Computer Society, 2019, Privacy Preserving Data Sharing Frameworks: http://www.acs.org.au/content/dam/acs/acs-publications/ACS%20Directed%20Ideation%20Report%20Aug%2019.pdf

[209] National Australia Bank submission, p. 9.

Recommendation 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.

Voluntary data sets

Required and voluntary data sets

Under the current Rules, CDR data sets that are not required to be disclosed by data holders are referred to as voluntary data sets. The data holder is required to obtain authorisation from the CDR consumer if they wish to disclose voluntary CDR consumer data, as they normally would with required CDR consumer data, otherwise referred to as mandatory CDR data. The protections and benefits applicable to required CDR data, such as Privacy Safeguards, also apply to voluntary consumer data sets. As with mandatory data, standards for voluntary data sets must be published in an open source environment.

A data holder is entitled to charge for the provision of voluntary data if requested, and the data holder must indicate in its CDR policy whether it accepts requests for voluntary product data or voluntary consumer data and whether it charges fees for disclosure of such data. When arranging authorisation to disclose voluntary data, the data holder must set out any fees they intend to charge.

All transfers between ADRs or from an ADR to persons outside of the regime (once either of these are permitted by the rules) must be voluntary. The regime only permits the mandating of disclosure by data holders in relation to data explicitly set out in a sectoral designation instrument. Disclosure of data derived from those types specified in the instrument likewise can only be permitted, and cannot be required by the regime.

The more familiar the CDR brand becomes in the Australian data economy, the more consumers will expect APIs to operate within the CDR framework. To generate this familiarity, data holders and data recipients should be able to conduct their business flexibly within the regulated CDR environment by utilising a growing range of data sources. If the CDR provides a safe environment for consumers and APIs to share mandatory data, trust and familiarity in the CDR generated using that data will accrue to those using the CDR to offer services using voluntary data sets.

Benefits of organic growth in voluntary data sets

If more data sets could be moved between businesses and customers as CDR data sets using the CDR network rather than outside it, consumers could be better served by the information security, liability and privacy protections built into the CDR framework. Businesses would be able to better leverage CDR IT and operational investments they have been required (or otherwise chosen) to build. The CDR liability framework would also be available to manage responsibility for businesses seeking to introduce new products and data sharing methods using CDR data sets not mandated. Stronger

protections for consumers relative to other data transfer methods will increase confidence in CDR data portability, and encourage participation.

Closer alignment of standards for voluntary data sets and required data sets could increase interoperability, providing opportunities for network effects and innovation in services offered within the CDR ecosystem. There is potential for the CDR to provide a 'baseline' of standards and infrastructure, from which expansions and innovations can be developed voluntarily. Where appropriate, these can be formally incorporated into the CDR.[210] Generally, if a particular data set has not been designated for sharing, and could be of use to CDR consumers, then it could be in the interests of consumers to make it accessible within the regulated CDR environment.

Potential voluntary data sets

In some industries there may be a desire to share data using the CDR system.[211] These industries could be suitable candidates for any process that allows voluntary data to be introduced to the CDR. Allowing the use of voluntary consumer and product data sets outside the scope of existing designated sectors would not prevent any new data from being mandated for sharing by data holders if it eventually falls under a designation.

Categories of data that currently are, or could be, voluntary CDR data sets include:

- data derived from data specified in sectoral designations
- data falling outside a sectoral designation
- data included in the data specified in sectoral designations but not mandated
- data mandated for disclosure, but packaged differently to the mandatory data payload standards, and
- data mandated for disclosure, but on terms that exceed mandated requirements.

These categories cover a broad range of possible data sets including:

- data already provided by APIs outside the CDR
- insights data that could inform decision-making for consumer switching
- materially enhanced data such as analysis or aggregation of a customer's income and expenses, and
- internet-of-things data where information held and transmitted by a device may offer a benefit to consumers.

The opportunity for data holders to charge for the provision of voluntary data creates a commercial incentive for both data holders and data recipients to improve the performance of their APIs beyond the mandated functionality. These are sometimes called 'Premium APIs'. Encouraging Premium APIs would be consistent with the principle that CDR functionality does not lag behind other international

[210] FinTech Australia submission, p. 9.
[211] Victorian Automobile Chamber of Commerce submission, p. 4.

data sharing regimes. The UK Open Banking regime is one example of a system that allows premium APIs.

There is a question about the scope of data that is suitable for inclusion in the CDR by data holders and ADRs. Given the process of sectoral designation is considering and introducing sectors gradually, it is possible that introducing data outside the designated sectors could undermine the strategic approach to rolling out new sectors and designing standards for APIs. When a sector is designated, the sectoral assessment assesses the risks of including some data sets and excludes those that pose particular risks, such as personal information that identifies an individual. Some sectors may not be suitable for designation, for example, those where related consumer data is of a highly personal nature. Data from such sectors would therefore not be suitable for voluntary inclusion. In addition, the combination of designated and non-designated data could lead to adverse outcomes if controls over new voluntary data sets do not complement existing processes for managing the introduction of CDR data.

The suitability of a proposed data set from within a designated sector could be assessed by the CDR regulator, based on existing analysis of that sector to support the designation instrument. Given the use of the sectoral designation process to identify suitable data, determining the suitability of data outside the designated sectors would require a separate process.

Means of developing standards for voluntary data

To facilitate the inclusion of voluntary data, both inside and outside designated sectors, barriers to entry would have to be reduced from the current state. A new process that provides sufficient assurance regarding the suitability of these new data sets, without creating a compliance burden, will encourage users of these data sets to operate inside the CDR ecosystem.

The development of standards for voluntary data sets could be managed with varying levels of flexibility regarding their consistency with existing CDR standards available in the public domain. The higher the level of government control over new CDR data sets, the more consistent the standards will be with existing data sets and the strategic direction of the CDR. Allowing a more organic approach to introducing voluntary data sets will provide flexibility for participants, but could reduce consistency with existing data sets and consumer experiences within the CDR environment.

Government-led approach

The DSB could lead the process of developing CDR standards for data sets that industry participants, or even individual firms, wish to introduce to the CDR ecosystem as voluntary payloads. Such a process may provide greater control over the setting of voluntary standards to ensure interoperability and security, but would draw resources away from the core work of the DSB.

A fee-for-service model could be one way for government to resource the task of designing standards for voluntary data sets. Allowing the Government to recover costs for these services could enable the scaling up of efforts, although timely resourcing may be difficult to manage if demand for such services is inconsistent and difficult to plan.

Industry-led data provision

Government-led consideration, design and testing of data sets undertaken during the creation of the initial phase of the CDR has allowed strong safeguards and consistency of standards to be built into the existing data sets authorised for use. This has also provided an open source library of standards industry participants can reference when developing and maintaining their own standards. Where a powerful use case or commercial incentive exists to encourage the inclusion of a voluntary data set in the CDR, industry can leverage their existing knowledge of CDR standards or external API design to develop their own standards.

Allowing industry-designed standards into the ecosystem could diminish the benefits of the government-led approach, ultimately undermining confidence in the CDR system. To protect against such risks clear guidelines and criteria would need to identify what is inappropriate for inclusion in the CDR, what features are essential to enable interoperability, and allow the opportunity for industry to engage with government when seeking to introduce new data sets to the CDR.

Bespoke proprietary approach

Similar to the industry-led approach, individual firms could develop their own standards for data they wish to use under the CDR framework. Allowing individual firms to use the CDR framework to share data would increase the scope of data and related products available to consumers using the CDR. As with industry-led standards, allowing bespoke standards design for these data sets could impact on the design consistency and strategic benefits of a government-led approach where interoperability and consistency are given a higher priority.

If bespoke data sets were allowed to be classified as CDR data, they would be automatically subject to the consumer and liability protections covering CDR data. Standards for these data sets would also be published in an open source environment, which may reduce any competitive advantage a firm is seeking to gain by introducing data to the CDR alone. A means of disallowing unsuitable data would be required to prevent bespoke data sets from undermining the safeguards built into the existing processes for introducing CDR data.

Alternatively, bespoke data sets could be distinguished as separate to CDR data, and simply use the CDR 'rails' without being subject to the protections and scrutiny covering CDR data. This could allow transmission over the CDR rails with fewer barriers to entry, and allow new data sets to be introduced without compulsory publishing of standards. Even if clearly distinguished from CDR data, allowing bespoke data sets on the CDR rails would dilute the protections provided to consumers under the CDR, to the detriment of the overall system on balance.

Role of the Data Standards Chair in developing standards

Under the CDR regime, the Data Standards Chair (DSC) is responsible for making data standards for voluntary data sets, in compliance with the Rules. Currently the DSB advises the DSC in this function. However, the current legislative framework does not make it compulsory for the DSC to only recognise standards developed by the DSB. This opens up the possibility that standards for new voluntary data sets could be developed and maintained outside the DSB by industry participants and recognised by the DSC.

Industry participants developing their own standards may choose to seek DSB advice on whether these standards are sufficiently consistent or interoperable with existing CDR standards. Clear guidelines and processes for developing such standards, including how and when to engage with the DSB, would assist industry participants to have confidence in the design of their developed standards. Where the suitability of the data is questionable, the DSC should have recourse to consult the CDR regulator for advice.

Means of promoting voluntary data standards

Standards for CDR data sets are already publicly available. As new sectors are designated, these standards will become more widely understood by those transferring data within the ecosystem. To achieve organic growth in the provision of data sets available in the CDR system, the mechanism to introduce these data sets to the CDR must enable a level of innovation and speed to market sufficient to compete with offerings across the entire digital economy.

A process enabling an industry to develop its own standards would encourage those seeking to leverage the CDR to compete effectively in the data economy. One approach could be to allow a set of standards for a new voluntary data set to be notified to the DSC, with the DSC then having the opportunity to disallow these data sets within a set period, if they are found to be unacceptable based on specified criteria, seeking input from the CDR regulators where relevant. A process where indefinite delays are allowed could discourage CDR participants from introducing voluntary data where commercial outcomes are time sensitive, or where services using the proposed data are competing with those offered outside the CDR.

To enable industry to adopt the role of a standards designer, clear guidelines and principles must be made available to provide clarity to participants considering the allocation of resources towards this process. Such guidelines could include:

- a process for engagement with the DSB should clarification on specific matters be sought
- any existing minimum standards, either domestic or international, that have to be met
- requirements to maintain these standards to an acceptable level as standards develop
- general limitations for acceptable CDR data sets, and
- principles for defining the risk profile of data sets, including whether handling of particular data would be limited to parties with specific levels of accreditation.

Responsibility for maintaining voluntary standards should rest primarily with the creators of these standards. Maintenance of these standards will need to be monitored by industry participants and the DSB, with the DSC empowered to notify participants and then disallow standards previously introduced by industry that have been allowed to fall behind an acceptable level.

Where industry feels less confident leading the design of their own standards, perhaps due to a lack of data economy expertise, it may still be desirable to address barriers preventing these data sets from being introduced to the CDR. An option where a new voluntary data set is proposed to the DSB, who can then charge industry participants for the service of designing standards, should also be

considered. Allowing this option would enable the DSB to provide a more consistent approach to standards development if they are chosen to perform the design function, and would prevent a situation where an industry or individual firm invests resources designing standards that may be deemed unsuitable by the DSC.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Recommendation 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.

Additional consent measures

The ability and willingness for CDR participants to create and use consent processes that are explicit and easy for consumers to understand will be important for the CDR to succeed. Consents and authorisations (which are discussed further below) outline the terms on which consumers are allowing data holders and accredited persons to act and interact through the CDR. Due to the importance of having consistency across consent processes, a desire was expressed in submissions for greater clarity in how consents should be worded and structured.[212]

The Inquiry has examined a number of additional measures that could increase consistency in consent terminology and bolster comprehension. The Inquiry finds that there is greatest scope to increase standardisation in usage consents, with authorisations and access consents already being highly standardised. The two potential measures most focused on are a dictionary of key consent terms, and a process for interest groups to endorse consents. The Inquiry also recommends that the consent process continue to be refined and updated based on the findings of ongoing consumer experience testing.

Consent Processes

The Consumer Data Right is built around explicit, informed consents. This empowers consumers to choose the terms on which they want to engage with the CDR. There are currently three types of consents: access consents, usage consents and authorisations.

- **Access consents** communicate to the accredited person the data sets and actions that the consumer is allowing them to access.
- **Usage consents** communicate to the accredited person the purposes for which the consumer agrees to their data being used and actions being initiated on their behalf.[213]
- **Authorisations** communicate to a data holder what data sets the consumer has authorised them to share, and what actions they are authorising be initiated on their behalf.

Table 6.1: Equivalent data sharing and action initiation terminology

	Accredited Person		Data Holder
	Access Consents	Usage Consents	Authorisations
Data Sharing	Consents to collect CDR data	Consents to use data collected	Authorisation to disclose CDR data
Action Initiation	Consent to initiate CDR actions	Purpose for which instructions may be sent	Authorisation to accept CDR instruction

[212] Tyro submission, p. 5, Cuscal submission, p. 3, Prospa submission, p. 3.

[213] Though these consents must currently be provided, changes to this requirement are being considered in proposed amendments to the Rules published for consultation on 1 October 2020. These changes would allow a consumer to more easily add or remove new purposes relating to CDR data sets and CDR action classes for which the accredited person already has consent to access.

The Rules currently require that consents are voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[214] Additionally, the Standards' consumer experience (CX) Principles seek to ensure that CDR system is consumer-centric, accessible and inclusive, comprehensible, simple and empowering, and that consents are current.[215] These objectives seek to ensure that the CDR enables consumers to act with independence, while still providing them with protections entrenched in the system.

Standardising consents

For the CDR to be effective, consumers must feel comfortable and confident engaging with the consent process. If consumers do not understand this process, they will either not engage with the CDR or will provide consents without properly understanding the implications of their actions. Accredited persons must also be confident about their requirements when designing consent processes. If accredited persons misunderstand these requirements, then they may unintentionally put consumers at risk of having data they have shared used in a way that does not align with their wishes. This would then put the accredited persons themselves at risk of regulatory consequences.

Increasing consistency in consent terminology would allow consumers to become more aware of how they are being asked to share data. This improves the quality of their consents and reduces the risk that their consent is not genuine or is inadequately informed. Additionally, increasing standardisation and consistency in terminology also allows accredited persons to be more confident that they are acting within the scope of their customer's consent.

> *A standardised consent taxonomy has the potential to reduce complexity and streamline consent requirements for participants and consumers under an expanded CDR regime, but must be balanced against the need to protect consumers, particularly in relation to their most sensitive information.*[216]

To assist both consumers and accredited persons, it has been suggested that further guidance around consent terminology be provided.

The case for government action

The current legislative framework already outlines what must be included in the consent process and what consequences there may be for not complying with these requirements. Without further government measures, it is expected that consent terminology will naturally emerge, and that a private market will form to assist accredited persons to meet their compliance obligations.

Despite this, a process that naturally emerges may not be beneficial to industry or consumers. For instance, an overly strong focus on avoiding non-compliance may result in consents being drafted overly cautiously and providing explanations which, though technically correct, are inaccessible to most consumers. This would leave participants confused and disengaged, rather than empowered. Consent terminology entirely developed by market forces would also likely diverge across industry

[214] Rule 4.9 or Part 1 of the Rules.
[215] Consumer Data Standards v1.5.1.
[216] Deloitte submission, p. 21.

boundaries. Specific industry terminology and standards would colour the consent process within that industry, reducing the efficacy of the CDR as an economy-wide regime.

However, further increasing government involvement through additional consent measures may introduce its own risks. Further regulation may make the CDR system overly prescriptive and could impose additional burdens on potential participants. Overly prescriptive consent language may also restrict innovation and reduce the number of viable use cases permitted under the CDR, reducing the attractiveness of the regime compared to unregulated alternatives.

The Government is in a unique position to create industry standardisation through the potential use of the Rules. Accredited persons can only be confident that consent processes created using supplementary standardisation guidelines will be recognised as being compliant if these guidelines are recognised by the Rules.[217] If this step of recognising certain standardisation practices as legally binding is not taken, then the risk to accredited persons of using any supplementary resources would remain, rendering them substantially less effective. Therefore, the Government must consider how best to give legal effect to desirable standardisation practices. The Law Institute of Victoria stated the following:

> *As consent must be unambiguous and cannot be inferred, it is important that clear guidance is provided under the law and regulations regarding what is acceptable consent. … To promote innovation and clarity for third party providers and the customers, the rules regarding consent should be made unequivocally clear.*[218]

Having the Government work with industry, consumer advocates and other interest groups to consider a range of consent measures would best assist data recipients in meeting the consent objectives set out in the Rules, while maintaining the system's overall vision for a vibrant and innovative data ecosystem.

The DSB is best suited to lead future work designing additional consent measures as part of its CX work stream. The findings from the DSB's CX work has been included in both the CX Standards and CX Guidelines, informing current best practice regarding CDR consent processes. The DSB's function should be expanded to more explicitly include ongoing consent research, both through independent research and through engagement with industry, interest groups, and wider government. The CDR rule maker and regulators should also work closely with the DSB to assist in evaluating standardisation practices and incorporating these into the Rules as appropriate.

Recommendation 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.

[217] Alternately, this recognition ability could be delegated to the Standards.
[218] Law Institute of Victoria submission, p. 5.

Evaluating consent measures

A wide number of competing positions were put to the Inquiry relating to further consent guidance. The diverse variety of stances make clear the importance of having a consistent set of principles to help guide decisions when considering potential consent measures. These principles should include consideration of how a proposed measure is expected to improve the CDR experience for consumers and participants, and whether it will likely impose additional costs on data holders or accredited persons.

Two messages were made clear through the submissions to the Inquiry. For consumers, additional consent measures should increase their ability to engage with the consent process by providing them with a more familiar experience and reducing the risk of consent fatigue. For data holders and accredited persons, additional consent measures should increase clarity as to their obligations, without restricting their ability to innovate and offer attractive products to consumers.

A large number of submissions raised the need for greater clarity surrounding acceptable consents so that consumers can clearly identify what specific consents entail. This would allow consumers to identify when an action contrary to this consent has occurred. On this, the Consumer Policy Research Centre (CPRC) stated:

> *We support greater consideration of a consent taxonomy and associated use cases that would provide consumers (as well as businesses and regulators) with a clear reference point for what their consents entail in real terms, and a consistent benchmark for evaluating and taking action where breaches occur.*[219]

However, a considerable concern to many fintechs and other potential accredited persons was that increasing rigidity in the consent process would hamper their ability to innovate and lead to poor consumer experience outcomes. This would subsequently reduce the ability for these data-driven businesses to create products that would benefit consumers.

> *Beyond the standardisation of the language to describe Data Clusters, as is already provided by the Data Standards Body's CX Guidelines, additional formalisation of consent taxonomy could stifle creativity, and the ability for firms to optimise the way consent is captured as the market grows and technology develops.*[220]

Others who were more supportive of greater clarity being provided surrounding the consent process were also clear about the need for broad industry collaboration in developing solutions. This was seen as necessary to ensure that the costs associated with any developments did not unreasonably deter participants of all sizes. In their submission, MYOB stated:

> *We support industry cooperation noting that it should include large and small providers. This would reflect outcomes that ensure costs associated with implementing compliance outcomes are not exclusionary to smaller players seeking to participate in opportunities as*

[219] Consumer Policy Research Centre submission, p. 4.
[220] Truelayer submission, p. 7.

> *a result of CDR broadening, which ultimately hampers innovation and employment creation.*[221]

In promoting the CDR as an economy-wide regime, there is also a need to consider the appropriateness of applying certain consent requirements, such as standardised language, indiscriminately to different sectors. While this may be appropriate for some measures, there are other times where a sector-specific approach may be more appropriate. The Australian Finance Industry Association stated that:

> *It is important that when developing the 'consent taxonomy' that each sector is considered individually, taking into consideration the nature, scale, complexity, and size of the various entities. A blanket approach across all participants would not be appropriate, and would likely lead to over prescription, causing unnecessary compliance complexities and costs and impeding competition, innovation, customer choice and accessibility. Industry guidelines that are tailored for each sector would ensure terminology and processes are aligned with existing practices in each sector (which in turn would maximise customer participation).*[222]

The Inquiry has attempted to synthesise the various considerations about further consent measures raised during consultation in a set of clear principles. These principles are set out on the following page:

[221] MYOB submission, p. 3.
[222] Australia Finance Industry Association submission, p. 3.

Principle 1: Additional consent measures should bolster consumer capability when engaging with the CDR.

A successful consent measure should increase a consumer's understanding about the terms of a consent without overloading them with information. It should make it easier for consumers to engage with the CDR system without compromising the validity of their consent and should be guided by consumer research.

Principle 2: Additional consent measures should make it easier for accredited persons and data holders to engage with the CDR, without constraining their ability to innovate.

A successful consent measure should make it easier for accredited persons and data holders to build their consent processes, but should not restrict or discourage them from innovating.

Principle 3: The method of implementing additional consent measures should be considered on a case-by-case basis.

Some measures may be best introduced through the Rules or Standards, giving them legal effect, while others may be better incorporated into the CX Guidelines.

Principle 4: Additional consent measures should be considered within an economy-wide CDR regime.

Some consent measures will likely be applicable to specific sectors, whereas others will be better applied to the CDR regime as a whole. It is important that the potential impacts of narrowing or broadening a measure are adequately considered.

Principle 5: Accredited persons and data holders should not be made to adhere to additional consent measures that would require them to bear unreasonable costs.

With the original consent process having already been determined, additional consent measures should help lower the cost of compliance for data holders and accredited persons. They should not require costly technical builds, or additional compliance obligations.

Principle 6: Additional consent measures should be designed with the protection of vulnerable consumers in mind.

Vulnerable consumers should include those traditionally considered vulnerable, as well as those who are vulnerable in the context of the CDR – for example those with lower levels of digital and data literacy.

Recommended additional consent measures

The Inquiry found that access consents and authorisations are already highly standardised through the existing Rules, Standards and CX Guidelines. Terminology used in access consents and authorisations are expected to be largely limited to the description of data sets and action classes, which are to be outlined in the CX Standards' Data Language Standards. Further work standardising these consents would likely not result in significant gains for data holders, accredited persons or consumers.

The Inquiry recommends that further consent measures focus on increasing clarity in usage consents. Specifically, the Inquiry recommends that a dictionary of standard CDR terms and use cases be developed and a method of industry certification be encouraged to assist consumers and accredited persons understand consents. Additionally, the Inquiry supports the DSB continuing to research what level of detail in the consent process leads to the greatest consumer empowerment and understanding.

Consumer Data Right dictionary

Ensuring that key words in CDR consent processes are used in a consistent way is important to increasing participant and consumer understanding, as per Principles 1 and 2. While a CDR consent dictionary would be most beneficial in defining key use cases and purposes, care should be taken to mitigate the potential for innovation to be harmed.

A dictionary that outlines key CDR use cases and purposes would help participants understand what a data recipient could reasonably do within the context of a given consent. There is currently limited guidance about how the wording of consents will be considered by regulators, leading to uncertainty. Without boundaries outlining what use cases can be understood as being included in specific terms, there is no guarantee that the services offered by accredited persons using identical consents will be in anyway comparable. A dictionary of key terms could help reduce this uncertainty by setting some boundaries on what a term can allow.

The dangers of creating a dictionary of consent terms however, is that it becomes too restrictive and impedes innovation. This would be contrary to Principle 2. This would be the case for a dictionary of use cases which disallowed any terms not explicitly listed. Not only would this dramatically limit the benefits to consumers, it would encourage participants to operate in the unregulated space outside the CDR system.

