

Part Two: Implementation and lessons learnt

The CDR has developed significantly since its establishment in 2019 and the initial rollout to the banking sector. As of 26 July 2022, 114 data holder brands are now live in the CDR system, with 76 designated data holders and an additional 38 brands. The number of ADRs has also been steadily growing, with 32 ADRs, 20 of which are active. This represents a market share of more than 99 per cent of Australian household deposits being covered by CDR data-sharing.

Part Two of the Report considers feedback on the development and functioning of the CDR to date and the lessons that should be gleaned to inform future rollout, including governance structure, speed of expansion, the level of system complexity and the accreditation process.

The CDR has expanded and developed since its launch, most notably with the designation of additional sectors (energy and telecommunications), and the ongoing assessment of Open Finance. Along with increasing the coverage of CDR data, there have been continuous developments in the rules and standards to support the expansion of the system, as well as improvements in the functioning of the framework in existing sectors. There have now been four version updates of the rules, while the standards have received rolling updates, with 10 maintenance cycles completed in addition to a number of narrower updates from Decision Proposals.

The CDR framework provides a foundation that has the potential to support economy-wide digital transformation and deliver significant consumer benefit. However, this Review's consultations have found that the system is not yet at a point where these benefits are being delivered. Part Two of this Report considers a number of concerns related to the implementation of the CDR to date and what lessons could be considered in relation to the statutory framework. These concerns include, but are not limited to, the quality of CDR data, the level of coordination between CDR agencies, the accreditation process, the lack of consumer awareness of the CDR, the uptake of CDR products, and some potentially adverse competition outcomes from the CDR rollout. Many stakeholders informed the Review that some of these concerns have directly prevented them from choosing to participate in the CDR – stakeholders whose participation would otherwise create additional consumer value and contribute to a vibrant CDR and digital ecosystem.

2.1 Data quality and screen scraping

Under CDR privacy safeguard 11, data holders and ADRs are required to take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up to date and complete.¹⁶ The data put into the system should be of a quality that maintains consumer trust and gives system participants confidence to invest in developing the innovative products and services that compel consumers to move away from alternatives, such as screen scraping. A number of Review participants spoke about issues of inconsistent data quality, with a number of ADRs suggesting that product development has been held back by data range and quality issues. The Financial Data and Technology Association (FDATA) noted that many of its “members regularly share concerns around poor quality data, delays in data being received (in some cases up to 24 hours by major ADIs), missing fields, erroneous data fields, garbled and inconsistent data”.

¹⁶ Chapter 11: Privacy Safeguard 11 – Quality of CDR Data, <https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-11-privacy-safeguard-11-quality-of-cdr-data>

Data quality issues won't resolve overnight. It will take a concerted effort by all participants in the CDR ecosystem to work collectively to resolve data quality issues as they arise. ADRs report feeling that the onus is on them to resolve issues related to the quality of data they have received from data holders, with little action taken by the data holders themselves. There is also the perception amongst ADRs that there is limited follow-up enforcement action by the ACCC. While the ACCC has powers to undertake enforcement actions, they have taken a facilitative approach to resolving data quality issues to date. The Review also understands that a regulatory agency cannot reveal publicly who they are investigating and intending to take enforcement action against, leading to some confusion around when action is being undertaken.

"It is clear from various stakeholder workshops that many banks are failing to meet the standards on data quality and it is often left to the data recipients to identify and flag these issues. To date, we are not aware of any enforcement action taken to date against data holders failing to meet the standards when it comes to data quality." – Finder

Finding 2.1

Data quality is limiting the wider adoption of the CDR. Addressing it as a priority, including through enforcement actions when necessary, will increase participant confidence in the CDR, leading to the development of new CDR products that benefit consumers and decrease reliance on risky practises like screen scraping.

While the CDR provides a safe alternative to screen scraping (also known as Digital Data Capture or DDC), submissions noted a number of reasons why businesses have continued to use screen scraping despite the possibility of receiving data through the CDR.

"When considering the ease and lower cost of implementation of DDC when compared to CDR processes, it is not surprising that the majority of financial services organisations continue to use DDC" – illion

"DSPANZ has heard specific feedback from our members on the quality of Open Banking data. Some members have reverted back to screen scraping methods (where they do not have access to direct bank feeds) due to the quality of the data" – Digital Service Providers Australia New Zealand (DSPANZ)

Many fintechs informed the Review that, until these issues are addressed, they will have little choice but to rely on screen scraping to support their use cases.

Once the data provided under CDR becomes comparable to that collected via screen scraping, most participants are willing to move fully to the CDR. Until that occurs, poor data quality will limit potential uses cases and continue to dissuade many from joining the CDR, even though they concede it is a superior data sharing system.

“illion’s conclusion is that CDR is technically a far superior solution to the Digital Data Capture mechanisms currently used in financial services” – illion

In its submission, Verifier recommended a sunset on screen scraping. The Government should consider this recommendation and provide an indication to industry of the intention to move away from screen scraping. Signalling the intention to prohibit screen scraping will provide participants with greater certainty and provide an incentive to direct resources into complying with CDR requirements rather than maintaining screen scraping capabilities. The Government could incentivise industry by clearly signalling when and how this prohibition will come into effect, providing them with certainty and adequate time to transition.

Consideration of prohibiting screen scraping should take account of the difficulty that small businesses experience in participating in the CDR, as well as the context of the Future Directions Inquiry, which previously proposed prohibiting it for payment initiation.¹⁷

Recommendation 2.1

Screen scraping should be banned in the near future in sectors where the CDR is a viable alternative. Importantly, the Government should clearly signal when and how the implementation of the ban would take effect. This would provide certainty and adequate time for businesses to transition, along with stronger incentives to invest in moving to the CDR.

2.2 Accreditation and compliance tools

Issues related to conformance testing, accreditation processes and compliance tools were raised throughout the Review. Stakeholder comments ranged from identifying potential conflicts of roles in these processes to unmet expectations about what these accreditation processes mean for data quality in the CDR system.

Some stakeholders implied there was a perceived conflict in the ACCC’s responsibility for CDR accreditation, operations and compliance enforcement; in other words, being responsible for onboarding new participants into the system makes it difficult to then undertake enforcement activities. Participants raised concerns that any engagement could later be used as evidence of non-compliance. In its submission, the ACCC also discussed separating these operational and enforcement roles.

While this is an understandable concern, there would be risks associated with possible conflicting interpretations of rules if accreditation and operations were separated from the body enforcing the rules and it is difficult to see where else the accreditation and operations responsibilities should go within in the existing governance of the CDR, if not the ACCC (see also section 2.3). While these functions are maintained by the ACCC, it will be important to address these concerns (real or perceived) to give industry confidence they can work in collaboration with the ACCC to address issues as they arise. To this end, it is encouraging to see the ACCC’s public willingness to take action when

¹⁷ Recommendation 5.17 of the final report of the *Inquiry into Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

data holders fail to meet their CDR obligations,¹⁸ as was recently observed in the issue of the infringement notice against the Bank of Queensland.¹⁹

Despite passing the Conformance Test Suite (CTS) (see Box 2.1), ADRs were also consistently concerned about the quality of data received through the system and noted that data holders routinely provided poor quality, non-conforming data. The Review notes that the CTS does not test the data quality of data holders. Before being ‘activated’ in the register by the ACCC to begin data sharing, both ADRs and data holders are required by the ACCC to complete testing of their systems and successfully complete testing against the CTS. Understandably however, data holders see compliance with the CTS as evidence of their provision of quality data. This often leaves ADRs feeling that they bear the burden of determining data defects, raising issues with the ACCC and ultimately working with data holders to correct data quality issues.

Box 2.1 – What is the Conformance Test Suite?

As part of the onboarding process, the ACCC operates a Conformance Test Suite, or CTS, whose purpose is to test if participants (data holders and ADRs) can conform with the Consumer Data Standards (CDS) in a secure environment without exposing consumer data or interacting with live products/data. Participants must pass the CTS before they receive an active status on the CDR Public Register.

The CTS is designed to test how a participant’s software interacts within the CDR ecosystem, give consumers confidence that participants can enter the CDR ecosystem without disruption, and demonstrate participants are capable of conforming with the CDS and the Register design. Participants must pass the CTS to become accredited as active by the ACCC.

Although there was generally positive feedback about the accreditation and onboarding process, there is still confusion among participants about the purpose of the CTS, despite the ACCC providing guidance on this. Participants appear to believe that, once an applicant has passed the CTS, the ACCC has effectively given them a ‘clean bill of health’ to participate in the CDR. The CTS, however, only tests whether participants conform with the standards and register design and meet their obligations, not whether the data provided is of adequate quality.

“Unfortunately the Conformance Testing that is performed to validate whether a Data Holder has met their obligations, does not test the quality of the financial data. As a result, nobody can confidently measure the quality of the data, nor guarantee that the data that is supplied via the Open Banking APIs is complete” – Basiq

18 Ms Gina Cass-Gottlieb speaking at the AFR Banking Summit 2022, <https://www.accc.gov.au/speech/acccs-priorities-and-approach-to-regulating-the-financial-services-sector>

19 Bank of Queensland pays penalty for alleged breach of Consumer Data Right Rule, <https://www.accc.gov.au/media-release/bank-of-queensland-pays-penalty-for-alleged-breach-of-consumer-data-right-rules>

Future consideration should be given to the service the ACCC offers in this space. Although it is understandable that participants would look to government in the formative stages of the CDR, the system would be better served by more comprehensive service offerings in the marketplace. It is noted several participants already offer testing solutions of some form, either in combination with their other offerings as turnkey solutions or as an individual product. This said, it's important to maintain that the Government remains the ultimate arbiter of regulatory compliance and that any market developed solutions assist participation but are not equivalent or a replacement for government regulation. Regardless of whether participants are offered government or market solutions to aid compliance and onboarding, the timing will be crucial to ensure they can be updated and available once the rules and standards are finalised to allow participants to quickly build, test and implement changes. This will rely on close coordination between CDR agencies, testing solutions providers and participants, as well as on visibility of forward timelines to appropriately plan (see section 2.3 for further information). The Government should regularly look to the market for solutions where it is better placed to provide them.

Recommendation 2.2

Creating a trusted ecosystem that supports the development of a range of products will encourage new market-driven innovation in the CDR. It is recommended that prospective Accredited Data Recipients (ADRs) have the flexibility to choose who they undertake preliminary systems testing with, including through an accredited private sector solution or the Australian Competition and Consumer Commission (ACCC).

Submissions from both the Commonwealth Bank of Australia and EY supported the announcement of a sandbox for ADRs to test their APIs and validate that these APIs function as expected in a realistic environment. In a submission from FDATA it was noted that the UK also experienced data quality issues, which were substantially improved after the development of a “dedicated testing function and sandbox for API validation and testing”. The implementation of this sandbox will be an important addition to existing resources for those seeking to become accredited under the CDR, and will offer participants further opportunity to resolve data quality issues beyond the CTS. There is also an opportunity here for the market to provide solutions for participants.

2.3 The role for an implementation body

The CDR has been operating since 2019 and has attracted feedback and suggestions on how implementation could or should have been approached differently. It is important in these discussions to maintain awareness of the system's context as a world-leading initiative, in terms of both depth and scope. Australia's CDR is an internationally unprecedented framework that supports broad multi-sector data sharing, with no set formula and few examples to learn from. The CDR has an ambitious vision and, to ensure its success, we must consider the lessons from its implementation to date.

Feedback from participants has indicated that implementing systems and engaging with the CDR and its administrators has been difficult and complex. While most were generally complimentary about their experience with individual regulators, many also spoke of the burden of dealing with multiple regulators, each with their own objectives, and a perception they were not well coordinated across government and lacking appropriate tools to support participants.

This Review's consultations revealed a common experience of participants being referred back and forth between regulators, without receiving clear solutions and resulting in a perceived lack of ownership. This highlights the complexity of the CDR's governance structure and the roles and responsibilities of the CDR agencies and the Minister, for further information see [Appendix C](#). The Review supports implementing a 'no wrong door' approach to interactions including for consumers (see section 3.7), which will require improving coordination and clarifying role and responsibilities between CDR agencies.

"While engaging on important CDR issues, the AEC has sometimes found it unclear what body or organisation was the responsible decision maker and there appeared to be administrative confusion between the respective bodies over who held responsibility for which roles. At times, this has had reduced the quality of consultation and made it difficult for data holders to receive the guidance they need on grey areas in the CDR ecosystem." – **Australian Energy Council submission**

Participants often cited the absence of a centralised implementation entity or market operator, such as the OBIE in the UK, to address these concerns. The OBIE was established to implement Open Banking in the UK as part of a multi-agency governance framework, with the key organisations being:

- the Competition & Markets Authority (CMA) which has responsibility for the obligations under the CMA Order and oversight the OBIE,
- the Financial Conduct Authority which authorises, regulates and supervises Open Banking and payment firms,
- the Payment Systems Regulator which is the economic regulator for payment systems, and
- HM Treasury which has responsibility for overarching financial policy.

This model offered participants (business operators using open banking as well as consumers using products and services supported by open banking) a clearer 'front door' for interaction with the UK Open Banking scheme and participation in it.

Box 2.2 – UK’s Open Banking Implementation Entity (OBIE)

The OBIE was established in 2016 in the Competition & Markets Authority (CMA) order, which also required the nine largest banks (covering 90 per cent of the market) to fund the entities’ implementation activities, including constructing the infrastructure and services underlying Open Banking, providing guidance and monitoring the rollout of Open Banking, and promoting the adoption of Open Banking. This body still receives government oversight through the CMA. As the implementation activities set out in the CMA order are close to completion, a Joint Regulatory Oversight Committee has recently been announced to oversee the development of Open Banking beyond the scope of the CMA Order and advise on how to transition from existing governance arrangements to a future, long term regulatory framework for Open Banking.

Many CDR participants questioned whether the current implementation and regulatory arrangements, with multiple implementation agencies coordinated via the CDR Board, which is an advisory body, remain fit-for-purpose as the CDR expands across multiple sectors of the economy. Envestnet | Yodlee’s submission raised that “[c]onflicting opinions or gaps in knowledge abound” between CDR agencies, and “areas where rules are made yet technical standards have been ignored or not thought through in their entirety”.

Inspired by the OBIE, many advocated the creation of a dedicated entity to implement, operate and maintain the CDR, act as repository of deep technical expertise in data and generate momentum to take the CDR across the economy as the solution to this lack of coordination. Participants envisaged that such an entity could maintain a single voice, advocate and educate around the system, as well as understand the complexity of IT builds. The entity would conceivably have a better understanding of the difficulty of constantly changing requirements and realistic timeframes informed by practical realities rather than externally imposed deadlines. The view is this would also assist participants, particularly smaller ones, who currently struggle to access and understand the information and lack the capital and technical expertise needed to participate in the CDR.

“The governance of the CDR should be simplified and consolidated under a single regulator with powers to set rules, technical standards, conduct accreditation, registration and enforcement. Treasury should retain policy responsibility for CDR and set the strategic direction.” – Australian Banking Association

The Review notes that the UK approach is also a multi-agency approach, the OBIE was time limited to the implementation of data-sharing by nine entities, and was made possible through industry funding in the UK by those nine major banks. The Review is conscious that participants and the government have already expended significant resources in building the CDR ecosystem and submissions did not offer solutions or proposals as to how such an entity would be resourced and funded in Australia. The UK approach was also designed to support a single-sector rollout with deep functionality, and is not readily transferable to supporting the policy objectives of the CDR as an economy-wide initiative. In the Australian context, the addition of another body may inadvertently lead to further fragmentation in the CDR ecosystem, particularly in any transition period, and would inevitably divert resources across the system at the expense of system expansion and deepening of functionality.

The current arrangements attempt to distribute policy, rule-making and regulatory responsibilities to the appropriate Government Ministers and agencies, balance technical and policy expertise with

industry involvement and ownership while continuing to provide appropriate compliance oversight. The Review does acknowledge CDR participant feedback that these arrangements have not always worked effectively.

In the future as the CDR and other digital initiatives mature, implementation and regulatory arrangements across initiatives should be revisited. However, in the short to medium term (up to five years), priority should be given to working with and improving the existing CDR governance structures, coordination and clarity between CDR agencies. Suggestions to this end include CDR agencies:

- Providing greater direction on future rollouts and timelines for key releases and consultation processes, ensuring a coordinated and consistent approach is taken to limit overlap, and maintaining a level of situational and environmental awareness to limit conflict with major dates and events inside and outside the CDR,
- Clarifying the roles and responsibilities of CDR agencies with clear ownership of issues to ensure participants are receiving consistent and clear messaging across all interactions, and implementing a 'no wrong door' approach,
- Publishing more comprehensive information, such as schedules and timelines on the progress of the scheme, and
- Having a coordinated and targeted communications and media approach, including websites, newsletters and general email communications.

Recommendation 2.3

Changes to CDR governance should not be made now, however, improvements to coordination within the existing CDR structures should be undertaken as a priority in the short to medium term. CDR agencies should make it easier for participants and users to resolve issues and seek advice, including by clarifying responsibility and ownership of issues, coordinating consultation and system releases, and publishing comprehensive statistics on the progress of the CDR.

When looking beyond the short to medium term, CDR governance arrangements should be revisited alongside that of other digital initiatives to ensure policy aims across the digital economy are met. For CDR specifically, this includes ensuring that the system works horizontally across sectors with a high degree of interoperability with other initiatives (e.g. PayTo, digital identity) and integrates effectively with a wider global digital economy. The CDR governance structure would need to be well-positioned to support a growing ecosystem by:

- Leading the vision of the economy-wide rollout of the CDR
- Providing a single source of truth for advice, guidance and resolution of issues
- Having the authority to make unilateral decisions, and
- Providing agile, customer-focussed service delivery.

"Whilst jurisdictions such as the United Kingdom and Brazil have established an independent entity to oversee the deployment and ongoing operations of Open

Banking, Australia's fragmented and fractured approach has created further misalignment, delays, assumptions and, in some cases, a false responsibility to carry out the priorities of others to the detriment of the overall Right." – FDATA

Since its inception, the CDR governance structure has not remained static, with changes made in 2021 to move some accountability and responsibility from the ACCC to Treasury to provide a more streamlined and unified approach to development and implementation (see [Appendix C](#)). However, as the system continues to evolve and expand, the roles and responsibilities (including service delivery, regulatory functions, and technical standards) of the current structure should be revisited and lessons learnt to ensure the best structure is in place to support the CDR going forward. This Review found no clear consensus around a suggested governance model and, in the medium term, suggests further consideration be given to what model best supports the CDR as it expands and integrates with the wider digital economy.