The Inquiry recommends a non-exhaustive approach be adopted. A dictionary should be created that defines key terms used in CDR consents. This should include definitions of words specific to the regime, as well as definitions for other terms commonly used in consents, such as standard use cases and purposes. These definitions should state in plain English what is understood as permitted or disallowed under a term, and should be written to be clear to consumers.

Accredited persons should not be limited to using listed terms when drafting consents. However, if they use a listed term, it should be taken as having the meaning in the CDR dictionary. An accredited person should be understood to have supplied the listed definition in full, even if they have not set

out the definition in full. If an intended use case or purpose expands on a listed term, then extra information should be provided to the consumer in the consent to explain these elements.

Additionally, CDR dictionary entries should be drafted in a sufficiently formulaic way so to enable the contents of CDR consents to be more readily codified. This will increase the sophistication with which consent data is interpreted within the CDR system. Tyro's submission touched on the importance of this when encouraging that 'consideration be given to the development of standardised interfaces and language around consent to foster better tooling for consumer consent management'.[223] Enabling the codification of consent information will also assist in driving innovation.[224]

This consent dictionary seeks to enable accredited persons to create consents that are easily understood by consumers without being overly prescriptive. Those using dictionary terms will be advantaged due to increased regulatory certainty and consumer experiences that are more aligned with industry norms. Restrictions to innovation will be minimal, as those offering new or distinct services will still be able to participate in the CDR.

This dictionary should be included as part of the CX Standards' Data Language Standards. Two illustrative examples demonstrating the structuring of potential entries to the dictionary are below. The wording of these examples has been drafted to be consistent with the rest of the CX Standards.

Box 6.1 – Consent dictionary – Illustrative use case

Personal Finance Manager

Definition

If an ADR uses the term *Personal Finance Manager*, it **MUST** have the following meaning:

> *A service that will analyse income and expenses to help manage finances*

A *Personal Finance Manager* **MUST NOT** inherently include *Direct Marketing*, a *Comparison Service*, or a *Switching Service*, though an ADR **MAY** use these terms additionally.

Consent Structure

ADRs **SHOULD** use the following structure for their consent statement:

> *We need to [collect and use your financial data] to provide you with a [Personal Finance Manager]*

An explanatory statement for a *Personal Finance Manager* **SHOULD** be phrased as follows:

> *We will analyse your income and expenses to help you manage your finances*

[223] Tyro submission, p. 4.
[224] The accessibility of consent information is discussed more in the External Consent Management section.

Comparison Service

Definition

If an ADR uses the term *Comparison Service*, it **MUST** have one of the following meanings:

1. *A service that will analyse bills and suggest more suitable providers*
2. *A service that will analyse cost and usage patterns to identify better deals*

A *Comparison Service* **MUST NOT** inherently include *Direct Marketing* or a *Switching Service*, though an ADR **MAY** use these terms additionally.

Consent Structure

ADRs **SHOULD** use the following structure for their consent statement:

> *We need to [collect and use your financial and/or energy data] to provide you with a [Comparison Service]*

An explanatory statement for a *Comparison Service* **SHOULD** be phrased as follows:

1. *We will analyse your bills and suggest more suitable providers*
2. *We will analyse cost and usage patterns to identify better deals*

The CDR dictionary should be informed by consultation with industry, consumer advocates and the relevant regulators, and should be regularly updated. CDR participants should be able to request that the DSB review terms or add terms. For this dictionary to have the intended legal effect, the DSB should work with the CDR rule maker to consider methods to appropriately incorporate it within the Rules. CDR regulators should consider this dictionary when forming a view about whether an accredited person has engaged in misleading conduct. In line with principle 6, this dictionary should be drafted to be accessible to those with limited digital and data literacy. Depending on the success of this dictionary, consideration should be given to making it available in multiple languages.

Recommendation 6.19 – Consumer Data Right dictionary

The Data Standard 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.

Industry recommended and endorsed consents

A second consent measure that the Inquiry recommends be explored is the ability for representative bodies such as industry groups and consumer interest groups to endorse or recommend consents. Interested industry and consumer bodies do this by creating standardised consents to be used by accredited persons for specific use cases, or by reviewing and endorsing bespoke consents created

by accredited persons. If consumer experience research indicates that this would benefit consumers in understanding consents, then data recipients who use endorsed consents should be permitted to include badges or other symbols of endorsement.

Enabling an accredited person to demonstrate to consumers that they are using a consent process that is either industry recommended or has been verified by a trusted third party may allow consumers to feel more confident about the relationship that they are entering into with the accredited person. This could potentially also make it easier for accredited persons to be confident they have met their obligations to provide consent processes that adhere to the Rules and Standards. As per principles 2 and 5, this measure should not limit the scope for innovation or put unreasonable costs on data recipients as accredited persons would not be required to use industry recommended or endorsed consents.

Clear communication of accountability would be necessary under this measure to prevent any uncertainty about who is responsible should an accredited person using a recommended or endorsed consent operate outside of the scope of that consent. The Inquiry recommends that liability in such cases should lie with the accredited person, as it is their responsibility to abide by their consent obligations. Third parties who endorse consents would also be independently incentivised to ensure parties who use those consents do so properly. If an accredited person using an endorsed consent is found to have breached this consent, then it could reflect poorly on the endorsing body by extension. As the CDR program develops, consumers will become more able to recognise trusted consents through recognition of trusted consent endorsers.

Though accredited persons are already able to use consents developed by third parties and feature endorsements of consents under the current Rules and Standards, making this allowance explicit would assist in promoting industry confidence in having their consents endorsed. The Rules should also outline the liability for using condensed consents.

Recommendation 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.

Further potential consent measures

The Inquiry acknowledges that the consents process could be further refined in a number of ways, and recommends that the DSB's CX work engage with industry, consumer groups and regulators to consider when further developments should be pursued.

Condensed consents

There are presently strict requirements on what must be included in a consent process. The DSB and CDR rule maker should continue to assess what level of detail in the consent process achieves the highest quality of consent. Incorporating too much information in a CDR consent process can have a

negative impact on consumer engagement by causing consumers to become fatigued and overwhelmed, contravening principle 1. This can then lead to consumers clicking through consent screens without engaging with the content or disengaging with the system entirely. Processes aimed at maintaining a high quality of consent while reducing the amount of information provided in consent screens have been a focus of recent CX research. For instance, in a recent report the DSB looked at how to '[p]rovide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent)'.[225]

Depending on the results of consumer research, it may be appropriate to make a number of changes to the CDR consent process to assist consumers engaging with the CDR system. Options aimed at 'decluttering' consent screens by (where appropriate) moving information from the consent process to other sources, such as the consent receipt, may assist in reducing consent fatigue and potentially lead to more informed consents. The CDR dictionary is another example of such a measure. Any such changes should be the result of consumer testing and engagement with industry, consumer advocates and regulators, and should reflect the principles outlined in this review. The ongoing cooperation of the CDR rule maker will also be required to enable the Rules to reflect any changes where appropriate.

Fine-grained authorisations

Consideration should be given to the benefits of enabling fine-grained authorisations in CDR data sharing arrangements. In the data sharing context, a fine-grained authorisation would enable a consumer to elect that only a specified subset of CDR data actually be shared with an accredited data recipient, rather than the entire data set. This would give consumers greater control over the data they choose to share, and enable accredited persons to request only the data necessary for a specific purpose.

Increasing the level of granularity able to be provided in a data sharing authorisation increases the level of specificity that a data holder needs to be able to accommodate. Requiring that data holders provide this functionality would further increase costs of participating in the system, potentially contradicting principle 5. In spite of the potential costs, the Inquiry received some support surrounding this from data holders. In recognising opportunities for further development in this area, the Commonwealth Bank of Australia identified benefits in:

> *Further enhancements to consent standards (including a consent taxonomy) to introduce optionality for more granular and specific consent. This will provide additional control to consumers over what data they share with ADRs by enabling consumers to only share what is necessary. For example, consumers could specify or filter what data is shared on an account (e.g. only sharing withdrawal transactions on an account, only sharing their postcode rather than their full address, or only sharing transactions that occurred within a particular date range).*[226]

[225] Data Standards Body, 2020, *Consumer Experience Research Phase 3: Round 4 and 5*, p. 12: https://consumerdatastandards.gov.au/wp-content/uploads/2020/07/CX-Report-_-Phase-3-_-Rounds4-and-5.pdf.
[226] Commonwealth Bank of Australia submission, p. 14.

Though not all data holders may want to offer such functionality, processes should be put in place to allow those who do want to offer fine-grained authorisation to do so in a consistent way.

Fine-grained authorisation functionality should be enabled on a voluntary basis at the data holder's discretion. The DSB and CDR ruler maker should work with data holders to assist in the creation of standards and amendment to the Rules to allow fine-grained authorisations to be introduced as seamlessly as possible.[227]

Combined data sets for standard purposes

As a possible extension to the CDR dictionary, consideration should be given to enabling access consents and authorisations that would allow a consumer to share all CDR data required for a standard use case through a single authorisation.

Enabling this could increase the ease with which consumers can provide access consents and authorisations with a general level of certainty that the data requested is reasonable for the service that they are receiving. This could also help limit the amount of unnecessary data transferred, as well as reduce complexity for consumers when reviewing their CDR data sharing arrangements. Should consumer experience research verify these assertions then this measure would align with principle 1.

This could be achieved by creating new use case driven CDR data sets that combine existing CDR data to contain all the relevant information for delivering a standard use case. In line with principle 5, data holders should be able to offer these data sets on a voluntary basis and should be able to charge for their usage.

The development of use case specific data sets would only be beneficial if accredited persons want to use these data sets, and data holders are willing to provide them. The DSB should therefore gauge the level of desire from industry and consumer advocates for the creation of combined data sets for standard purposes when developing the CDR dictionary.

External consent management

Consents and authorisations outline the terms on which a consumer agrees to accredited persons and data holders interacting under the CDR. It is necessary that it is simple and convenient for consumers to view and manage these consents and authorisations. This section considers ways to increase consumer control in the CDR by enabling a consumer to access all of their consents and authorisations in a single location of their choice.

This section first outlines the current measures in place to help consumers keep track of their consents and authorisations. It then highlights why these measures may prove insufficient as the

[227] Intermediaries should also be encouraged to play a role in offering fine-grained data transfers. For instance, an accredited data recipient should be able to collect raw CDR data and then share a filtered version of this data with other ADRs as a voluntary data set at the consumer's direction. Similarly to a data holder offering options for fine-grained consent, such a business would give the consumer greater control over what data they choose to share. However, such a model would not put any additional imposition on data holders.

CDR continues to develop. The section then considers what would be required for external consent management services to be made possible within the CDR ecosystem.

Different kinds of Consumer Data Right consents

The CDR is built around consumer consent. When a consumer requests that a good or service be provided to them through the CDR, they are required to go through consent and authorisation processes to inform them of the arrangement they are consenting to and the disclosure or actions they are authorising. This requires them to agree to clear, concise terms set out by the accredited person and data holder.

When a consumer enters into an initial arrangement using the CDR, they give an access consent and usage consent to the accredited person, and an authorisation to the data holder. Only a usage consent contains information about the purpose for which the consumer has engaged the accredited person, meaning they do not share this information with the data holder. As consumers build relations with more accredited persons, they will create more consents and authorisations. As demonstrated in the example below, this can lead to the number of consents and authorisations that the consumer will be required to manage quickly growing as they engage with more data holders and accredited persons.

Box 6.2 – A map of consumer consents

A consumer has a relationship with three accredited persons – a banking account aggregator, a comparison website, and an automatic billing solution.

The banking account aggregator has consent to access and display information from the consumer's three banks in a single location. Authorisations to disclose this data were provided to each of the customer's three banks.

The comparison website was given consent to collect and use CDR data to evaluate alternative energy, credit card and mobile plans. Authorisations to disclose relevant data were given to the consumer's energy company, mobile provider and one of their banks. These consents were provided on a one-off basis for a single service, and are no longer active.

The automatic billing solution provides two services. Firstly, it collects banking transaction account usage data to alert it to when bills are automatically withdrawn from the consumer's account. Secondly, it transfers money between the consumer's accounts at that bank if the balance of any account goes below a certain level, in order to prevent the consumer incurring additional fees. Separate consents to collect and use data and to send instructions are required for these use cases. Separate authorisations are provided to the bank to disclose the data and to accept instructions to initiate payments.

Under this system, the consumer has the following consents:

Accredited persons:

Banking account aggregator

- Consents to collect and use CDR Data
  - Bank A
  - Bank B
  - Bank C

Comparison service

- Consents to collect and use CDR Data
  - Bank A
  - Energy company
  - Mobile provider

Automatic billing solution

- Consents to collect and use CDR Data
  - Bank A
- Consents to send instructions for CDR actions
  - Bank A

Data holders:

Bank A

- Authorisation to disclose CDR Data
  - Banking account aggregator
  - Comparison service
  - Automatic billing solution
- Authorisation to accept CDR instructions
  - Automatic billing solution

Bank B

- Authorisation to disclose CDR Data
  - Banking account aggregator

Bank C

- Authorisation to disclose CDR Data
  - Banking account aggregator

Energy company

- Authorisation to disclose CDR Data
  - Comparison service

Mobile provider

- Authorisation to disclose CDR Data
  - Comparison service

Current consent management requirements

For the CDR to operate effectively for consumers, it is necessary that they can easily view, manage and revoke consents and authorisations. The Rules, Standards and CX Guidelines include measures to help consumers easily and effectively manage their consents. These include:

- the need for accredited persons and data holders to provide consent dashboards from which consumers can track and revoke their consents and authorisations
- the provision of consent receipts to notify consumers of the consent details each time a CDR consent is given or withdrawn
- a requirement for the accredited person to notify the consumer after 90 days of inactivity, and
- a maximum consent and authorisation duration of one year.

Although these measures are helpful to the consumer, they do not provide the consumer with an ecosystem wide view of how they have engaged with the CDR in one place.

Though it will be relatively manageable for consumers to track their consents and authorisations when they first engage with the CDR, it will quickly become more difficult as they become more involved.[228] CPRC stated in their submission:

> *We are … concerned that the necessity to access multiple dashboards across different providers will pose a burden for consumers hoping to maintain visibility of data consents across providers and data holders with whom they have established relationships. Accordingly, we strongly support the development of a centralised consumer consent dashboard. A platform of this kind would greatly improve the ability of consumers to comprehend and meaningfully assess how and where their data is being shared.*[229]

Lacking a centralised point from which the consumer can manage their consents and authorisations increases the risk that consumers will lose track of how they have agreed to their data being shared and used, and who they have permitted to initiate actions on their behalf.[230]

Conversely, a centralised consent management system could introduce new risks if implemented poorly. Enabling a single entity to view all of a consumer's consents and authorisations potentially gives them a large amount of insight into the consumer's behaviour. The CPRC also stated in their submission:

> *We also note that further stakeholder consultation would be needed to fully consider risks and sensitivities of a centralised data source holding metadata about consumer accounts, identity, and consents.*[231]

Though the sharing of these insights would likely be appropriate with the informed consent of the consumer, it would be problematic if it was required that this information be centrally collected and stored to participate in the CDR system. Additionally, the technical infrastructure required to enable this information to be collected and stored centrally could be costly to establish and could put undue strains on participants in the CDR system. External consent management should only be progressed if these risks can be effectively managed.

Mandated centralised consent storage

There are two ways that consent information could be made available in a single location, either by requiring that all consent information is mandatorily collected by or provided to a single central entity, or by increasing the ability for consumers to share their consent information with trusted third parties.

The Inquiry does not recommend the mandatory central collection and storage of CDR consent and authorisation information. The CDR has been intentionally designed so that no single entity is

[228] Centralised visibility of consents and authorisations will remain important for tracking past CDR consents and authorisations, for instance where there is a dispute.
[229] Consumer Policy Research Centre submission, p. 3.
[230] Consumer experience research conducted by the DSB indicated that a vast majority of prospective CDR users expected that there would be a central location where they could manage their CDR consents: DSB, 2019, Phase 1 CX Report, p. 103: https://consumerdatastandards.gov.au/wp-content/uploads/2019/02/Consumer-Data-Standards-Phase-1_-CX-Report.pdf.
[231] Consumer Policy Research Centre submission, p. 3.

mandated to have complete visibility of a consumer's interactions in the CDR. Requiring that a government body collects and maintains detailed information about the terms on which a consumer has engaged an accredited person could create concern as to how this data could be used. This could lead to potential users becoming more hesitant about engaging and reduce consumer trust and participation.

The Inquiry also recommends against a non-government body centrally overseeing and collecting CDR consent and authorisation information. Such a system can be appropriate when a non-government body already has responsibility for the overseeing of a regime, and the system has been intentionally designed for this body to centrally collect this information. For instance, the NPP will centrally oversee the MPS and collect MPS payment agreement information in a centralised store of payment agreements. This solution is appropriate in this situation, given the MPS's comparatively narrow domain compared to the CDR and NPPA's central position overseeing the system. Additionally, this regime has been designed with the intention that all this relevant information should be centrally stored, allowing solutions to be built into the overarching infrastructure. As there is no existing non-government body with responsibility for overseeing the CDR, and given the CDR regime's whole of economy scope, such a model is also likely to be difficult to achieve and potentially costly to enable. Additionally, while it may be appropriate for the NPPA to have oversight of any payment agreement information created, mandating a non-government body to collect CDR consent and authorisation information could raise similar concerns to government to collecting and storing such information.

As neither of these options would demonstrate a clear improvement over the current outcome, a system that mandates the centralised storage of consent and authorisation information is not the Inquiry's preferred position.

Recommendation 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.

Increased portability of consent data

Though the Inquiry does not recommend the mandated storage of all CDR consent and authorisation data in a single location, it recommends that options to increase consent and authorisation portability be explored. Enabling consumers to request their CDR consent and authorisation information be shared would be in line with the broader goals of the CDR, allowing private industry to engage with this information to innovate and create products to benefit consumers. By allowing industry to develop external consent management services and compete to attract customers, better and more consumer-centric products could arise. Additionally, allowing private industry to compete would result in CDR consent information remaining dispersed across multiple secure environments, rather than being stored centrally.

A government-facilitated external consent management service could operate alongside industry if there is insufficient competition among private services or if there is sufficient consumer demand for

one. In such a situation it would need to be ensured that industry remains able to compete fairly and effectively. As external consent management services are not expected to be required in the immediate future, private industry should be given sufficient time to create solutions before government action is considered.

Consent data as a CDR data set

The Inquiry recommends that consideration be given to designating consent and authorisation information as CDR data sets. This would leverage the existing CDR infrastructure and privacy safeguards, and would ensure that those offering external consent management services meet the high standards of security and privacy protection required to become an accredited person.

Similarly to banking information, CDR consent and authorisation information provides insights into a consumer's risk appetite and willingness to share information about themselves. Usage consents are particularly insightful, as they include the purpose for engaging the accredited person. As such, it is appropriate that CDR consent and authorisation information shared through the CDR is subject to the protections provided by the CDR's accreditation system and Privacy Safeguards.

Scope of designation

Industry should be consulted about the associated regulatory costs prior to designating consent and authorisation information. Though the Inquiry expects that the relative cost to data holders of designating authorisation data will likely be low, the cost to accredited persons of designating consent data will likely to be much higher and more variable.

Any data holders required to share other CDR data must already have strict customer authentication and authorisation processes in place, and must have undergone extensive testing to ensure that their systems operate correctly. Additionally, these data holders will already have been connected to the Register and Accreditation Application Platform (RAAP) and will have had to have created APIs to transmit other CDR data. As such, it is expected the regulatory burden of requiring these data holders to also share authorisation or consent data will be low.

Most accredited persons however, will not have been required to meet obligations of this kind. If all accredited persons are required to establish processes to enable the sharing of consent information as a CDR data set through publicly accessible APIs, then the cost of joining the CDR will likely become exclusionary. This would encourage the continued use of less secure alternatives, such as screen scraping.

Depending on industry feedback, the Inquiry recommends that only those accredited persons intending to share CDR data with a wide variety of accredited persons should also be required to share consent and authorisation data sets. Accredited persons who do not otherwise share CDR data in such a way should be encouraged to share consent data as a voluntary data set. The exact process for determining which accredited persons should be required to share CDR data should be considered as part of the designation process.

Box 6.3 – Requirements to share consent information

Data-Klean offers a data filtering intermediary service using the CDR. It collects relevant CDR data from a range of data holders and then shares filtered fine-grained subsets of this data with other accredited persons at the consumer's direction. Data-Klean has built an API to allow its services to be made available to any other accredited person. As CDR data collected by Data-Klean could be shared with a wide variety of accredited persons, it would be appropriate for Data-Klean to make its consent information broadly available to other accredited persons.

Heart-a-Tax (a CDR accredited tax accounting firm) has a bilateral agreement with Tic-Tax-Toe (another CDR accredited tax accounting firm). Under this arrangement, Heart-a-Tax may send CDR data to Tic-Tax-Toe with the consumer's consent to provide more bespoke tax services. As Heart-A-Tax has not developed the requisite API infrastructure required to allow CDR data to be broadly shared, such a requirement would be prohibitively expensive. As such, Heart-A-Tax and Tic-Tax-Toe should be encouraged, but not required, to share consent data with accredited consent managers.

Designating only those accredited persons already widely sharing CDR data will result in consumers being able to engage consent management services that could provide, at minimum, a view of all the authorisations the consumer has made. A complete dashboard of authorisations would provide a consumer with oversight of all the initial CDR data sharing and action initiation arrangements that they have entered into. This would help consumers to track the accredited persons they have engaged with, but would not necessarily let them see all their usage consents, or how their data has been further shared by ADRs at their direction. This additional information would however remain available separately through accredited persons' consumer dashboards.

Recommendation 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.

Consent transmission standards

To enable consent and authorisation information to be designated as CDR data, consent and authorisation standards should be created by the DSB. The DSB should seek input from industry and consumer groups about the appropriate standardisation level when designing transmission standards. Although increased standardisation could increase the ability for consent information to made machine readable, it could also limit creativity and innovation in product design. Data Republic made clear in their submission that a clear protocol is required for enabling consent to be captured in a consistent way across CDR participants and industries:

> *In our view, the concept of consent in CDR must evolve from a relatively simple workflow and UX recommendation with no standardised approach to use case taxonomy to a highly*

> *standardised, software enabled, taxonomical consent model which encodes consent and enables it to flow through a system capturing critical information at a use case level.*[232]

In designing consent and authorisation standards, the DSB should also consider the possibility that the framework established for managing CDR consents and authorisations could also be used to manage consents external to the CDR regime.[233] This could help enable a whole-of-economy consent management service, and provide consumers with a consistent and familiar online experience.

Limited action initiation

To operate effectively, external consent management services should be able to perform the same functions as a consumer dashboard. Presently this would include the ability to revoke consents and authorisations, and possibly in future the ability to amend and renew consents.[234] The DSB should create standards to facilitate this after consultation with industry.

A consumer should not be able to grant entirely new CDR consents or authorisations through an external consent management service. Current consent process requirements are intended to protect consumers. Allowing external consent management services to circumvent this process would undermine the foundation of the customer-centricity and control in the CDR and the safety measures determined by the Rules and Standards, and consents provided by this method would likely be of a significantly lower quality.

Recommendation 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.

Impact on vulnerable consumers

Enabling external consent management services should seek to empower vulnerable consumers, particularly those who have lower data literacy skills. Tracking and managing consents and authorisations is likely to be a key difficulty for consumers when using the CDR in the future as usage grows, and external consent management services propose one potential solution to this issue.