2.4 Increasing awareness and engagement

Submissions raised issues with the implementation framework that might be addressed with adjustments to the governance structure for the CDR. Most stakeholders noted that there is very little consumer awareness of the CDR. One submission by Finder cited their *Consumer Sentiment Tracker* survey, which suggests that, in May 2022, only 5 per cent of their sample could correctly identify what the CDR is, down from 8 per cent in March 2021.²⁰ Some submissions suggested that this lack of awareness results in little consumer demand for new use cases of the CDR, reducing incentives to produce new use cases.

"The CBA encourages the Government and the Regulators to support education for consumers on the use and benefits of the CDR regime to increase engagement and drive consumer benefits." – Commonwealth Bank of Australia

"An increase in consumer participation and awareness can only be achieved through planned educational and marketing programmes" – Cuscal

Increasing consumer awareness of the CDR has been discussed in previous review processes, including submissions to the recent sectoral assessment of Open Finance, as well as in recommendations from the *Open Banking Review*²¹ and the Future Directions Inquiry.²² This Review has found that the assertion that education would drive consumer uptake of the CDR overstates its role in consumer decision-making related to CDR-powered products. While understanding of the CDR may drive uptake for consumers who closely follow technological developments, for the majority of consumers, uptake will be determined by the new products and services on offer that can remove frictions from their lives or benefit them in other ways. This does not disregard the need for consumer education and

²⁰ Refer to <https://www.finder.com.au/cst>

²¹ Recommendation 6.4 of the final report of the *Review into Open Banking*, May 2018, <https://treasury.gov.au/consultation/c2018-t247313>

²² Recommendation 7.8 of the final report of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

awareness; consumers should understand the risks of data sharing practises, whether that be CDR or screen scraping.

“Community acceptance and use of the CDR regime will be boosted by timely consumer education focused on the benefits of data sharing and how to mitigate its risks and costs.” – Scientia Professor Ross P Buckley & Dr. Natalia Jevglevskaja, University of New South Wales

Any consumer education efforts concerning the CDR, regardless of the message, will also need to consider the target audience and adapt accordingly. Targeting small businesses will be especially difficult given the diversity of the cohort. Small business owners listen to different voices within their respective networks which makes cutting through difficult. Conventional government campaigns have historically had difficulty achieving broad coverage amongst these smaller business operators.

Consumer education and technical understanding are unlikely to be the core drivers of consumer adoption, and the focus should be on building the CDR brand as a trusted form of data sharing, a trust mark of sorts, and to provide the warning signs of unsafe practices. To borrow Scott Farrell’s analogy from the Future Directions Inquiry, if the CDR is the new highway for driving consumers to data quickly and securely, then consumers are primarily interested in getting to their destinations safely and quickly, rather than in the highway itself.

Further consideration will also need to be given to the education, guidance, promotion and incentivisation of system adoption for existing and potential participants. The CDR highway isn’t yet fully built, with some of it built in only one direction (that is, data sharing only in banking) or only partially constructed (energy and telecommunications). The Government needs to ensure there is enough awareness and understanding among those who will build the highway by demonstrating the utility of the system, drawing them into the ecosystem and committing to the long term vision of the CDR.

The Future Directions Inquiry addressed the concept of incentivisation for participation by recommending the establishment of a grants program to support developers to build products to benefit consumers.²³ Grants alongside other incentives were raised in submissions to both the Future Directions Inquiry and this Review. The Review suggests that more effective incentives than grants could be provided by other mechanisms such as challenge-based funding and sponsoring prizes. For example, the OBIE-backed ‘Open Up 2020 Challenge’ (see Box 2.3) is an example of the role incentivisation can play in promoting and encouraging innovation and the development of practical use cases. Indeed, Australia has not been absent in this space, with the Department of Industry, Science and Resources’ Business Research and Innovation Initiative, which offered similar incentives to solving various policy challenges.

²³ Recommendation 7.9 of the final report of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

Box 2.3 – The Open Up 2020 Challenge

The Open Up 2020 Challenge was the second open banking challenge offered in a partnership between Nesta Challenges and the UK's OBIE part of the UK's world-leading open banking agenda.²⁴ This challenge, which offered a £1.5 million challenge prize to unlock the power of open banking for UK consumers, was designed and timed to boost consumer awareness and adoption of open banking-enabled products. It sought products and apps that use open banking to help people better manage their money via more transparent, accessible and fair products.

Finalists were provided grants of £50,000 to further develop their solutions, with a bonus £50,000 awarded to those demonstrating the clearest alignment with the financial inclusion goals of the challenge. Winners of the challenge received a further £150,000 to finalise the development of their solution. These solutions included a personal finance tool aiding in mortgage applications (Mojo), an investing platform that included personalised savings suggestions (Plum), a savings tool that supports savings contributions in the course of ordinary spending activities (Moneybox) and a service for employers that allows employees to easily manage their earned wages (Wagestream).

In the case of the CDR, a challenge sponsored by Government could be run in parallel to CDR processes (e.g. during sectoral assessment) to generate and demonstrate use cases before designation. Challenges could also be run in partnership with consumer advocacy groups to solve a particular consumer problem where there are limited commercial financial incentives, for example, addressing financial concerns for vulnerable consumers.

“EML also believes education is critical to the adoption & application of CDR. EML would be in favor of the government providing incentives or grants to encourage adoption by fintechs and to help stimulate the creation of innovative use cases” – EML Payments

While education campaigns and guidance are part of the solution, to truly build awareness and drive development of working innovative use cases, it is time for Government to explore initiatives that incentivise industry participation.

Recommendation 2.4

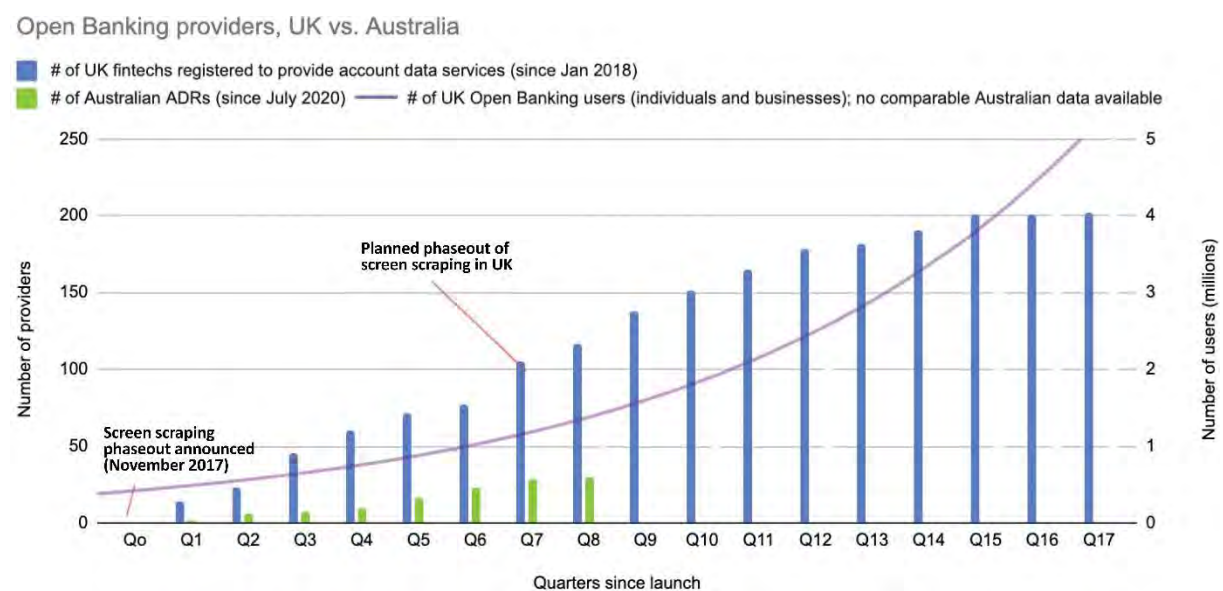
To encourage and incentivise the development of innovative use cases, the Government should look to support initiatives like the UK's Open Up 2020 Challenge, which could target a use case that drives social benefit that is not being developed by the market. Collaboration with consumer advocacy groups should be considered to help identify relevant consumer challenges that could be addressed by the CDR.

²⁴ Open Up 2020, <https://challenges.org/prizes/open-up-2020/#:~:text=What%20was%20the%20Open%20Up,of%20open%20banking%20enabled%20products.>

2.5 Balancing expansion with system maturity

The CDR's rollout of data portability to date has provided wide coverage and the focus should now turn to deepening the framework. While other data portability frameworks were able to achieve some capabilities faster, none has achieved Australia's breadth of coverage across sectors. For example, the Open Banking scheme in the UK commenced a phased delivery in early 2018, which enabled payment initiation in mid-2020. At the time of publishing, it has been two years since the first implementation of the CDR in the banking sector and the scheme does not currently include action and payment initiation. While the inclusion of payment initiation in Australia's data portability scheme in the banking sector will be later than in the UK, Australia has already implemented beyond banking and made significant headway in expanding to energy and telecommunications, while the UK is grappling with legislation required to expand its scheme beyond payments within banking and to other sectors. See Figure 2.1 for a graphical representation of differences in participation between the UK and Australia.²⁵

Figure 2.1 - Growth in open banking



The Review heard some concerns about the speed of rollout of the CDR. Stakeholders recognised the importance of balancing expansion with the iterative process of developing a secure and useful regulatory framework. While some stakeholders noted their appetite for receiving some CDR-enabled products faster (such as those enabled through action initiation), others noted moving ahead quickly with the scheme could leave some data holders already finding it difficult to meet compliance requirements and consultation deadlines behind.

“...the continuing compliance pipeline of overlapping commencement dates has reduced the capacity of many of our members to even consider becoming an accredited data recipient.” – Customer Owned Banking Association

²⁵ Figure 2.1 source Truelayer submission to the Statutory Review of the Consumer Data Right

“Future assessment and designation should consider where the greatest benefit will be realised. The current published focus is delivering a new sector/dataset per year whereas deepening the functionality should be prioritised.” – EY

Finding a balance is a difficult task – the system cannot move at the pace of the slowest participant, nor can it continue at a pace participants struggle to maintain. Consideration should be given to finding a tempo that focuses on implementing what has been proposed to date, bedding down the core CDR framework/rules/standards and allowing time for the system to mature before progressing into further expansion. This does not mean stagnation or resting on our laurels. To become truly economy-wide, the CDR should always look to the horizon for the next opportunity and be ready to move with consideration of the overall ecosystem and greater digital economy, allowing for expansion to new sectors or datasets with new rule changes made only as required.

Submissions to the Review illustrated a tension between the vision for a digital economy enhanced by a wide rollout of the CDR, and deepening and improving of functionality of the CDR in already designated sectors. Consultation revealed that the ambitions for an economy-wide CDR are widespread and will result in greater value in the long run.

“We believe that sectors should take time to implement the current framework, take time to gather learnings from an operational sector, ensure data sharing models are operationally efficient and then gauge the extent to which additional services or functionally is required under the scheme.” – Origin

This sentiment was also captured in the Strategic Assessment of the CDR, where stakeholders reported that including multiple sectors increased the value of datasets through sectoral synergies.²⁶ Several stakeholders consulted through the Statutory Review of the CDR indicated that, without fully completing one sector first, the rollout would not benefit from lessons learnt and could repeat the same mistakes in relation to new sectors. There were also views among some stakeholders that continuing to expand the CDR to new sectors could demand resources from the implementation agencies at the expense of higher priority policy changes like deepening functionality, for example, through action initiation. Balancing the breadth of datasets included under the CDR with the depth of functionality will continue to be a challenge for the CDR.

Recommendation 2.5

The current pace of CDR rollout into new sectors has not allowed enough time for the system to mature and capitalise on the lessons learnt. Focussing on improving CDR functionality and data quality within already designated sectors should be prioritised, balanced with overall forward momentum into new sectors over time.

²⁶ Treasury, *Strategic Assessment Outcomes Report*, January 2022, <https://treasury.gov.au/publication/p2022-242997>

2.6 Cyber security

The Review generally did not hear many concerns from stakeholders about the cyber security settings of the CDR. Where they were raised, security settings and requirements were generally discussed in the context of the sum of compliance matters that accompanies the CDR, rather than any observations as to the adequacy of the settings themselves. The Review acknowledges the role of the DSB and the Data Standards Chair to form data standards for CDR data security and the regular maintenance cycles performed in updating those standards. Although the CDR has these embedded processes and standards, it is understood that a whole of ecosystem review has not been undertaken on cyber security matters. As the CDR matures and expands across the economy to include new sectors, data holders and entities, the likelihood of compatibility and cyber security issues arising increases.

With the introduction of participants from the energy and telecommunications sectors, the Review considers that it is timely to revisit cyber security settings across the CDR ecosystem. While not a priority apparently raised by CDR participants, and with no known cyber breaches having occurred, the Review considers that the cyber security settings of the CDR are a fundamental element to ensuring the ability to, as well as viability of, delivering CDR-powered products and services. Conducting a review at this earlier stage of implementation would ensure not only that the settings remain appropriate to the operating environment, but also that they are resilient and can accommodate new challenges brought on by connecting increasing numbers of historically distinct data holders and data systems.

Recommendation 2.6

At this point in the CDR's development, the Government should consider undertaking a whole of ecosystem cyber security assessment to ensure that the CDR cyber security architecture continues to be fit for purpose into the future.

2.7 Consent journey and consumer experience

It is also clear that the CDR is not yet fully optimised to meet consumers' needs and experience. Data standards and consent requirements have a direct impact on the consumer experience. In its submission, Basiq noted up to 11 screens could be presented to a consumer in the steps to link a bank account to an ADR service (including pre-consent, consent, authentication and authorisation), and flagged that this doesn't include additional screens that may also be required for the bank account login process (user registration, email verification, Know Your Customer (KYC) checks etc.) to link to the service, to fully comply with regulatory requirements. Friction and high cognitive load can cause consumers to disengage before they obtain any value – only the most committed persist. At this stage in implementation, most participants focus on compliance and building trust and confidence in the system.

Further attention and consideration should be given to ensuring the experience is intuitive for consumers by designing the consent journey from a consumer perspective, for example, by allowing bundled consents, which involves a single bundled request that contains several requests to collect, use and disclose a consumer's personal information, which could increase convenience for consumers. However, this convenience potentially comes at a cost of apparent transparency and consumer comprehension, as bundled consents inherently do not provide a consumer opportunity to choose

which ones they consent to and which they do not. This is only one potential option and may only be applicable in some circumstances. In any scenario, changes to the rules would be needed (see Part 4) and care must be taken to ensure any changes do not undermine the consumer's informed consent.

Concern around consumer requirements has also been heard from consumer advocates – a submission from the Financial Rights Legal Centre (endorsed by the Consumer Action Law Centre and supported by the Public Interest Advocacy Centre) suggests there is a risk that the CDR's complexity could undermine a genuine consent process, with a resultant risk that “CDR consent in this context essentially falls back to the much maligned tick and flick settings that the CDR was meant to resolve”.

Unless further consideration is given to improving the consumer experience, consumers will become fatigued in their interactions within the CDR ecosystem and drop out before obtaining value. This, in turn, will reduce the adoption of CDR-powered products and increase the disincentive for participants to invest in innovative products and services.

“If consumers have poor experiences in open banking, there is a risk to future implementation across the economy. Consumer uptake will be essential to economy-wide expansion. A core concern of our members is the friction of consent being too great.” – FinTech Australia

“This flow appears designed to deliberately reduce the likelihood that a consumer will take advantage of data sharing. As a result, some TCA members have been reluctant to invest in developing services using CDR data” – Tech Council Australia

Furthermore, submissions to the Review noted the current disclosure and consent model of CDR is inadequate to fully inform consumers of potential privacy risk, given the comprehensiveness of the consent requirements.

“Therein lies the risk for consumers – that the complexity will lead to them to choose not to engage with the consent system enough to truly know and understand what they are consenting to.” – Financial Rights Legal Centre

Extensive consent requirements can perversely inhibit a consumer's understanding of what they are consenting to, and complicated consent processes can also deter consumers from engaging with CDR products and services.

Finding 2.2

The consent process is central to CDR's realisation of informed consumer decision making and delivery of consumer benefits. Complex consent processes may limit participation in the CDR and contribute to 'consent fatigue', which may undermine genuine consumer consent. As the CDR evolves, the consent process should be monitored and adjusted to ensure benefits are realised, and as the CDR expands to include actions and payments, further consideration should be given to other consent models, such as bundling of consents.

As the CDR continues to build momentum expanding in both functionality and sectors, it is expected that many consumers will access the CDR via multiple applications provided by their service providers, such as a bank or energy provider, a third party fintech, or a combination of both. It is easy to see how the average consumer may lose track and become overwhelmed if managing multiple consents across multiple applications and across various sectors that also differ in format. This has also been raised in the Future Directions Inquiry, along with the joint submission by the Chartered Accountants Australia and New Zealand, CPA Australia and the Institute of Public Accounts and a submission from FDATA ANZ, and so consideration could be given to improving the long term experience of consumers in the CDR ecosystem by providing a consolidated consumer dashboard to track and manage consents, with appropriate consideration given to potential risks and burdens on participants.

2.8 Complexity of rules and standards

Many participants also noted that, aside from the consultation processes, the rules and standards had also not been implemented in a way that was appropriate to their business needs. Stakeholders felt that there was an assumption, upon release of rules and standards, that there were technical experts waiting at their computers for the latest implementation updates. This experience was exacerbated by concurrent consultations and updates to both rules and standards which made the CDR rollout a very demanding process for stakeholders (see also section 1.5).

The complex and, according to one participant, “overly prescriptive” rules and standards may risk participants finding it difficult to meet the requirements set out for all products and services. The ABA noted in its submission “that regulation of the CDR should not be used to drive homogenous outcomes in products and should instead encourage and enable data holders to innovate”. A submission from EnergyAustralia noted the same was true of the energy sector. The Review heard from participants concerned that the overly prescriptive standards may cause some data holders to shift consumers from bespoke or niche products to standard offerings or, alternatively, may adjust their products to fit the standards resulting in more homogenised offerings across the market, less value for consumers and reduced competition in the marketplace.