External consent management services could also provide more benefits than just allowing a consumer to track their consents. For instance, an external consent management service designed to assist people understand CDR arrangements could potentially prompt consumers to cancel consents

[232] Data Republic submission, p. 6.
[233] Such additional considerations could include fields that outline the legal basis under which the data is being shared, whether this is a consent to 'push' or 'pull' data, etc. Though these fields will be consistent for data shared through the CDR, it will allow for the standards created to be used to manage consents more broadly.
[234] When initiating actions on a customer's behalf, external consent management services should adhere to the requirements set out in the Rules and Standards, and have regard to the CX guidelines. This includes suggestions such as the incorporation of positive frictions to encourage consumers to consider the implications of revoking their consents.

that may have become redundant, or provide additional detail to the consumer about the accredited persons they have engaged and the implication of the consents that they have given. These could become powerful tools for helping people better engage with and understand the CDR.

Privacy implications of designating consent information

Designating consent and authorisation data as CDR data sets will have implications beyond external consent management services. For instance, a beneficial use case would be enabling consumers to understand their CDR consents so that they can be re-established when they move data holders. This would significantly simplify the switching of data service providers.[235]

Consent data could however, also provide detailed insights about a consumer and their attitudes towards risk and privacy. These insights could be potentially harmful to consumers should they be disclosed to a malicious actor. The Inquiry, therefore, also recommends that the privacy impacts of designating consent and authorisation data be considered through a separate process before any designation is made.

Recommendation 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.

[235] Tyro expresses this point in their submission, where they raised that 'a customer that has provided authorisations on their account to share their data with accredited third parties may find the prospect of re-establishing these consents and authorisations on a new account to be too arduous that they elect not to switch. As such, if this is not managed effectively, Open Banking in itself may act as an additional barrier to switching inadvertently'. Tyro Submission, p. 3.

Chapter 7: Consumer safeguards

Chapter 4 looked at the elements required for action initiation and set out key accredited person and data holder responsibilities and a general liability framework. This chapter looks specifically at what additional CDR consumer safeguards may be required for action initiation. It also considers how the CDR can promote innovation in a manner that takes into account the diverse needs of consumers, including those with vulnerabilities. Lastly, it considers the potential privacy impacts of expanding the CDR's functionality and how privacy and information security risks should be addressed.

Empowering consumers to benefit while managing risks

The CDR creates digital infrastructure to be used by participants in developing and delivering innovative services to consumers. Over time, the increased data sharing and use enabled by the CDR should empower and lead to better outcomes for consumers. It will also impact how consumer markets operate and how consumers choose to engage with businesses in the digital economy.

Although expanding the CDR's functionality will open up new possibilities for consumers, action initiation will also bring risks that need to be managed. In considering the potential risks, it is important to recognise existing risks which action initiation could reduce. For example, the Open Banking Review reported that potentially millions of Australian bank customers have given their account login and password details to third parties that 'scrape' data from customer's internet banking interfaces and use it to provide services such as personal budgeting tools or small business lending. Some of these customers agree to grant 'write' access as well as 'read' access, allowing the third party access to the customer's account and the capability to transact on a customer's behalf.[236] The CDR offers alternative, safer ways to facilitate these business models, including by enabling fintechs and others to create and provide data driven services without exposing consumers to risks associated with sharing their banking login credentials with an unaccredited third party.[237] While CDR data sharing is a very significant advance in this respect, it would not be possible to replicate some of these business models using the safer environment of the CDR without CDR action initiation.

Consumer confidence will be critical to the future success of the CDR. Ultimately, consumers need to be able to trust that the right consumer safeguards are in place to ensure that innovation does not come at the expense of their rights, that their data and interests are protected, and that they have recourse to appropriate remedies when needed. However, the Inquiry recognises that not all issues that could arise in respect of services delivered to consumers through use of the CDR will arise solely, or even partly, due to its use, nor will those issues be unique to that communication channel. Indeed,

[236] Open Banking Review, p. 51 and p. 73.
[237] The disclosure of internet banking credentials may affect a consumers' rights under the ePayments Code (Reserve Bank of Australia submission, p. 3 and Financial Rights Legal Centre submission, p. 38). It may also present a range of data security, privacy and fraud risks to consumers: RBA submission, p. 3.

a number of examples of conduct raised in the Inquiry's consultations are issues that exist, and may continue to exist, in consumer markets irrespective of the availability of the CDR in a sector.[238]

In developing the CDR regime, a balanced consideration of potential benefits to, and impacts on, consumers will be required. The Open Banking Review noted that too great an emphasis on privacy and security could delay or undermine the effective implementation of the CDR, depriving consumers of its benefits.[239] Similarly, consumer safeguards set too tightly might inadvertently deter use of a safe and efficient system and, instead, push businesses and the consumers they service towards less safe alternatives. Accordingly, the Inquiry considers it important that, as the CDR is developed, the nature and character of potential risks are examined objectively, with risks and opportunities adequately balanced in system design and development.

Consumers and existing protections

The CDR mitigates risks associated with data sharing through the inclusion of several key consumer protections. These operate alongside general consumer laws, industry-specific consumer protections and other sources of obligations.

This section surveys sources of obligations relevant to consumers' relationships with accredited persons and data holders, and identifies additional consumer protection measures that are necessary or desirable if the CDR's scope and functionality expand.

Existing consumer protections under the Consumer Data Right

Broadly speaking, existing CDR consumer protections fall into one of four categories:

- requirements imposed on accredited persons, ADRs, or persons seeking accreditation
- requirements imposed on data holders
- specific prohibitions on particular deceptive conduct in connection with the CDR
- avenues for redress, in the event that an ADR, data holder or other person fails to comply.

These are summarised in Table 7.1.

[238] For example, consumers making switching decisions based on price rather than overall suitability, reliance by businesses on complex consumer contracts, offering different prices to consumers based on factors such as a consumer's propensity to switch, and product recommendations influenced by the payment of commissions.
[239] Open Banking Review, p. 50.

Table 7.1: Key existing consumer protections under the CDR regime

Obligation	Overview of requirements	Source of obligation
Requirements on accredited persons, ADRs, or those seeking accreditation		
Accreditation is mandatory	To have CDR consumer data disclosed to them, third parties must be accredited[240]	Sections 56BC and 56BD
Accreditation criteria	Accredited persons must meet requirements regarding insurance, being a fit and proper person, information security, internal and external dispute resolution, and comply with any conditions imposed	Sections 56BH and 56CA, Rules[241] – Parts 5 and 7, Schedules 2 and 3
Consent to request CDR data	Accredited persons must have consumer consent to request CDR consumer data. Consent should be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn. Accredited persons must ask for consent in compliance with the Rules	Section 56EF – Privacy Safeguard 3, Rules – Part 4
Data minimisation principle	Accredited persons may only collect and use CDR consumer data reasonably needed to provide the requested good or service	Rules 4.4 and 4.12
Protection of CDR data	ADRs must take specified steps to protect CDR data from misuse, interference, loss, and unauthorized access, modification or disclosure	Section 56EO – Privacy Safeguard 12
Notification of disclosure	ADRs are to take steps specified in the Rules to notify consumers of disclosure of CDR consumer data	Section 56EM – Privacy Safeguard 10
Deletion or de-identification	Consumers can request deletion of CDR data[242]	Section 56BAA
	ADRs must destroy or, with the consumer's consent, de-identify redundant data. Data becomes redundant when use permissions expire[243]	Section 56EO – Privacy Safeguard 12
Use and disclosure restrictions	CDR consumer data cannot be used for direct marketing except as authorised by the Rules	Section 56EJ – Privacy Safeguard 7, Rules 4.11, 7.5 and 7.6
	Consent cannot be requested to on-sell CDR data (unless de-identified) or to use CDR data to identify, compile insights or profile another identifiable person	Rule 4.12

[240] Or be a designated gateway: subparagraph 56BD(1)(b)(iii) of the CCA.
[241] All references to rules in this chapter are to the *Competition and Consumer (Consumer Data Right) Rules 2020* (the Rules).
[242] The Rules must not require deletion in certain circumstances, including where retention is required by law: sub-section 56BAA(2) of the CCA.
[243] Deletion or de-identification is not required in certain circumstances, including where retention is required by law: subsection 56EO(2) of the CCA. Use permissions are currently limited to 12 months: Rule 4.12(1).

Obligation	Overview of requirements	Source of obligation
Transparency and reports to regulators	ADRs must maintain consent dashboards and CDR policies. ADRs' twice yearly reports to the ACCC and OAIC are required to include a summary of CDR complaint data	Section 56ED – Privacy Safeguard 1, Rules 1.14 and 9.4
CDR consent receipts and record keeping	Accredited persons must give the consumer a CDR receipt as soon as practicable after the consumer gives, or withdraws, a consent. ADRs must keep records, including records and explanations of consents given by consumers	Rules 4.18 and 9.3
Ongoing notification for consents	If 90 days have elapsed since a consumer last consented, used their dashboard or was notified, the accredited person must notify the consumer	Rule 4.20
Reporting to consumer	Rules can enable a CDR consumer to direct an ADR to give reports about their valid requests, and any disclosures made in response	Section 56BI
Obligations applying to data holders		
Data holder to seek authorisation to disclose	Data holders must ask consumers to authorise disclosure of requested CDR data, and to disclose required CDR data where authorised to do so	Section 56BC, Rules 4.5 and 4.6
Eligibility	Where there is no existing authorisation, a data holder is only required to seek authorisation where they reasonably believe the request is made by an accredited person on behalf of an eligible consumer[244]	Rule 4.5
Withdrawal of authorisation and record keeping	Consumers can withdraw authorisation at any time. Authorisations expire after 12 months unless renewed. Data holders must keep records, including records and explanations of authorisations given by consumers	Rules 4.25, 4.26 and 9.3
Accuracy of data	Data holders authorised to disclose must take reasonable steps to ensure data is, having regard to the purpose for which it is held, accurate, up to date and complete[245]	Section 56EM – Privacy Safeguard 11
Notification of disclosure	Data holders must take specified steps to notify CDR consumers of disclosure of CDR data[246]	Section 56EM – Privacy Safeguard 10, Rule 7.9

[244] For example, for the banking sector currently, a CDR consumer will be eligible if they are an individual who is 18 years of age or over, and is the account holder for an account with the data holder that is open, and set up in such a way that it can be accessed online: Clause 2.1 of Schedule 3 to the Rules.
[245] This obligation also applies to ADRs when authorised or required to disclose CDR data: Section 56EN of the CCA – Privacy Safeguard 11.
[246] Currently these involve updating the consumer's dashboard: Rule 7.9. This is not required if considered necessary to prevent physical or financial harm or abuse: Rule 4.6.

Obligation	Overview of requirements	Source of obligation
Permitted refusal to disclose	Data holders can refuse to seek authorisation for or disclose CDR data in some circumstances, including to prevent physical or financial harm or abuse	Rules 3.5 and 4.7
Transparency and reports to regulators	Data holders are required to maintain consent dashboards and CDR policies. Data holders' twice yearly reports to the ACCC and OAIC are required to include a summary of CDR complaint data	Section 56ED – Privacy Safeguard 1, Rules 1.15 and 9.4
Reporting to consumer	Rules can enable a CDR consumer to direct a data holder to give reports about the consumer's valid requests, and any disclosures made in response	Section 56BI
Specific conduct prohibitions		
Holding-out	A person must not hold out that they are accredited if they are not	Sections 56CC and 56CD
Misleading and deceptive conduct	A person must not mislead another person into believing that a person is a CDR consumer, is making a valid request or consent, or satisfies other disclosure criteria	Sections 56BN and 56BO
Avenues for redress		
Range of remedies	Remedies include suspension or revocation of accreditation, injunctions for breach of the CCA or Rules, infringement notices, substantial civil penalties,[247] and fines for offences.	Various
Internal and external dispute resolution (EDR)	ADRs and data holders must meet internal dispute resolution requirements and be a member of a recognised EDR scheme for consumer complaints	Rules 5.12, 6.1 and 6.2
Direct rights of action	Consumers can take action to recover loss or damage arising from a contravention of the privacy safeguards or Rules relating to privacy or confidentiality of CDR data, certain CCA CDR prohibitions, or a contravention of a civil penalty provision of the Rules. Actions on behalf of consumers are also supported.	Sections 56EY, 82 and 87

[247] For contraventions of sections 56BO(1), 56BU(1), 56CD of the CCA or a civil penalty provision of the Rules (other than those that specify a lower penalty), these cannot exceed the greater of $10 million, three times the value of the benefit obtained or, if that benefit cannot be determined, 10 per cent of annual turnover: Paragraph 76(1A)(b) of the CCA.

Consumer protections outside of the Consumer Data Right

CDR participants also have obligations under economy-wide consumer laws and, in some cases, sector-specific legislation.

Consumer law

In their dealings with consumers, accredited persons and data holders must ensure that they do not engage in misleading and deceptive, or unconscionable, conduct or seek to rely on unfair contract terms in standard form consumer or small business contracts.[248]

Consumer laws also impose obligations in relation to the quality of the services that businesses deliver. Where a person supplies (non-financial) services to a consumer, the Australian Consumer Law (ACL) provides an automatic guarantee that they will be provided with due care and skill, be reasonably fit for purpose and be delivered within a reasonable time.[249] In contracts for the supply of financial services, there is an implied warranty that the services will be rendered with due care and skill, and will be reasonably fit for purpose or might reasonably be expected to achieve the desired result.[250]

Sector-specific consumer protections

Sector-specific legislation also contains relevant protections. For example, an accredited person or data holder who provides financial product advice to consumers, or deals in financial products, as part of a financial services business would be required to hold an AFS licence, or act as a representative of an AFS licensee.[251] AFS licence holders must comply with a range of obligations, including doing all things necessary to ensure that the financial services covered by the licence are provided 'efficiently, honestly and fairly', maintain competency, and have in place adequate arrangements to manage conflicts of interest.[252]

Depending on the financial service being provided, an accredited person could also be subject to additional obligations under the *Corporations Act*. For example, if providing personal financial product advice,[253] they may be required to act in the best interests of the client when providing advice, and must prioritise the client's interests in the event of a conflict of interest.[254]

---

[248] Schedule 2 to the CCA: Australian Consumer Law, and *Australian Securities and Investments Commission Act 2001* (ASIC Act), Part 2.
[249] Sections 60 to 62 of the ACL. Depending on the circumstances involved, remedies for non-compliance may include compensation for damages and loss.
[250] Section 12ED of the ASIC Act. An exception applies for contracts of insurance.
[251] Unless exempted or relieved of this requirement. Financial product advice generally involves 'a qualitative judgment about – or an evaluation, assessment or comparison of – some or all of the features of a financial product': ASIC, Regulatory Guide 244, p. 10.
[252] Subsection 912A(1) of the Corporations Act.
[253] Automated or robo-advice, provided using algorithms and technology, can be general or personal advice: ASIC, RG 255 Providing digital financial product advice to retail clients, p. 4.
[254] Sections 961B and 961J of the Corporations Act.

Similar to AFS licence holders, Australian credit licence holders are obliged to do all things necessary to ensure that credit activities authorised by the licence are engaged in efficiently, honestly and fairly, and have in place adequate arrangements to ensure that clients are not disadvantaged by any conflict of interest.[255] Mortgage brokers are also subject to a duty to act in the best interests of the customer in relation to providing them credit assistance and to give priority to the customer's interests where there is a conflict.[256]

Banks are subject to a range of conduct and prudential obligations, including APRA lending standards and licence obligations to act efficiently, honestly and fairly. In addition to obligations imposed on them as credit licensees,[257] banks who subscribe to the *Banking Code of Practice* are required to exercise the care and skill of a diligent and prudent banker when considering lending to relevant individuals and small businesses.[258] Further, banks who subscribe to the ePayments Code are bound by specific conduct requirements in connection with electronic payments.[259]

Outside of financial services, the *National Energy Retail Law* and *National Energy Retail Rules* provide a consumer protection framework for the retail sale of energy to consumers and small businesses in a majority of states and the ACT. Applying to retailers, this framework provides a range of consumer protections, including a requirement to obtain a consumer's explicit informed consent to enter into a market retail contract, cooling-off periods and obligations to assist consumers in financial hardship.

In the telecommunications sector an industry code enforceable by the ACMA, the *Telecommunications Consumer Protection Code*, covers matters including procedures and obligations when a consumer changes supplier.[260]

Other sectors will have their own legislation, industry codes and/or standards that grant, or affect, the rights of consumers in acquiring, managing or ceasing to acquire goods or services. As discussed in Chapter 4, the interaction and potential overlap between particular industry measures and the CDR regime needs to be considered when assessing the potential to designate a sector under the CDR, with any barriers or conflicts between the regimes identified and appropriately resolved.

[255] Section 47 of the NCCPA.
[256] Sections 158LA, 158LE, 158LB and 158LF of the NCCPA.
[257] Under sections 128 to 130 of the NCCPA, these currently include assessing whether a proposed credit contract will be unsuitable for the consumer, and undertaking inquiries about the consumer's requirements, objectives and financial situation. The Government announced proposed reforms to this legislation: The Hon Josh Frydenberg MP, Treasurer, Simplifying access to credit for consumers and small business, 25 September 2020.
[258] Australian Banking Association, *Banking Code of Practice*, paragraph 49.
[259] Chapter E of the ePayments Code.
[260] Communications Alliance Ltd, *Industry Code C628:2019 - Telecommunications Consumer Protection Code*. A range of other codes, standards and legislative obligations will also be relevant.

Recommendation 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.

General Law

Other potential sources of obligations relevant to the relationship between the consumer and an accredited person or data holder include general law protections, such as those arising under contract law or equity.

Use of CDR data sharing arises in the context of a consumer requesting that an accredited person provide them with goods or services, with the accredited person collecting and using the consumer's CDR data in order to provide those goods or services.[261] Similarly, action initiation would generally be expected to take place in the context of a request by a consumer to an accredited person to provide them with a product or services (for example, facilitating the acquisition of services from a data holder or the initiation of a payment), with the relationship between the consumer and the accredited person covered by an agreement between them. A data holder receiving an action initiation instruction could be someone with whom the consumer has an existing contractual relationship such as the consumer's bank (as is the case with CDR data sharing), or a prospective new provider.

Depending on the circumstances, the relationship between the consumer and the accredited person who provides them with goods or services may also resemble, or have elements of, agency.[262] This will be influenced by the contractual arrangements which are established for the provision of those goods or services. In this context, action initiation involves an accredited person, with the consumer's consent, initiating an action or actions with a data holder that are within the scope of that consumer consent, with the data holder obliged to progress valid requests to the same extent as if the request were initiated by the consumer through another channel. However as discussed in Chapter 4, it is recommended that the data holder would only be able to do so where it has confirmed that it has valid authorisation from the consumer.

Dependent on the nature of the relationship between a consumer and the accredited person or data holder, equitable obligations could also arise. Some categories of relationships are generally recognised as being fiduciary, giving rise to equitable obligations on one party to act in the interests of the other and not in their own interests.[263] While agency is commonly recognised as a fiduciary

[261] Rule 4.3. The CCA also provides for direct requests by a consumer for their CDR data.
[262] The term 'agent' is used colloquially to describe a range of relationships, including those that are not agents in a legal sense. Agency generally describes a relationship between two parties, where one acts on the other's behalf, but subject to that other's control or direction. Whether a party is at law an agent of another will depend upon the true nature of the agreement between them and the particular circumstances of their relationship.
[263] For example, the relationship between a solicitor and their client, or a trustee and beneficiary.

relationship, the existence, or nature, of any fiduciary duties that an agent may owe to a principal will depend upon the particular facts and circumstances.

Other regulation

The CDR regime also, of course, exists in the context of other regulation of general application. For example, anti-discrimination law prohibits discrimination in the provision of goods or services on the basis of protected attributes including disability, age, sex and race. Businesses adopting risk-based or personalised pricing, or otherwise drawing on CDR data in deciding whether and what service to offer consumers, will need to ensure that their data-driven approach does not involve discrimination on the basis of protected attributes, such as age, disability or race.

The *Privacy Act 1988* (Cth) (Privacy Act) (discussed later in this chapter) regulates how businesses above a certain size must treat consumer's personal information, other than CDR data which is regulated by the CDR regime.[264]

Depending on the context other laws will also be relevant when considering the current and future application of the CDR.

Consumer safeguards for action initiation

Action initiation allows consumers to give consent to an accredited person to initiate actions, using CDR infrastructure to communicate with data holders. While the actions that an accredited person could initiate on behalf of a consumer would differ in sectors – as discussed in Chapters 4 and 5 – they could range from making an inquiry, submitting a product application, acquiring a service or initiating payments out of a consumer's account. The risks associated with these activities are more diverse than those associated with CDR data sharing, where the focus of consumer protections is primarily on the privacy and confidentiality of the consumer's data. The consequences, should businesses conduct themselves in ways inconsistent with consumer's expectations, are potentially (but not necessarily) more severe.

This raises the question of what additional consumer protections and regulatory powers may be required to address these challenges. These are examined below.

Adapting existing protections for action initiation

Person offering to initiate actions – Accreditation and consent

As with data sharing, two key consumer protections required for action initiation are that parties seeking to initiate actions on behalf of a consumer are appropriately **accredited** and have the consumer's **consent**.

[264] The Privacy Act applies to CDR accredited persons regardless of business size. When handling non-CDR data, APP7 – which applies to use or disclosure of personal information for direct marketing – will also be relevant, as may be other restrictions on unsolicited communications, such as the *Spam Act 2003* (Cth). Some States and Territories impose additional privacy obligations, for example with respect to health information.

Under the CDR regime, the criteria for accreditation can be set in the Rules. As discussed in Chapter 4, the Inquiry considers that classes of actions posing greater potential risk to the consumer should require higher tiers of accreditation. It will be important to ensure that the regulatory settings enable the decision-maker, in considering applications for accreditation, to take into account all matters relevant to the applicant's suitability to initiate payments and other actions of the type proposed. Accredited persons should be obliged to advise when the types of goods or services that they offer to provide to consumers that involve use of CDR action initiation change.[265] As with data sharing, the accreditor or rule maker should be able to respond promptly, where necessary to protect consumers or to address other risks specified in the CCA or the Rules.[266]

As is currently the case with CDR data sharing, customer consent would remain the central plank of consumer protections for action initiation through the CDR. As identified in Chapter 4, the Inquiry considers that a robust process for consumers to provide genuine, active consent for third parties to initiate actions will be required. Action initiation should be enabled to the extent possible through adaptation of existing consent and authorisation processes that currently enable data sharing. Similar to the case with CDR data sharing, an accredited person should be prohibited from sending action initiation instructions unless they have a valid request from the consumer and the accredited person complies with all relevant Rules in doing so.[267] A range of remedies, including civil penalties and suspension or revocation of accreditation, should be available. The consumer should have the ability to take action against the accredited person to recover loss or damage in the event of breach. Action initiation consents should be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn. As noted in Chapter 4, there are some types of actions which should not be able to be permitted using action initiation, even with a consumer's consent, due to the security and privacy risks posed to the consumer.[268]

While action initiation should maintain the current ability to limit consent and authorisation durations, additional safeguards which balance the need for security with consumer experience should also be considered. As discussed in Chapter 4, this should include requirements for accredited persons offering action initiation enabled services to authenticate customers in certain circumstances. It will be important that action initiation consent processes are subject to customer experience standards and guidelines to ensure that processes produce genuine consent.

[265] Similar requirements already form part of accreditation requirements for CDR data sharing, with ADRs having to provide this information upon accreditation and subsequently in periodic returns.
[266] See Rules 5.10(3) and 5.17 (item 4), and subsection 56BS(1) of the CCA.
[267] Section 56EF of the CCA – Privacy Safeguard 3.
[268] As discussed in Chapter 4, these would include the ability to modify customer's passwords or change the customer's mobile phone number that a service provider uses to authenticate its customer.

Recommendation 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.