Despite some of these complexities, it was exciting to hear participants speak with optimism about the prospect of becoming an ADR and the introduction of action initiation as the “game changer”, which also highlighted the point that benefits will be realised only at that point. To get to this point, the system will need appropriate time to breathe and mature. The CDR is on the right path to providing certainty to participants, which, in turn, gives them the time to transition from being solely focussed on compliance to innovation and new product development.

*“We acknowledge that the implementation of CDR to date has been driven largely by compliance, and recognise that as the CDR matures and stabilises, the development of more strategic customer value propositions will emerge” –
Commonwealth Bank of Australia*

Finding 2.3

The Review heard from participants that their experience in the CDR has been compliance focussed to date. Concerns were raised by participants about complex and overly prescriptive rules and standards that have prevented them from focusing on developing new products and services. As the system develops and matures, including through the introduction of action initiation, consideration should be given to ways that implementation can reduce the complexity associated with rules and standards for participants.

2.9 Pathways for CDR participation

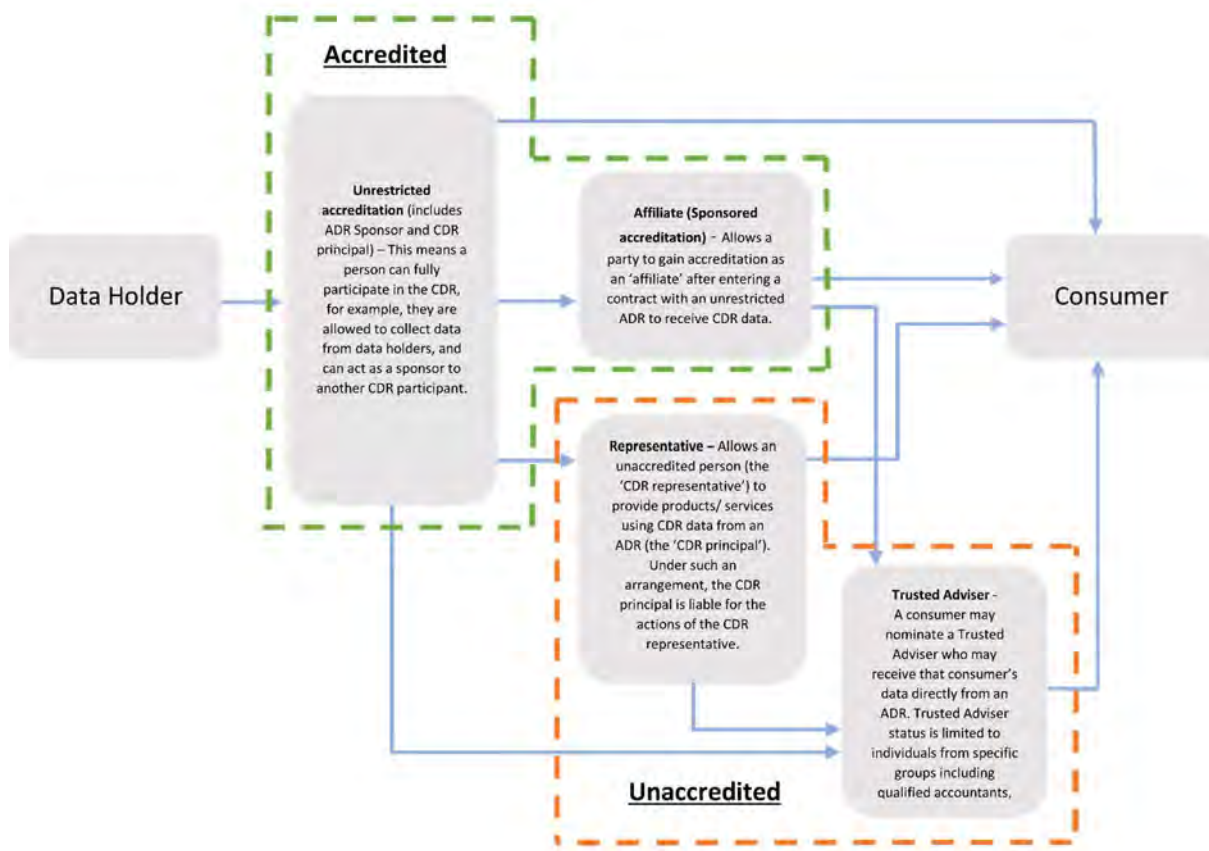
Submissions suggested that the compliance and liability settings for CDR accreditation and pathways for participation did not readily incentivise prospective business participants.

“Excessive compliance and accreditation burdens within the CDR ecosystem are having the perverse effect of encouraging more activity outside the CDR’s boundaries, ultimately undermining consumer protection and privacy” – TrueLayer

Introducing tiered accreditation was recommended in the Future Directions Inquiry as one way to reduce costs for prospective participants by offering alternatives to the demanding process of becoming an unrestricted ADR.²⁷ Additional access models were introduced to the CDR in version 3 of the Rules, which provided several new pathways to participating in the CDR other than becoming an ADR (with unrestricted accreditation), including the CDR representative model and sponsored accreditation, as well as establishing a role for trusted advisers (see Figure 2.2).

²⁷ Most notably Recommendations 6.12 and 6.13, but also 4.8, 5.7 and 6.4 of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

Figure 2.2 – Represents the data flow through the different access models



While these pathways to participation have created more options for prospective CDR participants, some have suggested that revision is needed for such pathways to be fit-for-purpose.

“Trying to gain accreditation or rely on another entity’s accreditation has become an enormous task due to the liability framework and the different accreditation models have not made a large difference” – Envestnet | Yodlee

The representative model, where a CDR Principal takes on the liability for a CDR representative, has the potential to expand the number of products and services powered by the CDR. This has been borne out in experience, where there are now almost as many CDR representatives as there are ADRs in the CDR ecosystem. However, this model also introduces risks to CDR Principals that may have adverse effects on the CDR ecosystem. A submission from illion suggested that large firms will be unwilling to “take on a large number of representatives due to the liability risk of non-compliance, as well as the reputational risk it places on their other business”, potentially encouraging higher risk thresholds and tolerances from Principals sponsoring representatives.

Introducing the representative model to the CDR ecosystem is a step forward, and while liability concerns may be justified, it is not clear whether there are alternatives that would do significantly better. The affiliate/sponsorship ADR model has a joint liability model where both a sponsoring ADR and the affiliate ADR are both liable for consumer data requests made by the sponsoring ADR. In comparison to the representative model, while few submissions noted the affiliate/sponsorship model, illion's submission noted that some non-bank lenders are actively choosing not to engage in this model (or unrestricted accreditation).²⁸ The submission noted many are avoiding this model as it would require them to meet reciprocal data holder obligations, so as an alternative are looking to engage through the representative model. However, to date no non-bank lenders have become CDR representatives. This suggests that other factors besides reciprocal data holder obligations are impeding non-banking lenders from participating in the CDR.

Noting the recent implementation of the representative (17 November 2021) and sponsored (1 February 2022) accreditation models, the Review suggests time be given to allow for current and potential participants to become accustomed to these avenues for participation before exploring alternatives. If a particular model has low uptake (e.g. sponsored accreditation), further exploration to understand why it is not being used would be warranted. Liability settings should be at front of mind when considering participation models so as not to inadvertently encourage risky behaviour.

Finding 2.4

The introduction of new access pathways, such as the representative and sponsor-affiliate model, has increased available avenues for participation in the CDR. Government should monitor participation and uptake to ensure settings remain appropriate. If a particular model or pathway has low uptake, further exploration should be done to understand why it is not being used and to affirm that liability settings are meeting desired policy outcomes.

A further concern was voiced in relation to the lack of recognition of the role of 'intermediaries' in the accreditation structure.

"Cuscal believes that to foster trust in the CDR ecosystem it is critical that CDR intermediaries are recognised, and separately accredited to enable new products and services under the regulatory umbrella of CDR." – Cuscal

"The designation of CDR intermediaries is a crucial aspect of growing the CDR ecosystem.... This new segment of CDR participants is not currently recognised under the CDR rules." – FDATA

In this context, the Review is treating an intermediary (including outsourced service providers (OSPs)) as someone who provides a service to another CDR participant that assists them in delivering a product or service to an end consumer. This could include, for instance, a business that specialises in

²⁸ "The majority of non-bank lenders are looking at representative models rather than sponsorship or unrestricted knowing that RDH obligations are likely to come into play." Submission from illion

the collection or storage of CDR data on behalf of other ADRs or a business that provides the data analytics software that allows an ADR to provide consumer services. These participants may not necessarily offer any consumer-facing CDR services of their own. The Review recognises the role intermediaries play in the CDR ecosystem, but the Review did not hear from submissions how the existing accreditation models fail to meet their needs and what potential changes might be required to facilitate their role in the CDR ecosystem. Without a clear picture of the underlying problem it is difficult to see what a bespoke intermediary accreditation process would look like in practice.

While expansion of accreditation may create new opportunities for involvement, it may also add to the complexity of the accreditation process and further add to existing concerns that further options have not made it easier to engage with the CDR to date, as noted by Basiq in its submission:

“Although these models have provided greater options, we feel that they have still not solved the underlying problems that were originally raised during the proposal phase. As it stands now, the accreditations are still considered to be expensive to implement, lengthy to acquire and complicated to interpret the rules associated with them.”