Recommendation 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.

Data holder – Customer authentication and authorisation

In CDR data sharing, the risk that an accredited person making a request to a data holder is doing so without the consent of the relevant consumer is managed by the data holder authenticating the consumer upon receipt of the request, and confirming that they have authorisation to share that data. When a data holder receives a data sharing request from an accredited person, they first check to see whether they have an existing authorisation from the consumer relating to the specific request. If not, the data holder connects with the relevant consumer, using details already known to it, to satisfy itself that the request relates to an existing customer. The data holder then confirms with the consumer that they are authorised to act (i.e. share their data).

A similar process should also be used for action initiation to ensure that an accredited person is acting with the valid consent of a consumer when making an action initiation request to a data holder. However, as discussed in Chapter 4, for some types of requests contemplated for action initiation, the data holder may never have previously dealt with the consumer and so will not have an existing relationship with them. This will mean that the data holder will be unable to authenticate the consumer in the same manner it would authenticate an existing customer. In those circumstances, the data holder will need to confirm that the person the accredited person presents to them is correctly described.

Whether or not the data holder already knows the consumer, the data holder who has received an action initiation request will also need to satisfy themselves that the consumer authorises them to receive and act on the action initiation instructions received from the accredited person. This requirement for the data holder to check that it already has, or obtains, the authorisation of the customer to action such instructions will be a fundamental consumer protection for action initiation. A range of remedies, including civil penalties, should apply, with the consumer having the ability to take action to recover loss or damage in the event of breach.

As discussed in Chapter 4, the CDR regime should allow for fine-grained authorisations and should require specificity in authorisations in some instances, embedding additional consumer protections into the regime. [269]

Recommendation 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.

Extending other Consumer Data Right consumer protections for action initiation

Many of the existing in-built consumer protections will be equally and, in some cases, more important in a write access context.

Holding out

The CCA prohibits a person 'holding out' that they are an accredited person for CDR purposes, hold a particular level of accreditation, or are an ADR of CDR data when they are not.[270] This behaviour attracts significant criminal fines or civil penalties.[271]

A party falsely claiming an accreditation will be unable to access data under the CDR's current data sharing functionality. This is because only accredited parties appear on the Register of Accredited Persons which data holders use to check the accreditation status of a requesting party, and will be able to decrypt data received. This would not, however, mean that consumers are not potentially exposed to harm. A consumer may, for instance, impart information about themselves to a person believing that the person is accredited and will provide them with a service using that information and their CDR data. The consumer could be exposed to harm if the person instead obtains the consumer's transaction data through less safe means, or be left worse off if the consumer acted on advice they understood had been tailored based on their CDR data, without that data ever having been obtained.

With action initiation, a consumer could provide an accredited person with important and/or sensitive information (for example, to sign up to a new service provider), as well as consents to do various things such as draw payments out of the consumer's transaction account. Were a person to lead a consumer to think that they were accredited for action initiation under the CDR, but were not and instead used less safe and secure services, such as screen scraping, to initiate actions (including payments), consumers could be exposed to detriment. Accordingly, the civil and criminal

[269] As discussed in Chapter 4 these could, for example, include the ability for a consumer to impose a maximum limit on amounts for transactions initiated by accredited persons.
[270] Sections 56CC and 56CD of the CCA.
[271] These are up to the greater of $10 million, three times the value of the benefit obtained, or if that benefit cannot be determined, 10 per cent of the annual turnover. In addition to the protections available through consumer laws, serious conduct such as fraud is prohibited by the criminal law.

prohibitions on 'holding out' should be extended to apply to persons who offer, or purport to offer, action initiation services to consumers.

Misleading and deceptive conduct

It is an offence for a person to knowingly engage in conduct that misleads or deceives, or is likely to mislead or deceive, another person into believing that a person is a CDR consumer for CDR data, or is making a valid request or consent, or has satisfied other criteria, for the disclosure of CDR data.[272]

Conduct which misleads or deceives, or is likely to mislead or deceive, a person into believing that another person has given their consent for initiation of an action under the CDR, or is making a valid request or consent, or satisfied other criteria, for initiation of an action, should similarly be prohibited. Both criminal and civil penalties and consumer rights of action should be available.

Other Consumer Data Right consumer protections

A range of the other CDR data sharing obligations and protections would need to be extended or replicated for action initiation, including notification,[273] transparency and reporting obligations imposed on both accredited persons and data holders.[274]

Currently accredited persons are subject to certain use and disclosure prohibitions, for example, an accredited person cannot request consent to on-sell CDR data (unless de-identified) or to use CDR data to identify, compile insights or profile another identifiable person.[275] Data holders are permitted to refuse to disclose, or refuse to seek authorisation to disclose, CDR data in certain circumstances specified in the Rules, for example, where the data holder considers it necessary to do so to prevent physical or financial harm or abuse.[276]

Similar protections are likely to be appropriate in an action initiation context. Appropriate and proportionate remedies (including fines and penalties) should also be available. As with data sharing, consumers should have access to CDR internal and external dispute resolution, backed by direct rights of action.

---

[272] Section 56BN of the CCA. As with holding out, significant fines apply. The CDR regime also contains a similar civil prohibition, for which proof of knowledge is not required: Section 56BO of the CCA.
[273] Reserve Bank of Australia submission, p. 2: The RBA noted the importance of consumers having good visibility over all authorisations in place and ability to easily cancel any authorisations.
[274] Existing data sharing notification (including receipting), transparency and reporting obligations relevant to consumers are summarised in Table 7.1.
[275] Rule 4.12.
[276] Rules 3.5 and 4.7. In respect of financial products, BCA submitted that extending exemptions to refuse switching where considered necessary to prevent harm or abuse and restrictions on accounts that can be switched should be considered: BCA submission, p. 4. Where there is no existing authorisation, a data holder is only required to seek authorisation where they reasonably believe the request is made on behalf of an eligible customer. In the banking sector, this currently does not include a person under the age of 18 years: Rule 4.5 and clause 2.1 of Schedule 3 of the Rules.

Recommendation 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.

Action initiation and accredited persons' obligations to consumers

While CDR data sharing allows a consumer to consent to an accredited person requesting their existing consumer data from a data holder, action initiation goes further, allowing the consumer to authorise an accredited person to initiate actions with existing or new service providers.

The risks associated with a consumer permitting an accredited person to initiate actions on their behalf will likely differ depending on a range of factors. These include the sector, the classes of action (for example, sending a product inquiry, initiating entry into an ongoing contract, or initiating on ongoing payment arrangement), the scope of the consumer's consent (including the degree of discretion afforded to the accredited person), and the particular circumstances or vulnerabilities of the consumer.

Additional risks facing a consumer when consenting to an accredited person initiating actions

Scenarios in which the conduct of an accredited person under action initiation could lead to risks for consumers include:

- **Scenario 1** – the accredited person transmitting action initiation instructions to a data holder without (or outside the scope of) the consumer's consent
- **Scenario 2** – the accredited person, who has the consumer's consent to initiate an action, failing to transmit the action initiation instruction
- **Scenario 3** – the accredited person, who has the consumer's consent to initiate actions, using that permission to initiate actions contrary to the consumer's interest

In Scenario 1, the accredited person is clearly acting outside the consumer's consent and, under the principles discussed above, the consumer would have access to a remedy under the CDR regime with respect to the accredited person.

With respect to Scenario 2, while a consumer may consent to an accredited person making a data sharing request, the CDR regime itself does not, in its current form, expressly require an accredited person to make that request. In the context of action initiation, the consumer could suffer loss if, for example, they consented to an accredited person initiating a payment and the consumer has failed to meet its obligations to a third person because the accredited person did not act on the request. The consumer could, however, have a remedy under contract law or a consumer guarantee or implied warranty.

In Scenario 3 the accredited person is not acting without the consumer's consent, but rather is acting in a way that disadvantages the consumer. An example could be where an accredited person with a consumer's consent to find and switch the consumer to a new provider and, motivated by increasing its earnings from commissions, repeatedly switches the customer between deals to the disadvantage of its customer. Another example could be where a debt collector obtained accreditation and, in reliance on a consumer's consent, initiates payments from the consumer's account leaving the consumer with inadequate funds. Either scenario could, depending on the circumstances, fall for consideration under general consumer law – for example, as unconscionable conduct, misleading or deceptive conduct or potentially involve an unfair contract term. However, unless these behaviours contravened a condition attached to the accredited person's CDR licence, they would not necessarily attract a remedy under the CDR regime.

Will other obligations adequately address these risks?

Consumers and businesses already use the services of others (i.e. third parties) to do things for them, or to formally act on their behalf. These include formal, regulated relationships such as a client engaging a solicitor to act on their behalf in a transaction or dispute. They also include a range of much less formal arrangements – for example, where a person authorises their spouse to handle their relationship with a service provider.

As discussed above the obligations owed by a business to a consumer in such a scenario are likely to depend upon a range of factors. These could include the nature of the services, the existence and terms of any agreement between the parties, the true nature of their relationship, and the level of trust and confidence placed by one party in the other.

If the service being offered by an accredited person to a consumer constituted financial product advice, for example, the accredited person would be required to hold an AFS licence and do all things necessary to ensure the financial services covered by the licence are provided efficiently, honestly and fairly. If the advice was personal financial product advice they would be required to act in the best interests of the client and to prioritise the client's interests in the event of a conflict of interests.

However, even where particular duties or obligations are imposed on a business in their dealings with customers due to the sector in which they operate, if they became an accredited person it may, but would not necessarily, be the case that those duties or obligations applied to all aspects of their dealings with a consumer in respect of initiating actions through the CDR.

Nor is it necessarily the case that a consumer would have a right to enforce those duties or obligations (although, in practice industry licensing arrangements often require businesses to be members of a scheme for resolving consumer complaints).

Conduct obligation for accredited persons

In light of the above, and:

- in recognition of the wide range of factual circumstances that could present themselves depending on:

  - the sectors in which the conduct arises
  - the relevant classes of action
  - the scope of the consumer's consent (including the degree of discretion afforded to the accredited person)
  - the potential for a consumer's consent to be influenced by factors including vulnerability, and
- the desirability of ensuring that the CDR regime itself provides an accessible remedy for consumers,

the Inquiry considers that persons accredited for action initiation should be subject to a conduct obligation in respect of their action initiation activities. If the accredited person's conduct with respect to a customer fails to meet this obligation, the consumer should be able to take action against the accredited person for any loss or damage suffered. Civil penalties and other remedies, including suspension or revocation of the accredited person's licence, should also be available.

In considering the content of this obligation, the Inquiry has considered views expressed by stakeholders, a number of which submitted that the CDR's functionality should not be expanded to include action initiation unless those authorised by consumers to act on their behalf were subject to a duty to act in the best interests of the consumer.[277]

The Inquiry has also considered the obligations imposed on persons providing advice or acting on another's behalf under relevant statutes and the general law, and considered parallels between formal powers of attorney relationships and action initiation under the CDR.[278] As discussed above, these range from obligations to act in the best interests of a person to the statutory duties imposed on credit assistance and AFS licence holders to act efficiently, honestly and fairly.

The Inquiry considers it desirable that the obligations imposed on accredited persons are able to be readily understood, so that accredited persons understand the standard of conduct expected of them. It also notes that while it is appropriate to impose a conduct obligation on accredited parties with respect to action initiation, this will not be the sole source of obligations on accredited persons in initiating actions with the consent of the consumer. Sector-specific and other legal obligations will continue to be relevant, while the CDR regime itself would impose obligations with respect to

[277] For example, Choice submitted that write access should only be granted to businesses acting in the best interests of customers and not receiving payments from other commercial entities when offering write access services, p. 4. The Australian Energy Market Commission recommended, in the context of energy comparison sites, that any party seeking write access within the CDR should be required to be acting in the best interests of consumers, p. 2. FRLC submitted there was a need to examine 'business models that are developed that act in ways that may require a financial advice licence, brokers licence or an AFSL, to ensure that the best interests of the consumer are protected when an accredited third party were to initiate payments in service of advice, broking or any other financial service', p. 21.

[278] Powers of attorney provide a formal mechanism for an individual to appoint another to act, and make decisions on, their behalf. The precise requirements in relation to powers of attorneys vary between jurisdictions. In Victoria, for instance, an attorney's obligations include acting honestly, diligently and in good faith: *Powers of Attorney Act 2014* (Vic), s 63.

suitability, consent, confidentiality, security, customer notifications and other matters, such as outsourcing.

Further, under the model of action initiation proposed in this report, the giving of consent by a consumer to an accredited person is not itself enough to cause the performance of the action by a data holder. It is recommended that the data holder, before progressing an action initiation instruction, must have authorisation from the consumer to accept the instructions sent by the accredited person. While it is proposed that authorisations could be ongoing, as discussed in Chapter 4, the Inquiry considers that for certain actions it may be appropriate to require that a consumer provide authorisation to the data holder at the time the accredited person seeks to initiate an action.

In view of these and other consumer safeguards recommended in this report, the Inquiry considers that 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 doing so. Depending upon the classes of action, potential risks and other factors (such as sectoral regulatory obligations), the Inquiry considers that 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 for any loss or damage suffered. Appropriate and proportionate remedies (including civil penalties and suspension or revocation of accreditation), should also be available.

Recommendation 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.

An inclusive Consumer Data Right

The CDR has been developed for the benefit of consumers. These benefits should be accessible not only to a subset of consumers that are data literate or perceived by business as 'high value', but should extend to all consumers. The Inquiry notes the view expressed in some submissions that as digital innovation has continued to occur in Australia and worldwide, the benefits of digital

innovation have not been adequately shared between consumers.[279] It has been asserted that those who are able to engage with the digital economy and are deemed 'high value' customers will be able to access a new range of benefits, whereas those who are unwilling, unable or whose business is viewed as less desirable will not equally receive these benefits. A contrary view is that by reducing the marginal costs of providing services, the CDR may result in services also being provided to more customers with lower marginal profitability to the service provider. Increased data portability can support the needs of different consumers in a wide variety of ways, but only if consumers know how to meaningfully engage, and there is a range of suitable products available for them to use.

Vulnerable consumers

The CDR opens up new opportunities for consumers to access and share data relating to them and, potentially, to enable others to initiate actions on their behalf. When considering the implications of this for consumers, both positive and potentially harmful, it is important to specifically consider how this will impact vulnerable consumers.

Vulnerability takes many forms, and there is no single model of a vulnerable consumer. As discussed extensively by the CPRC, vulnerability affects many people in many different ways.

> *At its broadest, consumer vulnerability refers to circumstances that make it difficult to use markets or receive adequate products and services, and create risks of harm, detriment or disadvantage. Those circumstances can be individual-based (for example, related to income level, age, disability or health conditions) or market-based (for example, markets can create or exacerbate vulnerability through unfair practices, complex market structures and pricing, and information asymmetries).*[280]

Consumers can find themselves vulnerable due to a number of different circumstances simultaneously, and these circumstances may be 'transient or entrenched conditions in consumers' lives'.[281] The diversity of circumstances that can lead to vulnerability means that policies must be considered from diverse perspectives.

It is also important to recognise that a consumer's vulnerability can change and evolve based on the specific context within which they are operating. For instance, a person who is fluent in one language would likely become vulnerable if required to engage with documents written in another language with which they are unfamiliar. In this way, vulnerability can also be contextual. When designing and implementing new policies, the ways in which these policies could alleviate or address vulnerabilities, as well as whether these policies could expose consumers to new vulnerabilities, should be considered.

[279] Consumer Policy Research Centre submission, p. 6 and Financial Rights Legal Centre submission, pp. 22-23.
[280] O'Neill E, 2019, *Exploring regulatory approaches to consumer vulnerability – a report for the Australian Energy Regulator*, CPRC, p.15. https://cprc.org.au/wp-content/uploads/Exploring-regulatory-approaches-to-consumer-vulnerability-A-CPRC-report-for-the-AER.pdf
[281] Consumer Policy Research Centre submission, p. 6.

Vulnerability online

The experience of a consumer engaging with an online service may be different to how they engage with that service or similar services offered in other ways; for example, in person or over the telephone. This can be beneficial in assisting consumers to overcome some forms of vulnerability. For instance, a consumer considering a service online may be able to engage through a preferred language, enabling them to more comprehensively understand what is being presented and empowering them in a way that may not be possible in person. The ability to receive services online can also reduce the isolating effects of living in more rural or remote areas, reducing vulnerability by enabling greater access to services that would otherwise not have been available. In spite of the dramatic impacts of COVID-19, the ingenuity of Australians in embracing technology has demonstrated some potential ways that greater online engagement can assist in reducing vulnerability.

While some consumers may find that engaging online can reduce their experiences of vulnerability, others may find the opposite, being exposed to new circumstances and vulnerabilities that they would not otherwise encounter. People with lower levels of digital literacy for instance, may be less capable of identifying fraudulent actors online compared to offline, increasing their susceptibility to online risks. The migration of many services to being predominately or exclusively offered online can also result in those without reliable access to the internet finding themselves vulnerable. These people are made vulnerable due to their varying ability to interact or engage with products and services online.

Vulnerability in the data economy

Operating online can also allow consumers' actions to be more closely recorded through the data they create. This similarly changes the potential for consumers to benefit or be exposed to new risks. If this data is collected and used by companies without the express consent of the consumer, then the consumer will be open to new kinds of vulnerabilities.

> *CPRC research repeatedly shows the need for consumers to have greater agency when it comes to their data and information, and the risk of harms and disenfranchisement when they do not.*[282]

Giving consumers greater ability to access and share data relating to them may help to reduce some of these vulnerabilities. For instance, by enabling consumers to share information held by their service provider about their usage of a product with accredited advisors, the consumer can be empowered to negotiate on more even footing.

Increased ability for consumers to allow access to personal data could also increase the ability for innovative fintechs and other data-driven start-ups to create products that help financially vulnerable consumers. A budgeting app may be able to help vulnerable consumers overcome a lack of financial literacy in an accessible way by providing them with details about the long term implications of negative spending habits and nudging them towards positive spending decisions.

[282] Consumer Policy Research Centre submission, p. 3.

Alternatively, products could be developed to assist those without a credit history demonstrate their ability to make strong financial decisions to potential lenders.

Increased data access could enable a financial counsellor to, with their client's consent, more easily gain detailed insights about the client's finances and provide better tailored assistance.

These benefits are dependent upon there being digital service developers able and willing to work, including with consumer representatives, to create products that operate for the benefit of vulnerable consumers.

If consumers are given greater agency over their data, and the ability to initiate actions, there must also be adequate safeguards in place and efforts made to raise consumer understanding of safely engaging with such a system. If not, this greater agency could itself expose consumers to new vulnerabilities. For instance, a malicious actor who obtains sensitive consumer data, either directly from the consumer or through some other means, will be in a much stronger position to prey on them. Alternately, consumers being denied access to basic services should they not agree to share data relating to them could also increase consumer vulnerability.

As a regime designed to give consumers greater ability to access, share and make use of data relating to them, it is necessary that the CDR is implemented carefully to mitigate consumer exposure to new vulnerabilities. In developing the CDR system, structural protections were included where required to protect consumers. As the CDR expands, ways to further support these protections need to be at the forefront of policymakers' minds.

Recommendation 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.

Personalisation

A key goal and benefit of the CDR is that it enables consumers to access third party data driven assistance when dealing with service providers. This will help to even the playing field by enabling consumers to access advice and analysis about options available to them independent of their current service providers. The CDR makes it possible for this advice to be informed by analysis of a consumer's own data, increasing the consumer's ability to identify whether a product or service recommended by others will actually be right for them.

Providers with access to a consumer's CDR data will have a higher level of insight into the customer and be better able to assess matters such as the customer's likely usage of, or ability to afford, a service. In this way, information asymmetries that would otherwise exist between the consumer's

existing and prospective future providers can be overcome, with service providers incentivised to offer better deals to keep or win the customer's business.

Access to CDR data can also be expected to enable prospective service providers to offer services tailored to the particular circumstances of the customer. For instance, if CDR data indicates a customer is very low risk for a loan or does not require insurance for a particular event, they may be offered a better priced loan, or an insurance package tailored to them, covering only the services the consumer actually needs.[283] Customers who may otherwise have difficulty establishing their suitability for a credit product may find that their ability to share their CDR data overcomes these barriers and enables greater access to products.

Conversely, CDR data may reveal that a prospective customer is in fact higher risk, or is less attractive than other customers and with the potential to eventually lead to some consumers having less access to services than they presently do. For example, a customer whose CDR data revealed a history of hardship and payment difficulties could be seen as a less attractive prospect, with providers unwilling to offer them the most advantageous deals.[284]

The Inquiry acknowledges the risk that increased personalisation, while benefiting consumers who are attractive to potential service providers, could be to the disadvantage of others, including those who are unable or unwilling to engage with the CDR. Submissions have recognised that the potential for such impacts would be more likely to arise at some future point.[285] The CPRC, for instance, observes that as markets become more data-driven, the ability of firms to discriminate between individuals will increase. [286]

It is not necessarily the case, of course, that a business deciding not to offer a service to a prospective customer will be inappropriate. Not offering a loan to a prospective borrower unable to afford the repayments is likely to be in the consumer's interests and be an appropriate way for a lender to manage risk. A consumer's capacity to borrow is dependent upon the application by prospective lenders of the applicable lending standards and these will operate whether or not CDR is the channel used. The CDR regime should not and does not seek to replace those laws.

The ability for consumers, including the vulnerable or those experiencing financial hardship, to access the services they require at a price they can afford is, of course, a broader issue that exists outside of the CDR. The scope for an accredited person (such as a competing bank) to use consumer data obtained from a data holder under the CDR to determine whether they are willing to offer the consumer a product or service, or the price at which they will make that offer, already exists with the

[283] Deloitte observed in its submission that the introduction of Open Banking is likely to mean that financial institutions will face competitive pressure to reduce interests rates and fees and that, in response, financial institutions will need to consider implementing strategic pricing, such as risk-based pricing, at an individual customer level, p. 37.
[284] In this respect, EnergyAustralia submits that if energy hardship or payment difficulties data were disclosed to an ADR operating across sectors, there is a risk that an ADR may use the data in a discriminating way in recommendations about banking or other services. EnergyAustralia submission, p. 6.
[285] Financial Rights Legal Centre submission, pp. 62-63, Consumer Policy Research Centre submission, p. 6.
[286] CPRC, 2020, *The experiences of older consumers: towards markets that work for people*.

CDR's current read access functionality. The addition of action initiation functionality would not change this.

As the economy becomes increasingly data driven, the ability of firms to identify and target customers with particular characteristics, such as those experiencing financial hardship or seeking access to short term finance, may increase.

Given the scope for action initiation to smooth and shorten the time required to acquire new products, it is appropriate to monitor the impact of the CDR on the availability and suitability of services offered to consumers (particularly the vulnerable), to ensure that any need to refine regulatory settings is identified.

Encouraging consumer engagement with the CDR

When considering the CDR, it is important to make a distinction between a function and a product. The CDR is not a product and is not generally expected to be used by a data holder to provide services directly to a consumer.[287] Instead, the CDR provides a function enabling a consumer to require those who hold specific data relating to them to share that information with a trusted or accredited person. This person then provides the consumer with a good or service. The benefits that can be provided by the CDR are linked not only to the willingness of consumers to engage with the system, but also the availability of products powered by the CDR that serve the needs of different consumers. To make the CDR a more inclusive system and reduce the risk of a digital divide occurring, it is necessary that barriers preventing consumers from participating are addressed, and that there are incentives to encourage a wide array of services to be provided to cater to consumers' varied needs.