Introducing new pathways to accreditation should remain a possibility as the CDR develops. However, in the spirit of allowing the CDR to mature before introducing further optionality to the system, constructing a new intermediary accreditation may not be a priority, allowing time for further exploration of how intermediaries interact with the CDR to understand how their participation in the CDR can be facilitated.

Several submissions also noted that the requirements for CDR accreditation could be more closely aligned with existing requirements under other government initiatives. For example, there are existing security and privacy requirements for Digital Service Providers (DSPs) under the Operational Security Framework (OSF) for the Australian Taxation Office (ATO), however, the CDR framework demands more of data recipients.²⁹ Indeed, many participants inside and outside the system may see it as an unreasonable expectation of businesses to undergo multiple accreditation processes for schemes focused on data protection.³⁰

“Xero is confident recognising this Security Framework [including the Privacy Act, the ATO OSF and the Security Standard for Add-on Marketplace (SSAM)] would materially increase ADR participation, connecting business consumers with the innovation and competition measures intended for the CDR.” – Xero

During consultations, it was suggested that, if ATO requirements are not sufficiently strong, they should be brought in line with CDR accreditation requirements – otherwise the Government should

29 A 2021 review of the Security Standard Add-on Marketplace (SSAM) by Digital Service Providers ANZ (DSPANZ) provides insight into the degree to which this framework can align with the CDR. See https://www.dspanz.org/media/website_pages/news/ssam-review-2021-report/SSAM-Review-2021-Report.pdf

30 The 2020 Inquiry into Future Directions for the Consumer Data Right touched on similar issues, recommending the formation of a common ‘data safety licence’ to manage participation in schemes where secure data holding or transfer is required. See pages 192-3 <https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf>

not feel the need to outline a distinct set of compliance requirements. Either way, participants are dissatisfied with the existing data compliance requirements across Government. Recognition of other accreditations (for example, the DSP requirements), where equivalent, could significantly reduce the complexity of the accreditation process for the CDR and reduce barriers to entry.

While mutual recognition may not always be feasible due to differing legislative requirements, as the rollout of the CDR continues, Government should continue to look for every opportunity to align CDR obligations with existing ones.

Recommendation 2.7

Where appropriate, accreditation under the CDR should be aligned with other obligations on participants, in particular, accreditation requirements for Digital Service Providers registered with the ATO.

2.10 Reciprocity in the CDR

Reciprocal data holder obligations were built into the system to grow the scope of data available for consumers and to ensure that those who join the system also contribute to the system, which is ultimately for the benefit of consumers.^{31 32} Not all ADRs are subject to reciprocal data holder obligations, the ADRs who are subject to them (such as non-bank lenders) are avoiding accreditation or looking to use alternative access models such as becoming a CDR representative (which does not activate reciprocal data holder obligations), resulting in no ADRs currently subject to reciprocal data sharing obligations.

Box 2.4 – Reciprocal data holder obligations

Where an ADR holds CDR data that was not disclosed to them under the consumer data rules (that is, not disclosed to them in their capacity as an ADR), they have reciprocal data holder obligations in relation to that data. Reciprocal data holder obligations mean that the ADR, like a designated data holder, will be required to share CDR data it holds free of charge. This includes data generated by the ADR.

31 Final report of the *Inquiry into the Future Directions for the Consumer Data Right*, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>.

32 Final report of the *Inquiry into the Future Directions for the Consumer Data Right*, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>.

The Review heard conflicting proposals on reciprocity. Submissions from major data holders (in particular, data holders in the banking and telecommunications sectors) advocated for the expansion of reciprocity to support competitive outcomes in line with the Future Directions Inquiry recommendations.³³ The inclusion of data holder obligations acknowledges that designated participants incurred significant costs in implementing CDR requirements and lose exclusive access to the data they hold. Reciprocity ensures that those firms that benefit from new data available through the CDR are required to make the other CDR data they also hold available.

“Based on the principles and scenarios identified under the CDR Act, and the desire to have CDR apply economy-wide, we would encourage greater use of the principle of reciprocity to ensure competitive neutrality in the CDR regime.” – Telstra

“It is clear that designing a system of economy-wide reciprocity would have a resource impact for regulators and ADRs, but the ABA considers it vital for consumers to fully benefit from the CDR and to ensure fair competition between designated and non-designated industries.”

– Australian Banking Association

Some participants commented that reciprocity requirements may serve to increase market share for incumbent data holders who are also ADRs because they create higher compliance costs for smaller ADRs and force the sharing of data that might otherwise be a competitive advantage for smaller participants. These obligations may therefore limit and disincentivise participation by smaller participants, which is at odds with the CDR’s objective to increase competition.

“Whilst reciprocity embodies the purist view of the CDR with open consumer data, it is seen to be unpopular amongst DRs (data recipient) as it exposes their consumer data to the major data holders (DHs), who are often also DRs, therefore presenting greater opportunity for the majors to capture additional market share.” – EY

“Unfortunately [reciprocity] ... has discouraged companies that would be beneficiaries of Open Banking data to avoid the adoption, or try and find loop-holes by seeking non-accreditation access such as via the Principal Representative (PR) model to circumvent this requirement.” – Basiq

As the system gathers momentum the disincentives of reciprocity obligations for smaller ADRs will be offset by greater data availability as the CDR grows. Developments to bring in Open Finance datasets into the CDR, including the potential designation of non-bank lending, is likely to further offset some of the issues raised around reciprocity. In the meantime, consideration could be given to whether reciprocal obligation deferrals are an effective way to support the transition of participants into the CDR until the system reaches a point of maturity and growth where these obligations could be reconsidered.

³³ Recommendation 6.9 from the final report of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>. This recommendation was focused on expanding to cross-sector applications of reciprocity so that ADRs could face reciprocal data sharing requirements from DHs operating in a different sectoral designation.

Finding 2.5

As the CDR gains momentum and the incentives to participate increase, reciprocal data holder obligations should be monitored to ensure they are appropriately supporting the growth of a vibrant CDR ecosystem.

2.11 Part Two – Conclusion

The CDR has not been easy to engage with. This is an issue that must be addressed if the CDR is to continue to develop. Significant efforts have already been made to improve the system, but further effort is needed to ensure that consumers and businesses can readily engage with it.

Priority should be given to improving coordination between CDR agencies and addressing data quality issues. More thought must be given to how consumers interact with CDR products and services, particularly with the consent requirements, about which concerns were raised by a variety of stakeholders. Work should continue on refining pathways for consumers to receive CDR data, with particular attention to liability requirements and how they could be adjusted to spread risk more effectively in the ecosystem. With this work, the CDR will be well placed to build the momentum it needs to become economy-wide and conducive to significant consumer benefit. Further changes to the system, including to the governance structure and reciprocal data holder obligations, may be in the future necessary to support its longer-term objectives.

Part Three: The CDR within an emerging digital economy

The Review heard significant enthusiasm regarding opportunities for the CDR to integrate with Australia's broader digital economy. Part Three provides an overview of some of the areas that were identified where the CDR could provide new opportunities, including aligning with technological developments in payments infrastructure as well as with regulatory developments underway.

The CDR could become a key driver of Australia's digital economy by providing consumers the infrastructure to share their data safely and securely to obtain benefits. The CDR also provides the framework that can create a flourishing data market in Australia. The Review has heard and recognised the need for alignment with other digital initiatives and regulatory frameworks, limiting duplication where possible.

A key area of the digital economy that has seen significant and rapid development is payments. The New Payments Platform (NPP) has already demonstrated improvements to consumer payment experiences and promises to deliver further consumer value in the coming years, including through its PayTo service. Further development of the CDR should consider how its unique framework for secure transfers of consumer, product and service data could integrate with and augment existing and emerging payment channels.

Alongside these technological advances, there have also been updates to the legislative framework of Australia's digital economy, for example, the recent *Data Availability and Transparency Act 2022* (DATA 2022) and the ongoing *Privacy Act 1988* review. The CDR is a complex statutory framework and, where possible, should seek to integrate and operate in concert with other government and international initiatives.

3.1 Improving settings to support CDR services for small business consumers

It was consistently acknowledged by stakeholders that the core user and focus of the CDR has always been, and should remain, the consumer – including small business consumers. However, obligations to facilitate the sharing of business data have either only recently taken effect (major banks commenced in November 2021) or have yet to take effect (non-major banks will commence in November 2022). With the majority of Australia's approximately 2.4 million businesses in a position to benefit from using the CDR to disclose their own data,³⁴ designing the CDR to facilitate the participation and particular needs of these businesses could significantly increase the value obtained from the CDR. These benefits have begun to be realised for small businesses under the UK Open Banking scheme, and were recently highlighted in the latest OBIE impact report³⁵ which focussed on how businesses utilise cloud accounting services with the integration of open banking.

34 Smaller businesses are likely to benefit from these disclosures, for example via accounting platforms. According to ABS data 93 per cent of Australian businesses have an annual turnover of less than \$2 million. ABS, Counts of Australian Businesses, including Entries and Exits, August 2021, <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release#turnover-size>

35 OBIE Impact Report June 2022, <https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-june-2022/>

Box 3.1 – The Open Banking Impact Report June 2022

Released in June 2022, the latest OBIE impact report focusses on how small businesses are utilising cloud accounting, of which Open Banking feeds are an integral part. It explored how the adoption of cloud accounting has delivered efficiencies and improvements in how small businesses are able to manage their accounts and improve business decisions.

While cloud accounting services pre-date Open Banking, cloud accounting services only started to be incorporated into Open Banking in 2019. 11 per cent of respondents would stop using their current service if the ability to incorporate real time transactions from Open Banking was lost and a further 50 per cent would seek out an alternative. The key findings from the report revealed:

- 77 per cent of small business respondents reported they now have more immediate and accurate insights into their financial position at any given time as a result of using cloud accounting services, and 84 per cent agreed cloud accounting led to them feeling more efficient.
- 72 per cent of respondents indicated the ability to connect to a bank account was an important feature, and 58 per cent felt the same regarding the availability of real-time transactions, a consequence of open banking connections.
- Some respondents suggested that cloud accounting services are saving them money, with 59 per cent saying it delivered internal savings and 64 per cent external cost savings.
- The service is beneficial when it comes to managing late payments, with 70 per cent of respondents saying so.

The CDR has so far been implemented with a primary focus on individual consumers, particularly their safety and security. It would be beneficial to give more consideration to the unique needs of small businesses within the CDR as the system matures, and of their service providers who may have additional regulatory requirements beyond CDR. Stakeholders have expressed concern that the high level of safeguards, along with obligations around handling derived data and data deletion, impair participation from service providers.

There is value in exploring an expansion of the consent time periods for small business consumers to recognise the higher frequency and enduring nature of their data usage, allowing them to maintain business setting continuity over a longer period. Under the current CDR rules, consumers choose how long they consent to their data being shared for, up to the maximum of 12 months.³⁶ In the event that consent from a small business consumer lapses, if that consent is not actively renewed, the ADR will be compelled under the CDR rules to delete or de-identify the data for that business, resulting in a potential loss for a small business consumer who relies on a CDR data product or service. It's easy to see how this could unintentionally occur in small businesses with many competing pressures. The CDR needs to reflect the realities for small business consumers by removing administrative burdens where able to allow them to focus on their core business priorities.

³⁶ Subdivision 4.3.2C Duration of consent, *Competition and Consumer (Consumer Data Right) Rules 2020*

A number of stakeholders also expressed their concern that the CDR includes data deletion requirements that compel an ADR to delete data when a consumer elects to withdraw their consent. This requirement raised concerns from participants that it would negatively impact professionals who rely on accredited accounting or business management software platforms, such as accountants, as they would be unable to meet their legal obligations to retain certain types of data (such as for tax purposes) received through the CDR. The Review also notes, however, that Privacy safeguard 12 does provide an exemption to the data deletion requirements for CDR data where “the accredited data recipient or designated gateway is required by law or a court/tribunal order to keep the CDR data”.³⁷

A further consideration influencing existing and prospective ADRs relates to derived data. The Act states that any data that is directly or indirectly derived from other CDR data is itself CDR data,³⁸ meaning that any previously non-CDR data that mixes with CDR data will attract the same CDR data handling requirements, including limitations on disclosure. This has caused concern among current and potential participants and is seen by some as a strong disincentive to participate in the system.

“The concept that CDR data is any data derived from mandated files and/or touches CDR data forever and ever until the data can no longer be attributed to the original individual/entity is near-sighted and a blatant overreach by the regulator”
– FDATA

“It is unclear why Australia has chosen to extend the definition of CDR data to derived data, as this is creating barriers to participation to avoid the ‘poison pill’ effect” – Joint submission CAANZ, CPA, IPA

A possible solution to this problem would be to ensure that everyone downstream undergoes some form of accreditation, but this ignores the significant cost and complexity of participating in the ecosystem (see also sections 1.5, 2.8 and 2.9), creating further disincentives for participation.

Finding 3.1

The CDR has the potential to provide benefits to millions of small businesses across Australia but, at present, participation is low. The Government should consider settings to facilitate small business participation, such as consent durations, data handling and deletion setting requirements. Derived data settings should also be revisited to ensure that they remain appropriately calibrated and reflective of data disclosure needs and uses.

³⁷ See Privacy Safeguard 12, <https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-12-privacy-safeguard-12-security-of-cdr-data-and-destruction-or-de-identification-of-redundant-cdr-data>

³⁸ The terms ‘CDR data’ and ‘directly or indirectly derived’ are defined by s 56AI of the Act

3.2 Data disclosures and small business consumer participation

Stakeholders have emphasised the CDR currently doesn't offer the appropriate levels of flexibility to allow business consumers to operate in the ecosystem. The recent introduction of trusted advisers has gone some way to alleviate this, but the framework falls short in addressing how a majority of small businesses operate in practice.

Under the current framework, the trusted adviser specification does not reflect the needs of small business consumers, including sole traders and small family businesses, where the role of a trusted adviser can often fall to a family member or employee. In some cases, this adviser may not hold formal accounting qualifications (e.g. a CPA) and might solely manage the business using an accounting or business management software platform, meaning that they would be unlikely to be included under the definition of trusted adviser.

"Many SMEs rely on bookkeepers, who may not otherwise have formal qualifications, to keep their business afloat. Disrupting this practice by excluding bookkeepers from the definition of 'trusted adviser' and limiting a consumer's ability to control who they trust with their data, fundamentally risks undermining the usability of the CDR and risks existing market practices" – FDATA

Many business consumers are unlikely to make the switch from unsafe but more convenient alternatives like screen scraping until the CDR can meet their needs and provide a comparable service. A factor for this is improving data quality (see section 2.1), with current service providers potentially hesitant to switch to the CDR due to the concern they will inadvertently provide a poorer quality experience and product for their customers than the less secure but more convenient alternatives.

"Treasury's intention for the rules to facilitate current consumer practices of the permissioned sharing of their data with trusted third parties ... is a good one and deserves support. However, it doesn't encompass the agency small businesses in Australia currently enjoy and depend upon to run their businesses." – Xero

The differences between individual consumers and small business consumers need to be acknowledged, including different requirements and potential tolerances around who the data is shared with. While both individual and small business consumers have access to trusted adviser disclosures, particular consideration should be given to providing small business consumers the flexibility to consent to sharing their CDR data with individuals outside the limited categories of trusted advisers currently defined under the rules, while maintaining the current protections offered to individual consumers.

The Review acknowledges that some submissions by contrast advocated removing trusted adviser disclosures entirely from the CDR due to the increased risks associated with CDR data exiting the CDR system. Some submissions raised concerns relating to instances where consumer consent can be given for data to be disclosed to unaccredited persons outside the CDR to whom the Privacy Safeguards, and potentially the APP, do not apply. In allowing disclosures to unaccredited parties, CDR settings should ensure that consumer risks are reduced by either limiting the eligible recipients or requiring that the data disclosed meet a specific, limited purpose. In the case of small business consumers, this would seem to favour the latter setting – where disclosures are explicitly for business-related purposes.

The Review recognises the importance of data handling protections and their importance in system and consumer safety outcomes. In balancing the settings for business and individual consumers it is important to recognise that risk and benefit profiles will be different for different cohorts of CDR users, particularly in relation to promoting safer data sharing practices (compared to practices like screen scraping) and supporting improved business operational outcomes.

A potential remedy to improve CDR utility for small business consumers is to give further thought to how small businesses operate and what services they use. For example, should the small business consumer desire, consideration should be given to allowing the data sharing outside the CDR with a third party with their consent.

There are some risks with this approach as any CDR data provided to an unaccredited third party (other than a CDR representative or an outsourced service provider) would then be outside the protections of the CDR and, where the recipient has an annual turnover below \$3 million, they would not be covered under the obligations of the *Privacy Act 1988*. This is unlikely to be optimal for an individual consumer but may be appropriate for the needs of small business consumers.

Any change would need to consider how to differentiate an individual versus a small business consumer and ensure the protection of vulnerable consumers (which can include small business operators). The Review recognises that many small business and sole traders can have significant overlap in their personal and business accounts, making it difficult to separate personal and business data, the latter of which could include financial information and activity from third parties. Careful consideration must be given to ensuring appropriate protections are maintained accordingly.

Recommendation 3.1

Government should consider ways to increase small business participation in the CDR. This could include giving small businesses flexibility to consent to share their CDR data with parties outside the limited 'trusted adviser' categories currently defined under the CDR rules. Consideration should also be given to enabling small businesses to consent to share data outside the CDR to a third party for explicitly business-related purposes.

Any amendments to support wider sharing of CDR data should ensure the maintenance of existing protections offered to individual consumers and carefully consider the impacts of any potential overlap between business and personal data.

3.3 Supporting cross-sectoral use cases across the digital economy

As Australia and the rest of the world move towards a more horizontally integrated economy where businesses provide products and services that span traditional sector boundaries, the vertical structures between sectors will become increasingly blurred and consumers will expect a greater level of integration across different domains of their lives. The CDR is optimally placed to facilitate this and is on the precipice of doing so by providing a conduit from which businesses can compete across multiple sectors. Some stakeholders suggested that cross-sectoral use cases had the greatest capacity to drive consumer value.