The first step in addressing the barriers that dissuade and prevent consumers from fully engaging with the CDR ecosystem is identifying the causes of these barriers. Though the CDR is not able to address all of the factors that can lead to these consumers being unable to engage with the CDR ecosystem, the Inquiry has identified two causes which further measures could potentially help ease:

- lack of familiarity with the CDR, and
- a general lack of relevant financial, digital and data consciousness.

Increasing consumer familiarity with the CDR

The CDR uses a consent based, opt in model, meaning that a consumer's data can only be shared at their direction. Though this provides protections for consumers from having their information unwittingly shared through the CDR, a number of submissions have raised concerns that consumers are likely to engage with the CDR without adequately understanding the regime or the implications of their agreeing to share data.[288] This could lead to some consumers choosing to engage in the system without adequately understanding the purposes for which they are allowing an accredited person to use their data, and finding themselves unsatisfied with the services delivered. Alternately,

[287] An exception to this is enabling CDR data to be provided directly to a consumer.
[288] Australian Finance Industry Association submission, p. 5.

if the process for sharing data through the CDR is not well advertised and fundamental security principles inherent in the regime are not well understood (for example, the fact that you will never be asked to share your banking password under the CDR), then consumers may be more likely to be subject to attacks by malicious actors seeking to exploit the lack of awareness around the new system (for example, phishing attacks). Both of these situations could lead to unfavourable outcomes for consumers.

It was announced in the July 2020 Economic and Fiscal Update that the Government will be conducting an awareness campaign to increase community understanding of the CDR. This will supplement educational material being provided by the ACCC and OAIC. Through this campaign, it is hoped that consumers will become aware of how they can engage with the CDR and gain an understanding of the privacy protections that have been put in place to facilitate this engagement. Additionally, the Inquiry has recommended measures to assist consumers engage with the CDR consent process, including the CDR dictionary. The Inquiry considers that these measures can be pursued while still enabling businesses to innovate for consumer benefits.[289]

Recommendation 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.

Increasing consumer financial, digital and data literacy

The issues of consumer inclusion discussed above are not unique to the CDR, and CDR educational campaigns or policy changes will not alone inform consumers about all matters required to confidently and independently take part in the digital economy. However, as the digital policy that will most swiftly put consumers in greater control of data relating to them, the CDR should be used, where appropriate, as an opportunity to educate consumers more broadly about the value of information that their actions generate, and the potential impact of sharing this information. As noted in the Open Banking Review, the inability of a consumer to understand the value of their information impairs the consumer's ability to make truly informed decisions with respect to it.[290] Without broader community understanding of these issues, consumers will fail to participate fully in the CDR, and the varied needs of all consumers will not be reflected in the products made available.

In discussing the requirements placed on consumers to meaningfully engage with the CDR, the Australian Banking Association raised the need for consumers to have financial literacy, digital literacy and data literacy. The Deloitte submission elaborates further on this by extending the need from 'literacy' to 'consciousness'. Deloitte asserts that 'literacy' only extends to a consumer's ability to understand information, while 'consciousness' also includes a consumer's willingness to seek out

[289] These additional measures are discussed in Chapter 6.
[290] Open Banking Review, p. 112.

information and their ability to use this information to inform how they act. For a consumer to fully engage with the CDR, financial, digital and data consciousness will all be required.

In this context, financial consciousness refers to the need for consumers to have an understanding of financial systems to engage with many of the products and services enabled by the CDR.

> *[I]f consumers are going to take advantage of the benefits of Open Banking, and open data when the CDR is applied to other sectors of the economy, or make informed choices about banking products, they will need to understand the differences in financial value between different offers.*[291]

For instance, although the CDR may make it easier for a consumer to receive information and comparisons about the different products on offer, financial consciousness is still required for consumers to be able to understand this information and make an informed decision about the product that will best suit their needs. Material to assist Australians improve their financial literacy and capability is available on the moneysmart website.[292]

Digital consciousness is understood by the Inquiry to mean having a sound understanding of how digital services are offered and how to engage safely online. This would include understanding of key security principles like keeping sensitive personally identifying information (such as passwords) secure, as well as a broader willingness to seek more information about services offered online and allow this information to influence digital decisions.

Data consciousness is likely to be the newest of these concepts to consumers, being an understanding of how data about their actions is collected and used for decision making and an ability to confidently engage in decisions to share data to empower themselves.

> *Data consciousness would enable people to provide express consent when deciding to share information; to provide informed consent based on an understanding of how the data recipient will be using the information shared; and to be able to understand the value that they are receiving in exchange for the data they are providing.*[293]

There are both government and non-government materials online that can assist consumers in gaining this understanding, but there is currently limited focus on their importance. As such, consumers are unlikely to seek out this information or allow it to influence their behaviours online.

Although the CDR is designed to make it easier for consumers to act in a safe and data conscious way, its safeguards cannot completely substitute for consumer education. Attempting to do so would result in the regime becoming overly prescriptive and stifling innovation, restricting the benefits that could be made available to consumers. Wider education on safely and consciously engaging in the data economy, along with a continued emphasis on financial literacy, should assist in driving consumer engagement with, and benefits from, the CDR.

---

[291] Australian Banking Association submission, p. 16.
[292] moneysmart.gov.au
[293] Deloitte submission, p. 10.

Promoting inclusive product development

Data securely shared through the CDR has the potential to support an extraordinary variety of use cases. Common uses cases include more tailored product comparison and switching services, account aggregators, and loan assessment services, but these represent only a subset of possible products.

Innovation that benefits all consumers

A variety of products must be offered for the CDR to benefit a wide range of consumers. For a business to be able to cover their operating costs, including the cost of becoming accredited to operate within the CDR, it will need to be able to profit from providing its services. CDR businesses are, therefore, most likely to create products for digitally engaged consumers from whom they are able to profit. The CPRC expressed the view in their submission, that 'direct or incentivised government investment to support the design and application of 'data for good' technologies in competitive market settings' would likely be required in order to realise many of the proposed benefits for vulnerable consumers.[294]

In their submission to the Inquiry, Super Consumers Australia suggested the following proposal:

> *Consumer organisations should be funded to develop non-commercial, conflict-free services. They are uniquely placed to ensure the data is analysed and presented purely in the interests of consumers.*[295]

Such a proposal could prove effective for bolstering the range of services provided to consumers, however it would likely also require ongoing government participation to be effective.

Initiatives run in the context of UK Open Banking have sought to encourage innovation which benefits specific consumer groups or attempts to resolve specific problems. This additional incentive has come in the form of funding for innovative developers through a variety of partnered challenges, including Nesta's 'Open Up Challenge' and Nationwide's 'Open Banking for Good' (OB4G), originating out of the Inclusive Economic Partnership. The 'Open Up Challenge' supported fintechs and other data driven businesses looking to use Open Banking to solve challenges faced by small businesses, while OB4G seeks to provide services to help the financially vulnerable with challenges within the categories of 'income and expenditure', 'income smoothing', and 'money management and help'. Examples of fintechs whose product development has been supported through such a program have included:

- *Tully* – a budgeting and debt management service aimed at helping empower users to address issues of money management, and

[294] Consumer Policy Research Centre submission, pp. 6-7. Professor Jeannie Paterson made a similar point in her input to the Inquiry.
[295] Super Consumers Australia submission, p. 18.

- *Touco* – a product designed to allow consumers suffering from mental health conditions seek support in managing their finances.[296]

The Inquiry considers that initiatives that seek to encourage the development of products that use the CDR to assist specific consumers groups are worthy of exploration. Consumers could benefit, and the CDR would be strengthened, if data-driven business and others with good ideas were encouraged to create and develop products to assist consumers, including those with vulnerabilities. Encouragement could potentially range from development funding, access to expert advice (from consumer representatives, developers and others), to a platform to promote and help consumers find their product.

Recommendation 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.

Involving consumers and consumer representatives

The needs of vulnerable people are not uniform, and even the most well-meaning products could potentially result in harm to some groups of consumers if not well-understood or designed with them in mind.

It was apparent from the Inquiry's consultations that the benefits of engaging with consumers, and consumer advocates, when designing the CDR regime and developing products using the CDR, are significant. At present, however, consumer advocacy groups generally lack the resourcing required to engage deeply.[297]

Interested consumers and consumer advocacy groups can provide important input which can help to ensure that the CDR system, and the products enabled by it, do not increase consumer exposure to vulnerability.

[296] Nationwide, *Seven FinTech firms join forces with Nationwide to address financial capability issues*, 23 April 2019, https://www.nationwide.co.uk/about/media-centre-and-specialist-areas/media-centre/press-releases/archive/2019/04/23-open-banking-for-good The Inquiry notes that Touco was known as Toucan when chosen to take part in OB4G. While Tully assisted clients with budget and debt management in 2019, with the onset of the Covid-19 pandemic they pivoted to helping people financially impacted by the pandemic to register for payment relief. https://www.tully.co.uk/about-us-covid

[297] Financial Rights Legal Centre submission, p. 9.

Recommendation 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.

Quality of comparison services

CDR data sharing enables comparison and advice services to provide more accurate, tailored advice to consumers, reducing complexity and increasing consumers' ability to locate a better deal. However, a consumer's willingness to accept that advice and switch via the CDR, will be influenced by whether they trust that comparison or advice service.

Comparator websites have been found to be one of the top three influencers of consumer's switching behaviour. However, while they are influential when helping people understand product information, many people may not yet trust them enough to provide them with their customer account and banking transaction information.[298] This lack of willingness to purchase via these entities stems from doubt about their motivations in making particular recommendations and the benefits they offer.[299]

Concerns regarding the disclosure of these entities' market coverage, their relationships with service providers and the use of commission-based incentive structures were raised in submissions to the Inquiry, and have also been raised in a number of earlier inquiries. In its 2018 Communications Sector Market Study, the ACCC found that 'comparator websites must fully and prominently disclose their commercial relationships, ranking methods and market coverage. In the absence of full and prominent disclosure, comparator websites can mislead consumers as to the extent of the comparison service, the amount of savings that can be achieved and the impartiality of the comparisons.'[300]

Similar findings were made by the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (FSRC) in regards to intermediaries and mortgage brokers. The FSRC found that while those entities played an important advisory role for many consumers, conflicted remuneration and trail commissions could be reasonably expected to influence the choice of product presented to the customer and operate to align the broker's interest with the lender rather than the borrower.[301]

[298] Deloitte, 2019, *Open banking: switch or stick? Insights into consumer switching behaviour and trust*, p. 41.
[299] Deloitte, 2019, *Open banking: switch or stick? Insights into consumer switching behaviour and trust*, p. 41.
[300] ACCC, 2018, *Communications Sector Market Study final report*, p. 125.
[301] This practice was significant in leading the FSRC to find that mortgage brokers should have a formal duty to act in the customer's best interest.

In the 2018 Retail Electricity Pricing Inquiry (REPI) the ACCC considered concerns that commercial comparators' websites and their sales teams may not always adequately disclose their fees and commissions, that comparators do not ensure that customers are fully informed about their decisions and that commissions received by third party intermediaries may influence the offers they recommend. While the ACCC found that the ACL could be applied to address these concerns, it did not consider that they could be adequately addressed through enforcement of the ACL alone and recommended a mandatory code of conduct for third party intermediaries.[302] The ACCC also suggested the Government consider extending a mandatory code of conduct for intermediaries beyond the energy sector, noting that many also offered services into other sectors.

Submissions to the Inquiry on this issue largely focused on the behaviours of comparator services in the energy market in the wake of the REPI. There were general assertions that the conduct of third parties was often not in the best interest of consumers, however support for a third party intermediary code was generally qualified. A number of submitters noted this as one of several issues to be addressed in the energy sector before any CDR write access was contemplated.[303] Another submission referred to concerns about the practices of intermediaries and their influence on consumer confidence.[304]

The Inquiry notes the ACCC's analysis and recommendations regarding the behaviours of comparator websites, as well as the submissions received from interested parties on this issue. However, given these concerns exist regardless of the availability of the CDR in a sector, the Inquiry considers that pursuit of a regulatory response is best addressed outside the CDR regime to ensure that the response is able to address the concerns comprehensively.

The Inquiry notes that where businesses use the CDR to offer comparison services, those businesses will be subject to the additional obligations and consumer safeguards required by the CDR, in addition to the ACL and other obligations. CDR data sharing and the ability to electronically compare the Product Reference Data of all products on the market should improve services offered by comparator services that use it, as it allows sites to draw on a wide range of data, and make recommendations tailored to the consumer's needs, based on their actual usage data. Over time, this will exert competitive pressure on all providers to improve the quality of services they offer.

[302] ACCC (2018) *Retail Electricity Pricing Inquiry final report,* pp. 277, 282. See also recommendations pp. 34-35.
[303] Red Energy and Lumo Energy joint submission, p. 2, Energy Australia submission, pp. 5-6.
[304] AEMC submission, p. 2.

Privacy and information security safeguards

Current privacy and information security protections in the Consumer Data Right

Privacy protections

Each Australian Privacy Principle (APP) has an equivalent but more onerous CDR Privacy Safeguard. The exception to this is APP 12 Access to personal information, for which the entirety of the CDR is the enhanced equivalent.

The Privacy Safeguards, while generally consistent with the APPs, are more restrictive and, in conjunction with supporting Rules, are more detailed than their equivalent APPs. In addition the Privacy Safeguards include Privacy Safeguard 10 which relates to notification of disclosures of CDR data for which there is no equivalent APP.

The Privacy Safeguards have broader application to catch all designated and derived data relating to identifiable natural and legal persons and to bind all ADRs in respect of CDR data they've received. Most of the Privacy Safeguards – with some exceptions – do not apply to data holders. This reflects that the Privacy Safeguards generally apply only to protect data within the CDR system and that it is not the role of CDR to displace existing sectoral requirements for the protection of data. Data holders are instead subject to their existing obligations. These may include those imposed by the Privacy Act in relation to personal information and common law and equitable duties. They may also be subject to sector-specific requirements such as duties of banking confidence, prudential obligations regarding security of information and the like.

The stronger protections included in the Privacy Safeguards seek to mitigate risks associated with more convenient and higher velocity transfers of valuable machine readable data, and to instil high levels of consumer confidence in the use of the system.

In addition, small to medium businesses accredited under the CDR are also subject to the Privacy Act where they are otherwise not captured.[305] The CDR provides that the general exception in the Privacy Act applying to these businesses is not available to entities that obtain accreditation to receive data under the CDR. This means the Privacy Act will apply to accredited persons in respect of personal information generally (other than CDR data, in relation to which the Privacy Safeguards instead apply). The Privacy Safeguards protect CDR data held by ADRs.

Under the Privacy Act serious or repeated interferences with the privacy of an individual (which can include breaches of any APP) attracts a civil penalty (up to 2000 penalty units and five times that for

[305] The Privacy Act defines SMEs as businesses with annual turnovers of less than $3 million.

corporations). The Government has announced an intent to increase penalties under the Privacy Act to align with those for the CDR Privacy Safeguards.[306]

Breaches of most Privacy Safeguards attract civil penalties, with no requirement for breaches to be serious or repeated – with penalties capped for individuals at $500,000 or, for corporations, at the greater of $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual domestic turnover of the entity committing the breach. This aligns with broader competition and consumer law penalty amounts. Unlike the Privacy Act, there is no requirement that breaches of the CDR Privacy Safeguards be serious or repeated.

In addition to Privacy Safeguards being hardwired into the CCA, the framework provides flexibility to respond to emerging privacy risks, through rulemaking and standard setting processes. The ACCC may make additional Rules regarding the transfer, holding and use of data within the system, building upon the Privacy Safeguards. The DSB may make technical standards to support the operation of the Privacy Safeguards and any further protections in the Rules – for example, information security standards.

Breaches of more specific Rules can also attract civil penalties up to an amount specified in the Rules. While maximum penalties are less for some Rules, generally these are capped for individuals at $500,000 or, for corporations, at the greater of $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual turnover of the entity committing the breach.

Information security protections

Privacy Safeguard 12 imposes obligations with respect to security of CDR data. It applies to CDR data held by an ADR and requires taking steps to protect CDR data from misuse, interference, loss, unauthorised access, modification or disclosure. There are supporting Rules that specify the information security requirements to meet this Safeguard.[307] These requirements refer to the information technology systems used for, and processes that relate to, the management of CDR data. In addition, there are also information security requirements in the CDR standards made by the Data Standards Chair, which are applied through the Rules.

The general rulemaking power can also be used to impose security and privacy requirements independent of the Privacy Safeguards.[308]

[306] Joint media release by the Hon Christian Porter MP, Attorney-General, and Senator the Hon Mitch Fifield, Minister for Communications, Minister for the Arts, *Tougher penalties to keep Australians safe online*, 24 March 2019.
[307] For example, Part 2, Schedule 2 of the Rules.
[308] Paragraph 56BB(f) and section 56BJ of the CCA.

Adequacy of current Privacy Safeguards and information security requirements for action initiation purposes

The current Privacy Safeguards are crafted to provide protections to data being collected and used in the context of CDR data sharing.[309] This limits the ease with which they can readily be adapted to provide equivalent or tailored protections for action initiation and, in particular, the instructions that an ADR sends to a data holder to initiate an action. Currently, the ACCC's general rulemaking power is more suited to crafting protections for other kinds of data collected or created through the use of the CDR regime.

Action initiation will require additional data to be exchanged between the consumer and the accredited person and the accredited person and the data holder to realise the action. This will include:

- authorisations and consents for instructions to act (discussed in Chapter 6)
- instructions to act (accredited person to data holder), and
- responses to instructions to act (data holder to accredited person and possibly also data holder to consumer).

As mentioned above the ability to initiate actions on behalf of a consumer may sometimes have greater potential for harm than ongoing data sharing arrangements, depending upon the nature of the instructions and the content they include. For example, an instruction may be created to:

- change the consumer's address and will include details of the new address (see example in Figure 4.1 Sarah's new home in Chapter 4); and
- pay a certain amount to another individual and will include that individual's bank account details.

It is foreseeable that, if compiled over time, elements of this instruction data would provide a proxy for transaction data and provide insights into consumer habits.

Currently instructions to act and the data they contain may be classed as CDR data to which the Privacy Safeguards apply, if that instruction includes data accessed under CDR data sharing or derived from such data.

However, future action initiation use cases will not necessarily require that data is first accessed using data sharing under the CDR. Instructions to act provided in the example in Figure 4.1 Sarah's new home may not be data to which the Privacy Safeguards apply and therefore, to the extent it is considered personal information, that instruction to act may instead be protected under the APPs. Similarly, most information security requirements in the Rules only apply to CDR data. However, as these requirements reside in the Rules as opposed to legislation they may be more readily adapted to cover authorisations, consents and instructions data in an appropriately tailored way.

[309] The Privacy Safeguards apply to CDR data in relation to an identifiable consumer.

It is highly desirable for privacy and information security requirements to apply consistently to these data sets. It will be important to address the issue that, to the extent that some action initiation instructions include data obtained or derived under CDR data sharing, different protections will apply potentially creating complexity for ADRs in managing their privacy and information security obligations.[310]

It should be noted that the current Privacy Safeguards are not designed specifically with these types of data in mind. They are, therefore, unlikely in their current form to deal with all relevant issues that may arise in the action initiation context. They would also apply requirements that may not be necessary or appropriate.

Privacy and information security assessments must take place to ensure that proportionate and appropriate protections are in place for sensitive data sets of these kinds.

A key challenge with the CDR is to ensure that privacy and information security arrangements are tailored and proportionate to the different data types and risks, while also avoiding complexity which harms consumer comprehension and exercise of their rights and imposes undue costs on participants. The current regime, generally:

- imposes one set of higher privacy and information security requirements on CDR data that is collected or used through the system,[311]
- leaves all other data to be subject to the privacy protections that would otherwise apply, such as the Privacy Act, and
- applies a range of other specific information security protections for other types of data required to action the sharing of CDR data.[312]

This categorisation of data types and corresponding level of regulation was extensively consulted upon and considered as part of the Open Banking Review and the subsequent development of the legislative framework. The Inquiry acknowledges that a range of stakeholders in those earlier consultations and in submissions to the Inquiry suggested uniform privacy protections – although with diverging views as to what those protections should be. While the privacy and information security treatment for action initiation instructions, consent and authorisations made under the regime should be reviewed, the Inquiry does not propose to revisit this overall approach.

At the same time, the design of appropriate privacy and information security requirements needs to remain consumer focused. It would risk undermining trust and confidence in the CDR regime if

[310] Concerns about the confusion, complexity and burden of two overlapping privacy regimes were raised in the Law Institute of Victoria's submission, pp. 9-10. In addition the Law Institute of Victoria was of the opinion that this complexity may undermine the economic benefits hoped to be obtained through increasing the ability of organisations to share and utilise data. Disjunction between privacy regimes can affect the choice to use, store and secure personal information and CDR data.
[311] Including data derived from data collected through the system.
[312] For example, encryption and other information security requirements for transmission of instructions. These protections are mainly provided for in the standards.

action initiation, a function that if misused could potentially expose a consumer to greater harm than the current data sharing, was to be accompanied by inadequate privacy protections or redress.

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.

The further expert analysis which is required as part of amending the Act to enable action initiation, as outlined in Recommendation 4.2 will be necessary to achieve the right outcome.

The designation process requires the Minister to consider the privacy and confidentiality of consumers' information, which in practice would be actioned by undertaking a privacy impact assessment.[313] The Minister must also consult the OAIC which must independently analyse the designation instrument and the impact on privacy and consumer information and report to the Minister and make its report public.[314] Similar analysis is also required at the rulemaking stage.[315]

Recommendation 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.

Upcoming Privacy Act review and consideration of recommendations of the ACCC's Digital Platforms Inquiry

The Inquiry is aware that the Government will shortly commence a review of the Privacy Act, included will be consideration of the privacy related recommendations of the ACCC's Digital Platforms Inquiry (DPI).

Recommendation 16 of the DPI proposed strengthening the Privacy Act in ways that would bring the Privacy Act into greater alignment with the CDR, extending certain protections currently offered by the CDR across the economy.

[313] Sub-paragraph 56AD(1)(a)(iii) of the CCA. Proposed amendments to the CDR legislation and the designation framework would see the responsibility for this element of the designation process shift from the Minister to the Secretary of the Treasury.
[314] Sub-section 56AD(3) and section 56AF of the CCA.
[315] Section 56BP of the CCA.

It should be noted that requirements that may be suitable for participants in the CDR regime – which deals with digital interactions in highly structured data by persons specialising in the provision of data driven services – may not be appropriate more broadly. Additionally, for noting is that the CDR does not purport to identify the minimum reasonable necessary protections for data portability in general.

DPI recommendation 17 recommended broader reform of the Australian privacy law including some elements which have parallels with the CDR regime. These include greater emphasis on privacy protections for data and the consideration of whether the application of the Privacy Act should be extended to some entities which are currently exempt, including small businesses.

Other aspects of recommendation 17 include reforms which would impact the current CDR framework such as consideration of protections or standards for de-identification, anonymisation and pseudonymisation of personal data to address risks of re-identification of data sets or protections around inferred information and possible outcomes of combined data sets.

In its response to the DPI the Government was focused on the need for the Privacy Act review to look at where consumer privacy protections can be improved while allowing for innovation and growth of the digital economy and how it empowers consumers and protects their data. The Inquiry flags these points of intersection on privacy matters in the data and digital landscape.

Chapter 8: Opportunities for connecting the Consumer Data Right to the data economy

For the CDR to reach its full potential, opportunities to integrate the CDR with other data systems and frameworks should be explored. This chapter considers the following areas where relationships could develop:

- making identity verification and customer authentication interoperable with existing and emerging processes
- leveraging data standards setting capabilities to encourage consistent standards across the data economy
- leveraging the CDR accreditation process
- linking the CDR to the AI ethics framework, and
- linking the CDR to international data portability regimes.

Customer authentication in the Consumer Data Right

The purpose of customer authentication in the CDR is to provide data holders or accredited data recipients with sufficient confidence that they are dealing with the right customer. Authentication ensures that authorities to collect, use or disclose data are given by persons who are entitled to do so. It also enables data holders or accredited data recipients to restrict the availability of customer data or CDR driven services to those entitled to access them. There are also various rights under the CDR regime that can only be accessed by the relevant customer.[316]

Difference between identity verification and customer authentication

Customer authentication in the CDR is designed to provide a level of assurance that the request to provide access to data came from the correct existing customer of the data holder. The CDR does not refer to nor require a particular method of digital identity verification. Identity verification and customer authentication are two distinct and separate processes. Box 8.1 defines the differences between these processes.

[316] For example, rights to access consent dashboards, access to records, deletion rights, correction rights.

As the CDR regime has evolved it has become clear that issues related to digital identity verification in Australia and the operation of the CDR regime are connected. Both are drivers and enablers of the data and digital economy that serve different purposes.

Developing methods that provide secure and trusted digital identity verification is recognised as a crucial element to encouraging greater trust in the use and growth of public and private online services. In this setting, it is important that an individual's identity can be verified to an appropriate degree of certainty that reflects the risks of incorrect identification. Doing this may require a range of unique personal identifiers, a digital equivalent to the 100 point identity check.[317]

The infrastructure that enables the CDR is a business-to-business communication framework. Over this infrastructure passes the confirmation:

- to use and access consumer's data, and
- with the expansion into action initiation, to take actions on the consumer's behalf.

The CDR also functions to pass that data to the approved entity. The CDR does not require a consumer's identity to be verified, rather, the CDR is intended to interoperate with digital identity solutions that provide appropriate and secure methods of authentication.

Box 8.1 – Key identification definitions

Identity verification is the use of a unique personal identifier or identifiers to prove the identity of a person.

Customer authentication is confirming that the person seeking to access services is the customer who is linked to an identifier or identifiers previously provided to (or by) the service provider, e.g. that they are the holder of the account from which data is sought.

Expansion of the CDR to include action initiation necessitates consideration of whether the current authentication requirements established for data sharing are sufficiently appropriate and robust to also be applied to that function. As the CDR expands to contain many and multi-sector data sets that can be accessed for a range of CDR functions, more granular consideration is needed of the appropriate authentication level for a greater breadth of consumer data.

Discussion of the relationship between the CDR framework, customer authentication and identity verification is necessary when considering its application to the banking sector and the KYC obligations under the AML/CTF Act.

[317] The 100 point identity check is a method of verifying an individual's identity using a range of key identifying documents. Points are allocated to the types of documentary proof of identity the person can supply, and they must have at least 100 points of identification. Examples of identifying documents include passports, driver's licences, Medicare cards, bank cards, marriage licences and utility bills. In banking an individual must supply 100 points of identification to be able to open and operate an account.

Competitive environment for customer authentication solutions

Currently the CDR imposes a specific way for data holders to authenticate their customers as part of the process to authorise disclosure of data. There is no such prescription upon accredited data recipients (ADRs) in relation to how they meet their customer authentication requirements.

The CDR should support participants to use their choice of authentication provider (or internally developed authentication solutions) when designing and offering CDR-based services provided those solutions are interoperable with the CDR and are sufficiently safe and convenient. This will help reduce accredited persons' costs, and avoid them having to use different assurance solutions for CDR and their other services.

Potential authentication providers should be able to include solutions developed as part of more comprehensive digital identity solutions, notwithstanding that the CDR does not require all elements of such solutions, such as identity verification functions.

Australia currently has two primary frameworks for digital identity verification providers. The Trusted Digital Identity Framework (TDIF) is the Australian Government's framework for accrediting providers of identity assurance for government services online.[318] It is based on international digital identification related standards. The Digital Transformation Agency determines whether a digital identification provider meets its accreditation requirements for both identity verification and authentication which includes strict privacy, fraud and security requirements.

The Australian Payments Council is developing the TrustID Framework, administered by the Australian Payments Network (AusPayNet). This framework has been developed by a range of commercial and government partners, including major financial institutions, retailers and payment systems. The TrustID framework is designed to support an interoperable network of digital identity solutions with a focus on private sector requirements for identity assurance. The framework has been designed to interoperate with the TDIF and use the same standards and specifications as the CDR.[319]

There is also a range of commercial identity service providers offering identity verification and customer authentication solutions.

---

[318] There are currently two TDIF accredited providers for identity services:
- Australia Post's Digital iD – originally intended for use in accessing government services and now expanding into broader commercial application
- Australian Taxation Office's myGovID – which is specifically for accessing government services.

TDIF accredits both identity service providers and credential service providers. Services accredited under the TDIF must also adhere to international digital identification standards.

[319] Australian Payments Council, 2019 Annual Review, p. 6: https://australianpaymentscouncil.com.au/wp-content/uploads/2019/12/APC_Annual_Review_2019.pdf

At the moment digital identity services are not mature, with limited take-up and use of any digital identification service. For many businesses customer authentication or identity verification processes are still largely analogue. However, in time it is likely Australia will see the emergence of a competitive market for digital identity solutions that provides strong value propositions for both consumers and businesses.

When digital identity services are broadly adopted, the Inquiry envisages a future where consumers may be able choose from a market that includes government and commercial identity assurance providers, supporting consumers' choice of identity provider and allowing consumers to use the provider (or providers) they most trust with their personal information.

Recommendation 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.

Customer authentication for future Consumer Data Right functionality

Recommendation 4.15 outlines the Inquiry's response to customer authentication by accredited persons offering services involving action initiation.

The method of authentication presently required to be used by data holders is one-time password (OTP) authentication.[320]

OTP is a recognised method of supplying identity credentials and adheres to international digital identification standards including NIST 800-63[321] and OpenID Connect.[322] It was a suitable method to adopt for Open Banking data sharing functions as it met the safety and customer experience needs required of a consumer data sharing system. It was also a method that banking consumers were already familiar with as a system used by many banks.

While the banking sector had an established practice of OTP authentication prior to the development of the CDR, this is not the case in other sectors. Requiring OTP authentication for CDR data sharing

[320] Consumer Data Standards: https://consumerdatastandardsaustralia.github.io/standards/#cdr-federation
[321] NIST is the US technology and measurement standards body. It is a non-regulatory body and standards are not mandatory. The relevant NIST Standard is NIST 800-63, Digital Identity Guidelines. CDR's OTP method satisfies NIST standard's second level of assurance and the TDIF equivalent, Credential Level 2 (CL 2)). The TDIF and the Trust ID framework are informed by NIST 800-63.
[322] OpenID Connect is an interoperable authentication protocol which provides a secure mechanism for an application to contact an identity service, get some user details, and return them to back to the application in a secure way. OpenID Connect is administered by The OpenID Foundation, a non-profit international standardization organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies.

as a general CDR requirement risks establishing a stricter assurance standard than currently exists for online interactions in some sectors and may impose significant compliance costs.

The Inquiry considered a non-regulatory approach to authentication and whether authentication requirements could be determined by individual CDR participants in future sectors. However, the Inquiry came to the view that this approach would not deliver the consistency and security needed to provide consumers with confidence that their data was secure and being handled appropriately and risked undermining the objectives of the CDR regime.

A minimum assurance standard for authentication

The CDR of the future will require a mechanism for ensuring that authentication for different data sets in different sectors can appropriately reflect the nature of the entity seeking authentication, the nature of the data, its sensitivity and the degree of harm to a consumer from any misuse.

While authentication obligations should require participants to assess the risks associated with their services and, therefore, the appropriate level of assurance needed in authentication, there should be a floor set for minimum safety levels reflecting the risks associated with given data or activities.[323]

A minimum assurance standard for authentication required by CDR participants should be determined by the DSB and be based on the following principles:

- it supports a competitive marketplace in authentication solutions
- is interoperable with the TDIF and TrustID, at a minimum
- is applicable for all sectors in which the CDR is implemented, now and in the future
- is developed in consultation with relevant regulators, and
- has regard to current physical verification requirements for similar functions within respective sectors.

The Inquiry notes that the NIST 800-63, Digital Identity Guidelines standard has three tiers of authentication assurance (as well as standards for determining appropriate authentication levels to be used) and considers this a useful guide for determining tiers of authentication assurance.

Creation of overly granular levels would introduce excessive complexity and cost and may, consequentially, harm consumer outcomes.

[323] The current one-time password authentication method would be recognised as one authentication solution that met or exceeded this minimum standard for all the data sets currently covered in open banking for read actions. This uniform solution may exceed the assurance level set in the minimum assurance standard for the reading of some of those data sets. Conversely, it may not be sufficient for some actions to be initiated in relation to those data sets (for example, updating personal information).

Development of this standard will also require a consumer experience overlay to make sure consumer participation is simple, informed and encourages trust in the data sharing experience when engaging with the requirements of identity assurance.

Recommendation 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.

Levels of assurance to be determined by reference to the risk to the consumer

The level of customer authentication required for access and use of data by CDR participants should be reflective of the level of risk to a consumer if data is misused. Authentication requirements should be based on the nature of the data and the likelihood of harm. It will be necessary to examine the risk to the consumer presented by different CDR functions or data sets in each sector. This will become increasing important as the CDR expands to include more and multi-sector data sets which can be accessed or combined for a range of CDR functions.

The minimum assurance standard should include a process for making an informed and consistent assessment of risk when determining the commensurate level of authentication. This should include the risks of access to particular data sets and the risks of undertaking particular functions, noting that this may differ across sectors.[324] For example, payment initiation, as a higher-risk activity, is subject to strong customer authentication requirements under PSD2.

This is a departure from the current single method of authentication required for data sharing and will require both CDR participants and consumers to adapt to the use and provision of a range of authentication requirements for CDR data related services.

[324] This approach aligns with observations made by Deloitte in its submission which identified that as CDR expands to other sectors and includes write access, more sophisticated authentication systems may be required. Deloitte also observed that over time users are likely to want to see consistent levels of assurance being used across both data holders and ADRs. Deloitte submission, p. 30.

Recommendation 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.

Consumer Data Right could authenticate consumers for commercial Know Your Customer requirements

While identity verification is a requirement for the banking sector, different sectors impose their own KYC requirements either due to regulatory requirements or are considered necessary for commercial purposes.

For example, a non-bank service provider may want a form of identity assurance to ensure that they are providing a service to a 'real' person who will pay their bills.

The authentication requirements of the CDR may create a weak form of identity assurance to meet the commercial verification needs of some firms. However it is unlikely to meet any regulated requirement for identity verification.

This level of authentication could assist with switching in industries that are not subject to identity verification requirements. For example, when a person authenticates using the CDR requirements in the energy sector, a new service provider may be satisfied of the new customer's identity. This may allow the customer to switch energy accounts.

Leveraging standards setting and the Data Standards Body

Data Standards Body and Consumer Data Right Standards

The DSB is responsible for assisting the Data Standards Chair (DSC) in the development of common technical standards and associated guidelines. The standards and guidelines allow Australians to access data held about them by businesses and – if they choose to – authorise or require the sharing of this data via APIs with trusted, accredited third parties. In close consultation with the ACCC and OAIC, the DSB designs and develops the open standards as the CDR is applied to new sectors.

The DSB also develops Consumer Experience Standards and Guidelines to provide CDR consumers with simple, informed and trusted data sharing experiences.

Technical aspects of CDR standards are supported by open work streams that make recommendations to the DSC relating to information security, API structure and formats. They are also accountable for documentation and reference materials to support the understanding and implementation of the standards. These working groups draw upon knowledge and experience from

international and domestic communities. Understanding of standards is supported by the DSB through initiatives such as their CDR Implementation Calls and their CDR Support Portal.

Advisory committees for designated sectors provide further support to the DSC, offering strategic counsel and expert advice from a range of stakeholders, including sector participants, fintechs and consumer bodies.

Benefits of consistent data sharing methods across the economy

Data standards developed for use by government and private sectors are generally based on existing knowledge of standards in these sectors and individual needs. Promoting the use of common standards between the CDR and other parts of the digital economy will make it easier for new data sets and APIs to join the CDR by reducing technical barriers to entry. Placing technical IT requirements for the CDR in data standards rather than enshrined in legislation also allows the CDR to respond to changes in the broader IT ecosystem.

While in some cases there may be good reasons for the use of bespoke standards, generally they will act as a barrier to operating with other participants in the digital economy, including support services, and drive up future costs for operators. The centralised CDR approach to data standards development places consistency and interoperability higher in priority when new standards are introduced into the data economy.

The application of universal rules and standards will enable the better use of common service providers in the data supply chain. Consistent standards mean technical or security updates can be applied more efficiently when required. Common problems could be solved more easily with common solutions offered by specialist service providers.

For existing government IT systems and APIs, various government agencies already impose data standards covering aspects such as information security, means of transmission, acceptable formats, customer authentication, service provider authentication and consumer experience requirements for data transfer. A lack of consistency and interoperability in these standards creates inconveniences and inefficiencies for businesses and consumers, such as when needing to use multiple digital solutions. These inconsistencies may lead to duplication of effort when new standards are designed, making it harder for a critical mass of expertise and capability to develop in the agencies charged with developing and maintaining them. Opportunities to align with economy wide and international standards for digital products and services will also suffer if a fragmented approach is adopted.

Broader application of standards developed for one part of the digital economy will lead to a more consistent experience for developers and users of data. The government has announced that a Data Standards Audit will be undertaken to review the current standards used in Australia's digital economy, and where opportunities may exist for coordination or improving consistency.

The existing ability for industry to leverage CDR standards and guidelines developed by the DSB may allow the API structures, consents, authorisations and security approaches designed for the CDR to spread beyond the CDR ecosystem. Continuing to leverage the DSB will be necessary to simplify

standards for consumer experience;[325] the NPPA's drawing upon CDR consumer experience guidelines is an example of this.[326] Over time this could improve data utility as existing data sets could be made available for use by more parties. Data collected across multiple different industries that use common standards can then be leveraged with consumer consent to better inform service providers.

Potential extension of the Data Standards Body role and use of standards

Development of non-Consumer Data Right private sector data standards

DSB standards are technical standards. They are more detailed than the higher level standards developed by other government bodies, and require a specialised skill set. The required open source publishing of CDR standards already allows those outside the CDR to observe the DSB designed standards for existing CDR participants, and those outside the CDR are able to use these standards when developing their own APIs.

Aligning data sharing standards and processes across industries is consistent with the core principles of data portability, and will reduce transaction costs for consumers in using their data across the economy.[327] Where the private sector is unable to coordinate development of their common standards, there is an opportunity for the work being conducted by the DSB to be leveraged to develop API-based interoperable ecosystems. This would result in more value being generated for consumers by the CDR regime, as information security standards would apply more consistently inside and outside the CDR, along with a more consistent customer experience.

One possible means of encouraging integration with the CDR regime would be to allow consultation with the DSB for the development of non-CDR specific industry standards. Many industries would be able to develop standards interoperable with the CDR using their existing expertise and API capability, so allocating DSB resources to this goal should not be necessary. Where participants do not wish to introduce new data sets as voluntary CDR data, they can still leverage the open source CDR standards without requiring consultation with the DSB. The DSB is funded to provide support for the scope of the CDR regime and not to act as a nationwide API support body.

Government data, data services and data regulation

The use of data is becoming increasingly important for the government to better develop policy and deliver services to Australians. As per the government's Public Data Policy Statement, the Australian Government commits to:

- optimise the use and reuse of public data

[325] Experian submission, p. 10.
[326] New Payments Platform Australia submission attachment, pp. 4-5.
[327] Commonwealth Bank of Australia submission, p. 2.

- release non-sensitive data as open by default, and
- collaborate with the private and research sectors to extend the value of public data for the benefit of the Australian public.[328]

In addition to proposed legislation supporting better sharing of data held by the government,[329] best practice data management will be required for users. These arrangements are likely to include information security standards.

Government is also increasingly establishing more digital services which include data access arrangements. For example, establishing business to government (B2G) data access arrangements to government registers through the Modernising Business Registers Program.[330]

There are also a number of regulatory arrangements that (directly or indirectly) impose B2G, business to business (B2B) or business to customer (B2C) data transmission or security arrangements upon the private sector; for example, e-invoicing[331] and regulatory technology (RegTech) obligations. As noted by the Productivity Commission in its information paper on Regulatory Technology:

> *Creating and maintaining a regulatory environment that supports the realisation of regtech benefits would mean improving the consistency and structure of data and the interoperability of, and standards for, technology - these are precursors to wider regtech adoption.*[332]

Those benefits include greater insights from increased data generation and availability, along with more straightforward and timely updating or implementation of changes in regulatory requirements.

Licensing regimes also increasingly impose information security obligations, which are currently developed independently by each sectoral regulator. Similarly there are data security accreditation requirements used by government (although not always named as such), that impose inconsistent obligations. For example, the ATO digital service provider (DSP) regime,[333] or the e-invoicing Secure Access Point regime.

A role may exist for the DSB to promote more consistent, more convenient, safer and more efficient technical requirements to support these initiatives. Many of the technical problems that it must solve in the CDR exist in relation to these other initiatives. As referenced above, these standards may cover such matters as information security, means of transmission, acceptable data formats,

---

[328] Department of Prime Minister and Cabinet, *Public Data Policy Statement*, https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf
[329] Office of the National Data Commissioner, *Exposure draft of the Data Availability and Transparency Bill 2020*, September 2020, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22library%2Flcatalog%2F01262505%22;src1=sm1
[330] Australian Government, Australian Business Register, October 2020, https://www.abr.gov.au/media-centre/modernising-business-registers-and-director-identification-numbers
[331] Australian Taxation Office, E-invoicing, October 2020, https://www.ato.gov.au/business/e-invoicing/
[332] Productivity Commission, *Information paper on Regulatory Technology*, October 2020, https://www.pc.gov.au/research/completed/regulatory-technology/regulatory-technology.pdf
[333] Australian Taxation Office, DSP Operational Framework, October 2020, https://softwaredevelopers.ato.gov.au/operational_framework

customer authentication, service provider authentication and consumer experience requirements for data transfer.

An expanded role of the DSB must not result in other government initiatives adopting CDR branded standards, to avoid the perception that they are covered by the CDR framework. The DSB would be developing generally acceptable standards with tiering and customised requirements for different uses – including for CDR.

Where other initiatives impose requirements to comply with relevant standards, they could reference DSB standards which the DSB would then be responsible for developing in consultation with relevant policy, regulatory and administrative agencies.

Consideration should be given to the DSB being the central point for maintaining data technical standards, even where there is little scope of alignment with other domestic standards. This would still enable better development of expertise and economies of scale. It would also provide a central point for Australia's engagement with international technical standard setting fora.

A role would exist for the DSB to develop and maintain standards for disparate data sets held by the Commonwealth, or to develop standards for data held by the government to enable safe and efficient use of data where use cases in the national interest have been appropriately authorised.[334] Where government is offering or imposing a specific licence or access requirement that references information security requirements, the DSB could assist in the development of standards. Such standards could cover where government held data is available for machine readable use by the private sector (for example on the business registers), intra-government data sharing arrangements, or RegTech initiatives that impose data transmission requirements on the private sector.

Recommendation 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.

Leveraging the accreditation regime

The Consumer Data Right Accreditation regime and Register and Accreditation Application Platform (RAAP)

CDR accreditation is a requirement for all data recipients under the current Rules. Accreditation is provided by the ACCC after confirming that among other factors,[335] an applicant's data protection, dispute resolution and insurance coverage meet minimum standards. Once accredited, the successful applicant will appear on the Register of Accredited Persons.

[334] PC Data Report.
[335] For example, that they meet fit and proper person requirements.

Opportunities to leverage the CDR accreditation regime, or for the accreditation regime to recognise external frameworks, should be explored to achieve consistency and efficiency across the data economy, simplifying the 'data start up' process and further integration. This includes the possibility of leveraging one or more of the following:

- the security requirements to keep data safe[336] (accreditation requirements)
- the processes for assessing a person as compliant with these requirements (accreditation processes), and
- the systems for recording and enabling others to verify a person as being accredited (accreditation infrastructure).

Potential for application outside the Consumer Data Right

The 'Data Safety Licence'

The CDR accreditation process is effectively granting a type of 'data safety licence' to ADRs. Subject to any required customisation, other systems outside of the CDR may find such a licence useful to manage participation where secure data holding or transfer is necessary. Properly tiered and non-prescriptive information security requirements should be applicable to a wide range of other activities or data types. Application outside of the CDR would require risk assessments to determine the level of accreditation required (and any customisations).

The ATO DSP accreditation regime is a key example of a regime that should be considered for incorporation into a common licensing regime. A common data safety licence would potentially reduce costs to business from duplicative requirements and enable the development of a larger ecosystem of supporting service providers – both for CDR and in this case the ATO DSP regime.[337] Other possible candidates include the secure access point regime under e-invoicing and the data safety elements of the digital identity provider regime under the Trusted Digital Identity Framework.

Alternatively, where a licence already exists with data safety elements, that licence could simply reference the data safety requirements of the appropriate tier of data safety accreditation. For example, the AFSL could reference data safety standards developed by the DSB, rather than ASIC maintaining and having to keep up to date separate requirements. Development of an appropriate set of generic mostly principle-based tiered requirements would be essential to enable the benefits of such an approach to be fully realised.

Use of the accreditation outside of CDR would require the licence to distinguish between CDR requirements and general data safety requirements; or for CDR specific obligations to be stripped out of the licence and form part of general CDR obligations contained in the rules or standards. It would also require data safety accreditation requirements to be fully contained in the standards (rather than CDR specific rules), so they could be referenced in other regulatory contexts. As

[336] Utilising this aspect only is dealt with in the proceeding section.
[337] Acknowledging that as a far less mature system, CDR would benefit far more from enabling access by ATO DSP data recipients than the other way around.

government seeks to streamline the sharing of its data with accredited persons,[338] there may be interest in government data sharing systems applying a type of data safety licence.

The CDR provides systems for developing and maintaining requirements for data safety, with enforcement mechanisms. If a type of common data safety licence proceeds, rather than the current CDR reliance on sectoral external dispute resolution (EDR) schemes, consideration might be given to establishing a specialised EDR scheme.

As per the government's Cyber Security Strategy 2020, cyber security accreditation and the potential to map any proposed framework to other licensing and accreditation regimes is being considered.[339] There is merit in maintaining a consistent set of cyber security requirements for organisations that transcends industry-specific requirements for data security, where practical.[340] Close engagement in development of security requirements and governance should be pursued with Home Affairs and the Australian Cyber Security Centre in relation to broader cyber security policy and initiatives.

The Consumer Data Right Register and Accreditation Application Platform (RAAP)

The Register of Accredited Persons provides a list of 'data safety licensees' and a means to verify them, with the ACCC acting as registrar. The register's capabilities include the ability to hold and revoke digital certificates, and the ability to support encrypted communications between participants.

The RAAP has two main functions, to create a trusted data environment where encrypted data is only shared between the intended accredited participants, and to provide a portal where businesses can apply for accreditation. If other government regimes are seeking to provide accreditation for parties needing to access data securely, the RAAP infrastructure provides a secure environment for the granting and maintenance of accreditations.

Use of the underlying CDR information technology (IT) infrastructure would be of benefit where the costs of developing new infrastructure exceeds the marginal cost of building upon what has been established for the CDR.

Recommendation 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.

[338] Office of the National Data Commissioner, *Accreditation Discussion Paper,* September 2020.
[339] Department of Home Affairs, *Cyber Security Strategy 2020*, item 70.
[340] Deloitte submission, p. 36.

Recognition of accreditations

Just as it would create efficiency gains for CDR accreditation to be applied outside the CDR, it would benefit the CDR if accreditation or licensing regimes outside the CDR could be recognised as comparable with CDR accreditation, at the unrestricted or any proposed lower tier. Acknowledging these would enable participants to efficiently enter through the CDR accreditation process and join the CDR ecosystem quicker. In some cases, systems calibrating their own on-boarding criteria may choose to align some of their elements with those set for the CDR to enable compatibility and mutual recognition.[341]

This proposal is an alternative to the proposals above to merge existing disparate data safety licences into one regime. It is acknowledged that approach may not be possible for some types of licences – for example, foreign licences.[342] This proposal is also put forward as a possible transitional step to full subsuming of different data security accreditations under a common regime.

The transfer of high risk data is already securely managed by government agencies. The ATO operates the DSP Operational Framework to manage risks associated with data transfers which has controls in common with the CDR, such as data encryption and default onshore data hosting. Consistency with CDR controls, including any updates, may be recognised so that digital service providers compliant with the DSP framework, or relevant equivalents, are free to offer services in the CDR. Furthermore, the DSP framework uses a risk differentiated model in determining the requirements needed for utilising their APIs, including the volume of records, use of intermediaries and data hosting arrangements. Differentiated models may become compatible with a tiered accreditation system developed by the CDR.

The potential for recognition of international data sharing accreditations is discussed in the Linkages and interoperability with international data portability regimes section.

Currently, ADIs can apply for streamlined CDR accreditation at the unrestricted level. Where other data safety regimes are deemed adequate to cover CDR requirements, but are not yet able to be merged into the CDR data safety framework, participants in these regimes should be able to apply for streamlined accreditation at the appropriate tier. For example, energy retailers can be trusted with energy data and so should receive streamlined accreditation to a lower accreditation tier that is required for CDR access to that data.

Candidates for streamlined accreditation might include those compliant with certain levels of the ATO DSP requirements, as the ACCC has proposed, and those adopting the Security Standard for Add-on Marketplaces developed by the Australian Business Software Industry Association.[343] Recognition and merger of data safety frameworks would be preferable in the long term to eliminate existing unjustified differences in data safety practices, to prevent future divergence, and to make updates more efficient across the data economy.

[341] New Payments Platform Australia submission, p. 4.
[342] Although, consideration might be given to sharing a common data safety licence with New Zealand.
[343] Xero submission, p. 4.

Recommendation 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'.

Recommendation 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.

Linkages with the AI Ethics Framework

The CDR presents significant opportunities for consumers and entities providing data-driven services. The additional data shared, with the consent of the customer, under the CDR provides opportunities for entities to use artificial intelligence (AI) technologies for both product innovation and insights into a business's consumer base.[344] Data and AI complement each other, with AI improving the more data it is given. AI technologies have the ability to rapidly read and analyse large aggregated data sets using algorithms. Advanced algorithms have the capacity to learn, adapt and apply that learning to their own internal decision-making.

Ethical responsibilities for use of data generally (including but not limited to CDR data) include consideration of how data is interpreted through algorithms and an understanding that unintended consequences or potential biases may materialise. For example, the use of particular personal information (gender, ethnic background, family status) may have unintended consequences when used by an algorithm to inform pricing decisions and may result in discrimination.[345]

Aggregation of Consumer Data Right data by accredited persons

An accredited person may use CDR data and CDR derived data to provide the service requested by the consumer. If an accredited person wants to use CDR data to conduct data aggregation activities to profile or build insights about a consumer to deliver a requested product or service, this is possible with the consumer's consent.

Such data may also be used by accredited persons for purposes that support the service they are offering; for example, it may be used to verify or analyse the consumer's financial situation in banking. In the banking example, depending on a consumer's spending habits, CDR data may reveal sensitive information (a health condition, or gambling habits) which may also be analysed or combined with other data to gain further insights, where this is relevant to the consumer's financial situation.

[344] Deloitte, *Open Banking, what does it mean for analytics and AI?*, September 2018, p. 3.
[345] Deloitte, *Open Banking, what does it mean for analytics and AI?*, September 2018 p. 5.

De-identified data and combination with other data sets

Once CDR data collected as part of a valid consumer request is no longer required it must be destroyed or de-identified. The Rules explicitly state that CDR data may not be used for the purposes of creating a profile for compiling insights on any other person identifiable by that CDR, and CDR data may not be on-sold to other entities.[346]

However, de-identified CDR data[347] may be sold and when combined with other data sets may be able to be re-identified. As the CDR expands to other sectors the amount of data accessed and transferred via CDR increases. As this occurs firms will have the capacity to process and combine data sets, which may include de-identified CDR and data from other sources. They may be able to link data sets to reveal an individual's lifestyle, consumer habits, social networks and more – even if no single data set reveals this personal information.[348] This could present significant privacy risks.

AI and consumer safeguards

From a consumer perspective, the absence of common industry standards about how data aggregation activities are explained and represented makes it difficult for consumers to understand how data about them is used. Further, accredited persons can use CDR data if it is authorised or required under another law, which means a consumer's CDR data may be used in a way outside their expectations.

The challenges associated with providing transparency for data aggregation activities are not unique to the CDR. However, given the high volume of granular data that will be transferred, the CDR will make it easier for an accredited person to accurately profile, to make decisions and build rich insights about a consumer in ways that may not be expected.

In its submission to the Inquiry the Financial Rights Legal Centre observed that there is currently no mechanism beyond explicit informed consent requirements to ensure consumers understand exactly how their data will be used by AI technologies, how decisions are made or how value will be extracted from their data.[349]

Government initiatives regarding AI and data ethics

Similarly to the CDR, for consumers to realise the benefits of AI they need to be able to trust that it is safe, secure and reliable. The ethical and reputational consequences of how data is utilised need to be kept front of mind by entities developing AI capabilities. Some of the most commonly discussed challenges for AI technologies include ensuring that:

- AI is fair (free from bias)
- there is an appropriate level of transparency in how decisions or predictions are made

[346] Rule 4.12.
[347] Privacy Safeguard 12.
[348] Deloitte submission, p. 23.
[349] Financial Rights Legal Centre submission, p. 25.

- individual privacy is protected, and
- a human is accountable for the outcomes of AI.[350]

In November 2019 the Government launched the AI Ethics Framework[351] to guide businesses and governments looking to design, develop and implement AI in Australia. This includes a set of eight voluntary ethics principles to prompt organisations to consider the broader impacts of using AI enabled systems.[352] The AI Ethics Framework is complemented by the AI Technology Roadmap[353] which is intended to help guide future investment in AI and start a national dialogue on the ways AI could drive new economic and societal outcomes for Australia. It also identifies key areas of AI specialisation that represent opportunities for Australia. In addition, Standards Australia released the *Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard* in March 2020 (the Standards Roadmap).[354] The Standards Roadmap includes a series of recommendations to shape 'responsible AI' through the development of standards and grow Australia's capacity to develop and share best practice in the design, deployment and evaluation of AI systems.

The Department of Industry, Science, Energy and Resources is currently developing guidance for organisations to apply the ethics principles to their work.

Recommendation 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.

Linkages and interoperability with international data portability regimes

International data portability regimes

Around the world, customer controlled standardised data portability regimes are being developed using different implementation approaches. Each regime is unique, with differences in scope,

[350] ACMA, *Artificial intelligence in media and communications – occasional paper*, July 2020, p. 13.
[351] https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework
[352] The eight ethics principles in the AI Ethics Framework are: human, social and environmental wellbeing, human-centred values, fairness, privacy protection and security, reliability and safety, transparency and explainability, contestability, accountability.
[353] Hajkowicz SA, Karimi S, Wark T, Chen C, Evans M, Rens N, Dawson D, Charlton A, Brennan T, Moffatt C, Srikumar S, Tong KJ, *Artificial intelligence: Solving problems, growing the economy and improving our quality of life*, CSIRO Data61, 2019.
[354] Standards Australia, *Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard*, March 2020.

functionality and standard setting. At one end of the spectrum, government-led regimes such as Australia and the United Kingdom require industry participation by data holders and accreditation of data recipients by regulatory bodies. At the other end of the spectrum a market-led approach, as developed in the United States that allows a regime to develop without any government initiatives or guidance. Somewhere in between, countries including Singapore, Hong Kong and Japan provide guidance and encouragement to promote participation.

The **United Kingdom** was the first to start Open Banking at a systemic level in January 2018. It commenced with the nine largest banks and offered account information and payment initiation services. By June 2020 it had over 260 regulated providers.[355] Services have emerged including account aggregation services, expenditure monitoring, tools for business to track expenses and manage tax obligations, and tools for consumers to find better deals. Following the success of Open Banking, the government is extending the use of data-driven technology under the 'Smart Data' initiative, beginning with the energy and pension markets.[356] A publication setting out the next steps for accelerating smart data initiatives was released in September 2020.[357]

In the **European Union**, Payment Services Directive 2 (PSD2) is the framework which provides for payment initiation and data portability in relation to payment services. PSD2 requires European banks to give authorised third-party payment initiation and account information service providers access to customers' accounts. In September 2020, the European Commission published its Digital Finance Strategy, which sets out key priorities relating to data use in digital finance, including the promotion of open finance through a common financial data space and a principle of same activity, same risks, same rules.[358]

Also relevant for data sharing is the General Data Protection Regulation (GDPR) which requires consumers to be made aware, in a way that is clear, concise and transparent, how their personal data will be used and by whom. Consumers need to provide explicit consent or another legitimate basis for their transaction data to be used. GDPR also imposes legal duties to protect consumer data and ensure its accuracy and completeness. GDPR provides consumers with a general right to data portability.

India has taken a government-led approach to implementing a data sharing system, known as Data Empowerment and Protection Architecture (DEPA). As well as establishing the legal framework and supporting infrastructure, Government data was the first to be shared in the system. Regulated data, including telecommunication data, financial data and health data is in the second phase, which has recently started rolling out. In terms of Open Banking, India's system has a somewhat unique order,

[355] Open Banking Implementation Entity, *Open Banking Highlights - June 2020,* 18 August 2020, https://www.openbanking.org.uk/about-us/latest-news/open-banking-highlights-june-2020/
[356] HM Government, *Smart Data, Putting consumers in control of their data and enabling innovation,* 2020, HM Government.
[357] Department for Business, Energy and Industrial Strategy, *Next steps for Smart Data, Putting consumers and SMEs in control of their data and enabling innovation,* 2020, Department for Business, Energy and Industrial Strategy.
[358] European Commission, *Digital Finance Package*, 24 September 2020, https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

developing from a comprehensive digital identification framework, to payment initiation though the Unified Payments Interface before read access data sharing has been rolled out. In August 2020 DEPA released a discussion paper inviting recommendations to refine DEPA as it evolves.[359]

Singapore, led by the Monetary Authority of Singapore, has taken a facilitated approach to open banking by providing guidelines, including an 'API playbook' with more than 400 recommended APIs. There is no regulatory framework or obligation for banks to join the system. Singapore is currently consulting on provisions for data portability and data innovation which go beyond the banking sector.[360]

Hong Kong has also taken a facilitated approach. The Hong Kong Monetary Authority published its Open API Framework for the Hong Kong Banking Sector in July 2018.[361] The intent of the high level framework is to allow banks some flexibility in how they implement Open Banking. The framework applies in phases, commencing with product information, then customer acquisition, then account information and payment information services. Phases one and two have been implemented, with technical standards for phases three and four due in 2020. [362]

Japan has taken a facilitated approach to Open Banking by implementing a more inclusive regulatory framework for electronic payment service providers. Banks are obliged to publish their own Open API policies and are encouraged to contract with at least one third party provider by 2020. Banks and third party providers need to negotiate contracts for data sharing and payment initiation, including the charging of any fees.

In January 2020, the **Canadian** Government released an advisory committee report which recommended enabling 'consumer-directed finance', through a framework involving both industry and government. The report recommended that the role for Government would include connecting consumer-directed finance to discussion about the broader application of data sharing across all sectors and to government efforts on enabling a data-driven economy. [363]

New Zealand is exploring the appropriate model for their country. The New Zealand Government released a discussion document on whether to develop a consumer data right in August 2020. It canvasses four options: (i) the status quo that continues a market-driven approach, (ii) a sectoral-designation approach similar to Australia, (iii) an economy-wide consumer data right and (iv) a

[359] NITI Aayog, *Data Empowerment and Protection Architecture, Draft for Discussion*, 2020 India, NITI Aayog.
[360] Personal Data Protection Commission Singapore, *Public Consultation on Review of the Personal Data Protection Act 2012 - Proposed Data Portability and Data Innovation Provisions,* 2019, Singapore: Personal Data Protection Commission Singapore.
[361] Hong Kong Monetary Authority, *Open Application Programming Interface (API) for the Banking Sector*, 2019, Hong Kong: Hong Kong Monetary Authority.
[362] Hong Kong Monetary Authority, *Open API Framework for the Hong Kong Banking Sector,* 2018, Hong Kong: Hong Kong Monetary Authority.
[363] Government of Canada, *Consumer directed finance: the future of financial services*, 2020, Government of Canada.

sector-specific approach. The sectoral-designation approach is assessed as most likely to meet the required criteria. The discussion document also states:

> *There may be some benefits in aligning any CDR in New Zealand with similar requirements in overseas jurisdictions. For example, the Australian and New Zealand Productivity Commissions identified a number of areas where a trans-Tasman approach to open banking and data portability could benefit both countries. This included making it easier for firms to obtain finance for trans-Tasman trade activities, broadening the market for emerging fintech firms and encouraging increased competition in trans-Tasman financial services.*[364]

While each data portability regime is unique, there is scope for interoperability as discussed below.

Australia's CDR regime is one of the leading data portability regimes in the world. It was one of the first regimes to be implemented in the banking sector and has been used as a model for other regimes. Australia was one of the first to consider customer-controlled data portability beyond banking, and its economy wide framework has inspired other countries to extend their regimes. Maintaining this world leading position is critical to deliver a world class digital economy for Australians and provide opportunities for Australian fintechs and other data driven start-ups.

Interoperability with other regimes

International interoperability means that technology and systems built for one regime can be used with minimal changes in another regime or that similar systems can be connected relatively easily by 'technology bridges'.

In its submission the Office of the Australian Information Commissioner says: 'Interoperability does not mean uniformity – but rather recognises the differences in regulatory frameworks and provides a bridge to ensure that information is protected, regardless of where it flows.'[365]

A CDR that is internationally interoperable offers benefits for Australian consumers and businesses. For Australian consumers, it could create a competitive market for their custom and more choice. It may accelerate adoption of the CDR by allowing agile ADRs and intermediaries to join. For Australian businesses, it is an opportunity to access overseas markets.

Elements of a system that foster international interoperability may include leveraging common standards, streamlined paths to accreditation and similar overarching design principles[366]. These could be facilitated by cooperation and improved information sharing, including through international forums.

[364] Ministry of Business, Innovation and Employment, *Discussion Document, Options for establishing a consumer data right in New Zealand,* 2020, Wellington: Ministry of Business, Innovation and Employment.
[365] OAIC submission, p. 8.
[366] Equivalent principles are discussed in Box 8.2.

Box 8.2 – Equivalent principles

Even where standards and accreditation requirements differ, interoperability may still be possible where data portability systems are built on similar principles and use a common technical language.

Principles generally emerge over time, usually through international forums or agreements as the regimes they support grow and develop.

As an example, the Principles for Financial Market Infrastructures emerged in its current form as part of the international response to the global financial crisis. The Principles outlines comprehensive minimum standards for Financial Market Infrastructures and establishes a set of responsibilities for Central Banks, Market Regulators and other Relevant Authorities.

So far, principles which have emerged as important in consumer controlled data portability regimes internationally include:

- **Consumer focus** – designed to benefit the consumer
- **Improving competition** – improves competition by making it easier for consumers to compare and move between providers
- **Data protection and security** – that consumers' data is secure and protected.
- **Clear allocation of liability** – where there is a breach or a consumer incurs a loss, it is clear who is responsible for compensating the consumer.

Equivalent principles should be supported by a common technical language. A common technical language will assist in providing certainty and in streamlining agreements as it enables entities from different jurisdictions to have confidence that core terms of agreements are understood. Data Republic's submission suggested the development of common foundational definitions for cross-border data-sharing as harmonised definitions and taxonomies would create space for the concepts in domestic laws.[367]

Common rules and technical standards

Rules and standards are required to ensure efficient implementation and compliance, interoperability between parties and across sectors, and to promote competition.

In its submission, American Express stated:

> *Where it makes sense to employ common international standards, Australia should do so. Within the finance industry, the global shift towards ISO20022 for messaging is an example of beneficial international convergence around a common standard.*
>
> *Where it's not possible to standardise specific data points and definitions, then the use of open protocols with built in flexibility to be able to evolve as technology develops, will provide the best opportunity to capitalise on emerging solutions for interoperability.*[368]

[367] Data Republic submission, p. 12.
[368] American Express submission, p. 3.

The Open Banking Review included as one of its recommendations: 'The starting point for the Standards for the data transfer mechanism should be the UK Open Banking technical specification. The specification should not be adopted without appropriate consideration, but the onus should be on those who wish to make changes.'[369]

The Inquiry considers that the use of open international standards remains important for the future directions of the CDR.[370] The DSB currently uses open standards wherever possible. The DSB has Outcome Principles which articulate qualitative outcomes the API definitions should seek to deliver. Their second outcome principle is 'In order to promote widespread adoption, open standards that are robust and widely used in the industry will be used wherever possible.'[371]

The Commonwealth Bank of Australia submission stated that:

> *where feasible, we support greater consistency with existing international standards and industry standards. Where solutions become increasingly bespoke, this creates issues with future extensibility, security and interoperability with other regimes.*[372]

There is a balance required when setting standards. Many international and open standards provide a common framework for interoperability but are often set at a very high level which does not provide the detail that may be required for them to be operationalised consistently. More detailed standards are subject to periodic revision which can be disruptive to businesses if their systems are not interoperating based on the same version of standards. So while they can be (and have been) relied on to an extent, additional technical details and specifications or adjustment for domestic circumstances will always be required.

Further, where Australia is the first to enable data sharing in a particular industry, open standards may not be available. In this circumstance, there is an opportunity for Australian standards to inform standard development in other jurisdictions.

Recommendation 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.

Recommendation 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.

[369] Open Banking Review, Recommendation 5.2, p. 83.
[370] The Inquiry notes that the Budget 2020-21 included $6 million over 3 years to strengthen Australia's role in international standard-setting and supporting business to apply these standards.
[371] Consumer Data Standards v1.5.1, under 'Principles'.
[372] Commonwealth Bank of Australia submission, p. 13.

Streamlined accreditation

Some submissions to the Inquiry suggested that accreditation provided by other jurisdictions could be recognised as meeting Australian requirements.

For example, Xero stated:

> *International alignment could streamline CDR ecosystem participants' access to open data regimes in new markets. This would work to both import competition, leading potentially to better domestic consumer outcomes, and enable Australia to export new technology solutions with a far lower regulatory burden. Recognising the accreditation of existing open data participants or establishing a global accreditation framework is key to fostering interoperability and exporting a new wave of Australian data companies.*[373]

Allowing foreign accredited parties streamlined access into the Australian Open Banking system was considered in the Open Banking Review, with the report suggesting that the regulator consider what would be needed to passport accredited entities from other jurisdictions once both regimes are established.[374]

While to date efforts have been focused on establishing the accreditation system, the launch of Open Banking is an appropriate time to consider options for recognising accreditation from an international jurisdiction.

Options for streamlining accreditation could vary from full recognition where an international accreditation is considered appropriate to satisfy the Australian requirements, or partial recognition where international accreditation is considered appropriate to satisfy some elements of Australian requirements to enable a quicker, streamlined process. The extent of additional requirements could vary depending on the tier of accreditation being sought.

Recognising international accreditation would lower costs for business holding that accreditation, which would lower barriers to entry, improving competition and providing more options for consumers. However it is not without risk. By relying on an assessment performed in another jurisdiction, there is a risk that the assessment is not performed to the standard expected. There is also a risk if the entity subsequently loses its accreditation in another jurisdiction (or is subject to some other adverse finding) and Australian regulators may not find out for some time.

Other design options to consider are whether such a regime is unilateral, mutual bilateral or multilateral:

- **Unilateral:** where Australia recognises accreditation provided by another jurisdiction. This type of regime is generally the easiest to implement and could be expected to improve choice and competition, but would not facilitate opportunities for Australian accredited entities to export their products. It could be introduced as a transitional stage to one of the other options.

[373] Xero submission, p. 2.
[374] Open Banking Review, p. 27.

- **Mutual bilateral:** Australia and another jurisdiction negotiate and agree to mutually recognise each other's accreditation. This type of regime requires negotiation so would take longer to establish. It could be expected to increase competition and choice for consumers and provide export opportunities for products accredited in Australia.
- **Passport regime:** two or more countries agree to recognise each other's accreditation. This type of regime, which is the most complex to negotiate and execute, could be expected to improve competition and provide export opportunities. It is something that could be explored as part of an international forum.

Recommendation 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.

As discussed above the United Kingdom was the first to develop open banking at a systemic level. Its open banking system is in operation with regulated providers serving customers. Its design had a significant impact on the way the CDR was designed and implemented resulting in many similarities. There are also broader similarities between the Australian and United Kingdom's economies and rule of law. These factors support the United Kingdom as the first candidate for a mutual bilateral recognition program.

Recommendation 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.

New Zealand is currently exploring the appropriate model for a customer-controlled standardised data portability regime, and has noted there are benefits from using similar requirements to other regimes. Their discussion document includes the example of a trans-Tasman approach.

If New Zealand chooses an approach similar to Australia's, a trans-Tasman passport arrangement would benefit Australian consumers and businesses. It would increase the choice available to Australian consumers and increase opportunities for Australian businesses.

Recommendation 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.

International forums

An international forum may help progress cooperation and interoperability. Ai Group submitted:

> *It is vital that Australian industry and consumers have support and access to all international forums involved in standards development to ensure our national interests are preserved. This will allow for effective contribution to standards development at an ideal stage in which products and services are still under development.*[375]

While there are international forums focused on financial services and banking, to date there does not appear to be an international forum focused on economy wide consumer controlled data portability regimes.

An international forum may provide a platform to:

- **Share learnings:** As this a developing area, a forum to share learnings will help countries avoid mistakes and improve functionality in rolling out data sharing systems.
- **Encourage interoperability:** Engaging in discussions could contribute to systems that can work together more coherently. As Australia is leading in implementing an economy-wide data sharing system, the forum could be an opportunity to share learnings with other countries and encourage development of similar, interoperable systems.
- **Develop a common language:** As noted above, a common technical language will promote interoperability across different systems as open data terminology emerges.
- **Develop common standards:** A forum could lead to the development of common or more consistent technical standards.
- **Improve security of data:** Countries want to ensure their citizens and business data is protected. Discussion, a coherent system and common language is likely to improve the security of the international system.
- **Support trade:** An international system will improve competition by improving choice for consumers. This will make services cheaper and easier to use. It could also make it cheaper and easier for businesses to expand internationally.

The target institution from a country would be responsible for the policy and overall design of the system. In some countries where a regulatory-led approach is being pursued this is likely to be a government endorsed body or implementation entity (for example, Australian Treasury, UK Open Banking Implementation Entity). In countries where a market-led approach is being pursued this might also include an industry association.

[375] Ai Group submission, p. 12.

Establishing such a forum within or alongside an existing international body (for example, the Organisation for Economic Co-operation and Development) should be considered as it would provide infrastructure and experience to support the forum's ongoing success.

As such a forum will take time to set up, to ensure relationships are maintained in the interim a quarterly dialogue could be established. To begin it might include:

- The United Kingdom, due to the similarities in regimes and recommendation to seek a mutual recognition regime.
- New Zealand as it seeks to establish a regime, considering the benefits to both countries of a trans-Tasman approach.
- India, in line with the commitment to enhance technology collaboration expressed in the 2020 Comprehensive Strategic Partnership.
- Singapore, in line with the commitment to closer cooperation in the 2020 Australia-Singapore Digital Economy Agreement.

Recommendation 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.

Chapter 9: Consumer Data Right Roadmap

This chapter sets out a roadmap for the implementation of recommendations of the Inquiry, along with issues for further consideration as the CDR progresses. Submissions offered a range of views on options for progressing the CDR. Against the backdrop of a challenging economic environment, some favoured a carefully phased expansion, while others saw great opportunities for the economy coming from a more rapid expansion of the CDR's capabilities.[376]

Implementation of the Inquiry's recommendations

The Inquiry's Terms of Reference related to the future direction for expanded functionality and framework of the CDR rather than the identification of future sectors for roll out. The CDR roadmap will therefore focus on the method of prioritisation and sequencing of the implementation of the Inquiry's recommendations.

In making this assessment, the Inquiry considered:

- the interests of consumers
- providing certainty to stakeholders for investment decisions
- the complexity of implementation
- promoting data-driven innovation
- promoting participation in the CDR
- the likely regulatory impact and compliance cost, and
- how recommendations complement and interact with each other.

Product reference data

While the Inquiry is not focusing on which sectors should be prioritised for CDR designation, it is possible that for some sectors the designation of product data could be prioritised over consumer data in the same sector. In some sectors, existing industry codes or regulatory requirements mandate the provision of standardised product information that could be readily made transferable using the CDR framework. For example, the Telecommunications Consumer Protections Code and the Telecommunications (NBN Consumer Information) Industry Standard 2018 require that customers be provided with billing and product data,[377] which could form the starting point for the data sets to become standardised CDR product data.

Where requirements already exist for the provision of product data in a sector, an opportunity exists for rapid introduction of this data to the CDR, and use by consumers. Excluding consumer data from scope removes the need for a Privacy Impact Assessment, and could allow participants in some

[376] FRLC submission, p. 3, Business Council of Australia submission, p. 3, Data Republic submission, p. 4.
[377] Communications Alliance submission, p. 3.

sectors to transition to the CDR in a gradual process by only requiring APIs for CDR product data in the first instance, with consumer data to follow.

Recommendation 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.

Prioritisation and sequencing of implementation

Consumer benefit should be the primary driver of what aspects of the CDR are prioritised.

Implementation timetables should recognise that where particular aspects of implementation are more complex, long periods of time may be required for their development, build and testing. Prioritisation of implementation should also look to realising 'quick wins' for consumers.

Streamlined product switching is one example of a function that will drive considerable benefits for customers using the CDR, however, not all of the Inquiry's recommendations to support this can happen immediately because a number of elements of the expanded CDR regime need to be implemented first to enable it.

Prioritisation should also be based on the understanding that indirect enablers of participation and competition, such as inclusion of intermediaries and tiered accreditation, also drive positive outcomes for consumers and help establish the system.

Some recommendations refer to the potential for leveraging the CDR infrastructure and linking the framework with external aspects of the data economy. The implementation of these recommendations will partly rely on cooperation with external agencies and initiatives. For example, any leveraging of digital identity will be dependent upon the emergence of widely adopted solutions that provide a convincing value proposition to their users. Where implementation relies on external factors, an integrated approach to prioritisation could increase chances of successful execution.

Open Banking has only recently gone live, and energy sector data is in the process of being introduced to the CDR. Limited CDR-related skills and knowledge in both the government and private sectors could create a bottleneck in the early stages of implementation.

A clear list of priorities will help to set expectations for those investing in the CDR ecosystem.

Phasing of implementation

Initial Phase

Many recommendations from the Inquiry require no changes to legislation. Given the lead time required for updates to legislation, it would benefit the CDR to commence implementation of these elements as soon as possible to enhance data sharing functionality and lay the foundation for future additions to the CDR. The ACCC is already consulting on some Rule changes, such as ADR to ADR

transfers and lower tiers of accreditation.[378] Once these consultations conclude, new elements such as voluntary data sets and permitting the receipt of some CDR data by unaccredited data holders could be introduced, which will help facilitate functions such as switching.

Workstreams leading up to payment and action initiation can also be prioritised in the initial phase, where they are not dependent on changes to legislation and are critical to future implementation. As recommended, Treasury and the DSB should engage with operators of major payments systems to commence consultation and design work on standards for payment initiation. Early engagement on such technical aspects will provide a good platform for finalisation of the standards and implementation of payment initiation once the necessary changes to legislation and rules are made, and allow for alignment with major payment systems, such as the NPP.

A third party payment initiation roadmap should provide guidance for stakeholders on when such engagement will occur. Recommended clarifications to the ePayments Code, ongoing and explicit customer consent processes and work on authentication standards for action initiation can also be developed before the framework is in place.

As sectors are identified for inclusion in the CDR framework, attention can be turned to any sector-specific regulatory barriers that will be faced when action initiation applies to a particular sector. Analysis of how to make better data about bundled products available and comparable for consumers can also be undertaken by the DSB ahead of action initiation designation and implementation.

Where opportunities for international leadership in the data economy arise, they should be prioritised to maximise the benefits to CDR participants. For example, the Australia-United Kingdom Free Trade Agreement currently under negotiation could present the CDR with an opportunity for international integration, this may be more difficult after the agreement is settled. If the CDR is able to integrate with offshore regimes, initiatives can take effect on a much wider scale and access to the CDR market could open up broader opportunities for some participants and consumers. Early engagement or alignment will also reduce the likelihood that the CDR will have to adjust to offshore developments later on.

Action Initiation Phase 1 – Payment initiation

Legislative amendments will be required for the CDR to support general action initiation and payment initiation. An updated banking sector designation will then be required to specifically set out the classes of general action initiation and payment initiation that should be supported.

Once these frameworks are established, payment initiation should be prioritised to allow the maximum value to be extracted from the foundation already provided by Open Banking, and to encourage early coordination with industry in the initial phase.

[378] ACCC, CDR rules expansion amendments Consultation Paper, September 2020, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-cdr-rules

Action Initiation Phase 2 – Broader action initiation

To further benefit consumers, enablers of switching should also be prioritised as the broader action initiation functions are implemented. The ability to instruct an ADR to open and close an account or establish a customer relationship; and to acquire products are key components required to enable switching of providers.

Elements such as the altering of communications preferences and the maintenance of personal details could be implemented later if limited resources compel further prioritisation.

Review Phase

As required for Open Banking, and recommended for payment initiation and action initiation, a post implementation review should be conducted to assess the impact of these capabilities, once fully functioning. These reviews should be comprehensive, including analysis of how the CDR is performing against its stated objectives, including its impact on privacy and vulnerable consumers.

Recommendation 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.

Integrated Consumer Data Right Roadmap

The CDR will link with numerous other industry and government frameworks, and become more complex, with the introduction of new elements such as action initiation. As noted by KPMG:

> *if the legislative framework for the regulation of data continues in a piecemeal, sector specific and fragmented way, Australia will miss an opportunity to create a legal and regulatory data framework that works for business, government, the public sector, consumers and for the entire economy.*[379]

Given that infrastructure, market and consumer needs are continually evolving, Cuscal has submitted that it is crucial the CDR regulator develop a technology and governance roadmap, alongside a longer-term industry engagement and participation model. This could help establish where CDR infrastructure can be leveraged for other purposes.[380]

Areas of collaboration

Collaboration and consultation with the following stakeholders as the CDR is rolled out will enable clearer communication of the proposed obligations and opportunities available to CDR participants:

- Government

[379] KPMG submission, p. 5.
[380] Cuscal submission, p. 5.

- CDR regulators
- non-CDR regulators – but related to the data economy
- private sector industry bodies
- consumer and privacy groups
- participants in sectors to be designated, including their technology departments, and
- international counterparts.

The development of the CDR should be consistent with broader Government policy objectives, and strengthen coordination and direction-setting across the network of agencies. The Inquiry understands that to support these objectives, some work relating to the roll-out of the CDR will be moved into Treasury, including rule making functions and the ability to undertake sectoral assessments, and hosting of the DSB from the CSIRO.

Related initiatives

As noted in the introduction, various reviews, inquiries, updates to legislation and implementation roadmaps cross over with the work required to implement the Inquiry's recommendations. Observing or working alongside related initiatives will enable a smoother implementation of the CDR for both participants and regulators, while maximising opportunities for integration with other initiatives in the digital economy.

Adding to concerns about the roll out of the CDR at present is the pipeline of other regulatory interventions that business is having to plan for. For instance, the government has committed to reviewing the *Privacy Act 1998* which may in turn require a policy response in relation to privacy safeguards to which CDR participants must adhere.[381]

CDR information security standards will need to adjust to any cybersecurity policies and practices emerging out of either industry or government. To ensure this occurs, developers of CDR standards should continue to participate in collaborative cybersecurity workstreams, such as the Australian Government's Cyber Security Strategy 2020, and related initiatives from the Federal Budget.

Findings from these, and other workstreams must be integrated into the CDR's policy framework as seamlessly as possible. Further examples of related initiatives for consideration include:

- proposed amendments to the AML/CTF Act regarding reliance on KYC assessments
- developments in the Digital Identity System[382]
- rule changes proposed by the ACCC,[383] and the Energy Rules Framework Consultation[384]

[381] Business Council of Australia submission, p. 3.
[382] Digital Transformation Agency, Digital Identity System, October 2020, https://www.dta.gov.au/our-projects/digital-identity/digital-identity-system
[383] ACCC, Consultation on proposed changes to the CDR Rules, October 2020, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/consultation-on-proposed-changes-to-the-cdr-rules
[384] ACCC, Energy rules framework consultation, July 2020 https://www.accc.gov.au/focus-areas/consumer-data-right-cdr/cdr-in-the-energy-sector/energy-rules-framework-consultation

- possible Government responses to the final recommendations of the Senate Select Committee on Financial Technology and Regulatory Technology[385]
- New Payments Platform Roadmap[386]
- an upcoming RBA review of the New Payments Platform functionality and access[387]
- ACCC Home Loan Price Inquiry[388]
- Digital Technology Taskforce[389]
- RBA Review of Retail Payments Regulation,[390] and
- The Artificial Intelligence Ethics Framework.[391]

Recommendation 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.

Issues for future consideration

Post-implementation assessment

Each new experience in the CDR journey will offer new lessons and opportunities for reflection on what elements worked well, or did not go to plan. A post-implementation review for each major stage of the CDR roll out will provide a clear process for stakeholders to provide feedback on their experiences. Reporting on the outcome at each stage will allow the Government to respond to stakeholder feedback and to build knowledge with the aim of reducing negative unintended consequences as further elements of the CDR are implemented.

As noted in the Open Banking Review, the scheduling of the post-implementation assessment should provide sufficient time to properly observe the practices and behaviours that arise as a result of the

[385] Parliament of Australia, Senate Select Committee on Financial Technology and Regulatory Technology, September 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology

[386] New Payments Platform, NPP Roadmap, April 2020, https://nppa.com.au/wp-content/uploads/2020/04/NPP-Roadmap-April-2020_final.pdf

[387] RBA, *New Payments Platform Functionality and Access: Conclusions Paper*, June 2019, https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/functionality-and-access-report.html

[388] ACCC, 2020, *Home Loan Price Inquiry interim report*, https://www.accc.gov.au/focus-areas/inquiries-ongoing/home-loan-price-inquiry

[389] Department of the Prime Minster and Cabinet, Digital Technology Taskforce, October 2020, https://www.pmc.gov.au/domestic-policy/digital-technology-taskforce

[390] RBA, Review of Retail Payments Regulation, October 2020 https://www.rba.gov.au/payments-and-infrastructure/review-of-retail-payments-regulation/

[391] Department of Industry, Science, Energy and Resources, AI ethics framework, October 2020, https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework

reforms. It is expected that there will be a period of fine-tuning following the launch of any reforms, and sufficient time must be given for this to occur. Indeed, the ability of the system to identify problems and adjust accordingly is a key factor that the post-implementation review must assess. As firms and consumers may take different period of time to join and use the system, a reasonable amount of time should pass before conclusions are drawn.

The Inquiry has concluded that after commencement, a 24 month period would provide sufficient time for the evaluation of the effectiveness of action and payment initiation. It is also proposed that the review engage with those involved in their respective subject areas and interested parties, such as consumer advocacy groups.

Recommendation 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.

Glossary

Accredited data recipient (ADR):	A person who has satisfied the accreditation criteria set by the ACCC and has, as a result, received CDR data under the Consumer Data Right.
Accredited person:	A person who has satisfied the accreditation criteria set by the ACCC and can, as a result, enter into data sharing or action initiation arrangements under the Consumer Data Right.
Action initiation:	A third party with write access to a data holder sending instructions to the data holder. Instructions may include initiating payments from a customer's account, and actions, such as switching, opening or closing an account, or updating details.
AFS licence:	A licence authorising the carrying on of a business of providing financial services.
Application programming interface (API):	Software designed to help other software interact with an underlying system.
Australian Competition and Consumer Commission (ACCC):	An independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians.
Australian Privacy Principle (APP):	Outline how most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information.
Authorisation:	In the Consumer Data Right context, communication to a data holder regarding what data sets the consumer has authorised them to share, and what actions they are authorising be initiated on their behalf.
Bank:	An authorised deposit-taking institution (ADI) as defined in the *Banking Act 1959.*
Consumer Data Right (CDR) agencies:	These agencies include the ACCC, OAIC, DSB and the Treasury.

Consumer Data Right (CDR) data:	Information within a class specified in a CDR designation instrument, or information wholly or partly derived from such information.
Consumer Data Right (CDR) regulator:	One of the bodies responsible for CDR Rules, accreditation, registers, compliance and education.
Consumer Data Standards:	Specific standards for participants on how to connect, transfer and satisfy the Rules written by the Data Standards Body. The Standards could include detailed information on engineering, technology, data and security.
Comparator website:	Sites that generally compare products across a product category offered by a range of suppliers, according to specific characteristics provided by the consumer. Also referred to as comparison services or comparison websites.
Consent:	Communication to an accredited person of the data sets and actions that the consumer is allowing them to access or perform, and the purposes for which the consumer agrees to their data being used and actions being initiated on their behalf.
Consumer Data Right (CDR):	The right of Australian consumers to have access to their data, and the regime that implements this right.
Data:	Information translated into a form for efficient storage, transport or processing. Increasingly synonymous with digital information.
Data economy:	Economic activities conducted or facilitated through use of data.
Data ecosystem:	The community of participants, their environment, and all their interrelationships within the data economy.
Data holder:	A party that holds data to which the Consumer Data Right will apply, carrying obligations to provide that data to CDR participants.
Data sharing:	The transfer of product and consumer data, usually referring to sharing under the CDR framework with consent.
Data Standards Body (DSB):	A body responsible for assisting the Data Standards Chair in the development of common technical standards to allow Australians to access data held about them by businesses and direct its safe transfer to others.

Data Standards Chair (DSC):	The person responsible for creating data standards for the CDR, supported by the DSB.
Designation:	A legislative instrument creating consumer rights via the CDR to access and transfer a class of data from a specific sector, or to instruct a class of action.
Digital economy:	Economic activities conducted or facilitated through digital computing technologies.
Digital identity:	Information that represents a person or organisation on a computer system. A digital identity allows a user to prove to a remote system that they are who they say they are.
DSP Operational Framework:	Framework that outlines what is required of digital service providers (DSPs) that access and use the ATO's digital wholesale services.
e-invoice:	A machine-readable invoice issued, received and processed electronically. It is digital from its creation in the issuer's financial system until it is received and processed by the recipient.
ePayments Code:	A code that regulates consumer electronic payments in Australia, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking, and BPAY.
Interoperability:	The ability of software systems to exchange information efficiently.
Mandated Payments Service (MPS):	NPP-based service to support payers preauthorising payments within certain parameters be made from their account to another specified account.
Mutual recognition:	Where two jurisdictions agree to recognise each other's laws or regulations.
New Payments Platform (NPP):	Payments infrastructure that enables real-time, data-rich payments between bank accounts connected to the NPP.
Office of the Australian Information Commissioner (OAIC):	The independent national regulator for privacy and freedom of information.
Open Banking:	The CDR based system giving customers access to and control over their banking data and data on banks' products and services.
Open Banking Review:	Review into Open Banking in Australia published by the Treasury in December 2017 to recommend the best approach to

	implementing Open Banking through the creation of the Consumer Data Right.
Outsourced Service Provider (OSP):	A person who, under a CDR outsourcing arrangement, receives CDR data from, or potentially discloses CDR data to, an accredited person.
One-time-password (OTP):	A method of authentication involving a consumer being sent a password through a separate channel (this could be by any other means such as email, phone app, or text) to enter into the service provider's customer interface.
Personal information:	Any information or an opinion about an identified individual, or an individual who is reasonably identifiable, as per the *Privacy Act 1988*.
***Privacy Act 1998*:**	Legislation designed to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information.
Privacy impact assessment:	A systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
Productivity Commission Inquiry into Data Availability and Use (PC Data Inquiry):	Inquiry into the benefits and costs of options for increasing availability of and improving the use of public and private sector data by individuals and organisations, reporting in March 2017.
Read access:	Access to view data, but not to change data or initiate actions.
Register and Accreditation Application Platform (RAAP):	The IT backbone of the Consumer Data Right, providing a trusted data environment where encrypted data is only shared between approved participants; also refers to a portal where businesses can apply to be accredited.
Regulatory technology (regtech):	The use of technology to better achieve regulatory objectives, intended to support the improved targeting of regulation and reduce the costs of administration and compliance.
Rules:	Rules for the CDR.
Screen scraping:	The practice of third parties using a customer's login credentials provided by the customer to extract data (such as account balance

	and transactions) from the information that the customer may see on their digital display.
Specialised service provider:	Party that provides a specialist service to data holders, ADRs or intermediaries. This could include, among other things, collection, storage, aggregation, filtering or analysis of data.
Transaction data:	Data that is generated as a result of transactions made on a customer's account or service.
Trusted Digital Identity Framework (TDIF):	The Australian Government's framework for accrediting providers of identity assurance for government services online.
TrustID Framework:	A framework designed to support an interoperable network of digital identity solutions administered by the Australian Payments Network.
Value-added customer data:	Data that has been enhanced by a data holder, for example to gain insights about a customer.
Voluntary data:	CDR data that is authorised, but not required, for a data holder to provide.
Write access:	The ability for the third party to give the data holder instructions to take actions. This can enable them to cause the data holder to create or change information that they hold, in a sense 'writing' new information.

Key Acronyms

ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ADI	Authorised deposit-taking institution
ADR	Accredited data recipient
AEMC	Australian Energy Market Commission
AFS	Australian financial services
AI	Artificial intelligence
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
API	Application programming interface
APP	Australian Privacy Principle
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
BECS	Bulk Electronic Clearing System
CCA	*Competition and Consumer Act 2010*
CDR	Consumer Data Right
CPRC	Consumer Policy Research Centre
CX	Consumer Experience
DEPA	Data Empowerment and Protection Architecture (India)
DSB	Data Standards Body
DSC	Data Standards Chair
DSP	Digital Service Provider
EDR	External Dispute Resolution
EIC	Explicit informed consent

FRLC	Financial Rights Legal Centre
FSRC	Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry
GDPR	General Data Protection Regulation (EU)
IDR	Internal Dispute Resolution
KYC	Know Your Customer
MPS	Mandated Payments Service
NEM	National Energy Market
NERL	National Energy Retail Law
NPP	New Payments Platform
OAIC	Office of the Australian Information Commissioner
OBR	Open Banking Review
PC	Productivity Commission
PRD	Product Reference Data
PSD2	Payment Services Directive 2 (EU)
RAAP	Register and Accreditation Application Platform
RBA	Reserve Bank of Australia
REPI	Retail Electricity Price Inquiry
TDIF	Trusted Digital Identity Framework

Appendix A: Terms of Reference

Inquiry into Future Directions for the Consumer Data Right Terms of Reference

1. The Inquiry will make recommendations to the Treasurer on options to:

    1.1. Expand the functionality of the Consumer Data Right.

    1.2 Ensure the Consumer Data Right promotes innovation in a manner that is inclusive of the needs of vulnerable consumers.

    1.3 Leverage Consumer Data Right infrastructure (such as the Data Standards Body and accreditation regime) to support the development of broader productivity enhancing standards and a safe and efficient digital economy.

    1.4 Leverage the developments of the Consumer Data Right with other countries that are developing similar regimes to enhance opportunities for Australian consumers, businesses and the Australian economy.

2. The recommendations will include examination of:

    2.1 How the Consumer Data Right could be expanded to include 'write' access to enable customers to apply for and manage products (including, for Open Banking, by initiating payments) through application programming interfaces.

    2.2 Linkages and interoperability with existing and potential frameworks and infrastructures, including the New Payments Platform.

    2.3 How the Consumer Data Right can be utilised to overcome behavioural and regulatory barriers to convenient and efficient switching between products and providers.

    2.4 Similar regimes being developed in other countries and how Australia should be engaging with these countries to leverage the Consumer Data Right.

3. The Inquiry will have regard to:

    3.1 The Reserve Bank of Australia's *New Payments Platform: Conclusions Paper*.

    3.2 The ACCC's home loan price inquiry, in particular its proposed examination of obstacles to home loan switching.

    3.3 The Government's response to the ACCC's *Digital Platforms Inquiry*.

    3.4 Best practice developments internationally and in other industry sectors.

    3.5 Competition, fairness, innovation, efficiency, regulatory compliance costs and consumer protection.

Appendix B: Public submissions

The Inquiry received 73 written submissions, including 2 confidential submissions. The organisations and individuals that made public submissions are included in Table B.1. The public submissions are published on the Inquiry's website.[392]

Table B.1 – Public submissions

Organisations and individuals	
Australian Banking Association	Data Republic
Australian Energy Council	Deloitte
Australian Finance Industry Association	Energy Australia
Australian Financial Markets Association	Energy Queensland
AGL Energy Limited	experian
Australian Industry Group	Finder
Alinta Energy	FinTech Australia
American Express	Financial Planning Association of Australia
ANZ	Financial Rights Legal Centre
Australian Business Software Industry Association	Greater than X
Australian Energy Market Commission	illion
Australian Institute of Superannuation Trustees	innopay
Australian Payments Network	Insurance Council of Australia
Australian Privacy Foundation	KeyOne Consulting
Australian Retail Credit Association	KPMG
Business Council of Australia	Law Institute Victoria
Block8	Lixi
CHOICE	Mastercard
Customer Owned Banking Association	Meridian Energy
Commonwealth Bank of Australia	Mortgage and Finance Association
Communications Alliance Limited	MYOB
Consumer Policy Research Centre	National Australia Bank
Controlabill	New Payments Platform Australia Ltd
CPA Australia	Office of the Australian Information Commissioner
Cuscal Limited	OpenID Foundation

[392] https://treasury.gov.au/consultation/c2020-62639

Organisations and individuals	
Oracle Corporation	Syamantak Saha
Origin Energy	Telecommunications Industry Ombudsman
Prospa	Telstra
Public Interest Advocacy Centre	The Law Society of NSW, Young Lawyers
Red Energy	TrueLayer
Reserve Bank of Australia	Tyro
Salesforce	Victorian Automobile Chamber of Commerce
Simply Energy	Visa
Spriggy	Westpac
Super Consumers Australia	Xero
Swift	