“The TCA recommends moving away from the current sector-based model toward a sector-agnostic, use-based model that is standardised by data use cases such as online payments and mortgage applications.” – Tech Council of Australia

“Continue with expansion and acceleration of CDR to include broader government and private sector datasets to enable more innovative customer value propositions.” – Commonwealth Bank of Australia

Facilitating these use cases may be particularly difficult under the existing sector-by-sector approach to rolling out the CDR.

“The government needs to consider the impacts and consequences as sectors are designated, as sectors do not function in isolation. It is important to understand and recognise some sectors have cross sector dependencies.” – PEXA

Box 3.2 – Cross-sectoral products, use case example

Considering the purchase of rooftop solar can be a complex process. To make an effective decision, consumers need to consider their existing household energy usage, whether they have the capacity to absorb the upfront costs or whether a loan might be required and, if so, whether the benefits of installation outweigh the cost. To support this difficult decision, a CDR-powered service could access customer financial data and energy data simultaneously to provide a complete picture of the value of pursuing rooftop solar, as well as provide bespoke product recommendations.

Whilst the sector-by-sector rollout is a pragmatic and intuitive approach in the short term, it has also resulted in new rules/standards/consent processes for each sector. These bespoke processes are developed in response to the particulars of each sector, but also reinforce the vertical sectoral silos, increasing system complexity and friction for cross-sectoral activity, potentially providing a barrier for more innovative cross-sectoral use cases. This also increases the burden on participants, who either spend considerable time and effort trying to understand and build to different requirements by business activity, increasing costs, or forgoing expansion to a particular sector. Neither result is desirable, with the first disincentivising participation and the second resulting in reduced consumer value and innovation.

To build a truly cross-sectoral CDR, further consideration will need to be given to moving towards greater alignment and sector neutrality of the rules, standards and consents for participants. The CDR should aim for horizontal integration and reusability across sectors in its design and differences should be by exception.

“CDR authorities must work together to create a single set of standards and rules that all sectors can use. Only then will we be able to see the full potential of the Consumer Data Right” – Intuit

Alignment must also extend to address the use of different unique identifiers between sectors to identify the consumer. Currently, energy providers use an address and/or metering device, banking uses a customer identification number, government financial initiatives use a Tax File Number (TFN), and businesses are primarily identified by an Australian Business Number (ABN). To support future cross-sectoral use cases, it will be critical to have an overarching unique identifying layer or data interoperability mechanism between unique identifiers within the CDR to reliably identify the consumer and manage consents while maintaining appropriate privacy protections. Without this, it will be more difficult to bring together consumers' datasets from across sectors and providers. Consideration needs to be given to addressing this issue to allow better cross-sectoral operation, both within the CDR and across the broader digital economy, with the use of common, economy-wide identifiers, such as digital identity.

"Without introducing a common identification framework or including a Digital Identity, cross-sectoral data sharing will be impossible from a consent perspective"
— FDATA

Finding 3.2

Expanding the CDR to deliver cross-sectoral use cases will require a method of consumer identification that spans different sectors and interactions. This will require utilisation of identity solutions beyond the existing unique identifiers adopted in energy, financial and telecommunications sectors to enable seamless user experiences.

Australia's CDR does not operate in a vacuum. It is part of larger global digital economy, a fact highlighted in the Future Directions Inquiry.³⁹ It has been suggested the CDR is "quite simply world leading",⁴⁰ but we risk losing this position and missing opportunities to compete in a larger global ecosystem if we don't address the issues that prevent interoperability across sectors. Failure to do so will leave Australian businesses at a disadvantage to competitors from international markets and consumers potentially ultimately worse off. It may also lead to a situation of increased compliance burdens on participants operating across multiple schemes internationally.

Australia is uniquely placed to promote the CDR as defining the standard for data portability frameworks, particularly given that there is no universal or preeminent standard globally.

"Wherever possible, we suggest harmonising data security and privacy obligations with existing systems and international standards. With many Australian businesses operating overseas, adopting internationally consistent rules minimises compliance burden" — Tech Council of Australia

³⁹ Recommendations 8.9 and 8.10 from the final report of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

⁴⁰ Submission from Scientia Professor Ross Buckley and Dr Natalia Jevglevskaja

Finding 3.3

Prioritising the development of the CDR as an internationally interoperable data portability initiative will deliver significant consumer benefits by way of a greater willingness for participation from international product and service offerings.

3.4 Role for government participation in the CDR

The CDR already includes some government participation – the Australian Energy Regulator (AER) will act as a data holder for the energy sector. A clear theme of the recent Treasury Strategic Assessment was the desire for the wider inclusion of public sector data in the CDR. This assessment suggested the use of public sector data to drive innovation and improve how consumers use government services, as well as to increase consumer trust in both government data use and the CDR. Similar suggestions were heard in submissions to this Review.

“The convenience to have data securely shared both between government agencies and between agencies and business, and the efficiencies to deliver services faster will provide significant value to Australian citizens.” – EY

*“Rather than scrap Public Datasets from the CDR, a concerted effort much (sic) be made to find a way to include them in the CDR, as this will supercharge the adoption of CDR through the development of complex and beneficial use cases.”
– FDATA ANZ*

There is also potential for consumer value through government agencies participating as recipients of CDR data. Australians are increasingly interacting with government services through digital channels, and when government agencies are able to use consumer information with consumers’ consent, they can deliver more seamless experiences for Australians through a more integrated digital ecosystem. The use of consumer data to support tax payments should be considered as one possible starting point for expanding the CDR to government participants.

In March 2021, Her Majesty’s Revenue and Customs (HMRC) partnered with the private sector to deliver an open banking solution to paying personal taxes. This solution enabled taxpayers to consent to allowing a third party provider to initiate a payment by prefilling payment reference number and amount, decreasing human error and risk of fraud. As of January 2022, open banking was used to support the transfer of over £2.4billion with 13 different tax categories now supported under the scheme.⁴¹ HMRC’s participation in the UK Open Banking scheme demonstrates that government participation has the potential to unlock significant opportunities for consumer benefit, and to provide opportunities to support private sector innovation in the digital economy.

41 Open Banking UK, UK open banking marks fourth year milestone with over 4 million users, January 2022, <https://www.openbanking.org.uk/news/uk-open-banking-marks-fourth-year-milestone-with-over-4-million-users/>

Box 3.3 – Unlocking Government-held data, use case example

Businesses often rely on trusted advisers and other services to understand their tax requirements and status, effectively manage their finances, and comply with regulatory obligations. This includes providing tax returns, business activity statements and other tax information for loan and credit applications. Finding and accessing appropriate financing could be simplified for consumers with the ability to share relevant tax data directly from the ATO to the service assessing their loan applications or helping to manage their finances.

More government-held data could be included in the CDR. With most Australian governments (State and Federal) supporting and promoting the opportunities of the digital economy to unlock future growth and productivity gains, it is important for the Government to model the behaviour it seeks from the broader economy.

Some modification to the CDR framework may be necessary to support expansion of the CDR into government datasets (see also Recommendation 1.1). The existing sectoral approach has limited capacity to designate government data as government-held datasets can currently only be included as part of a CDR rollout to a designated sector.⁴² This Review has already suggested that a more discriminating or targeted approach may be warranted for designating new datasets, and this may need to support the incorporation of government-held data, unless government-held data can be designated as its own ‘sector’. Undertaking a sectoral assessment of government-held data would be extremely difficult to facilitate given the wide breadth of functions government fulfils. Designating government as a sector could also overlap with existing government data sharing initiatives (such as DATA 2022), which would unnecessarily add to the complexity of the data regulations in Australia. If legislative changes are needed for a more targeted approach to CDR expansion to support high-value and safe use cases facilitated by government data, this should be addressed as a matter of priority.

Further areas of existing legislation that may require attention include:

- secrecy provisions that prevent the sharing of government-held data, even with a consumer’s consent. The Data Availability and Use report found that together these (over 500) provisions “impose considerable limitations on the availability and use of identifiable data.” With these provisions in place, the existing CDR statutory framework may not be able to enable sharing government-held data.⁴³
- fitness-for-purpose of the scheme’s accreditation and other requirements for government recipients. This could include how the scheme’s privacy safeguards would operate in practice for government ADRs,⁴⁴ and implications of derived data requirements.

⁴² This is how data held by the AER became designated under the CDR.

⁴³ See, for example, section 355-25 and 355-35 of the Taxation Administration Act 1953.

⁴⁴ See for example, Privacy Safeguard 9 – Adoption or disclosure of government related identifiers by accredited data recipients.

Recommendation 3.2

Facilitating government participation in the CDR should be a priority to ensure consumers benefit from more seamless government interactions and an ability to share their data across a greater range of services. Consideration should be given to how designation, accreditation and standard setting processes can optimally facilitate government involvement alongside other initiatives, such as the Data Availability and Transparency scheme.

3.5 Awareness of the regulatory landscape outside the CDR

The CDR should align with regulatory changes and limit duplication where possible. Participants spoke of the impacts caused by separate but concurrent regulatory processes and obligations within and outside of the CDR. There are several changes that are set to have a significant impact on shaping the digital economy, including the *Data Availability and Transparency Act 2022* (DATA), the review of the *Privacy Act 1988*, the review of the Financial Services Legislation, the payments system reforms, and the ongoing Quality of Advice Review. It is crucial that these policies work together effectively and minimise unnecessary overlap and compliance burden.

The recent passage of DATA will allow government agencies to share data with accredited Australian state and federal government agencies and Australian universities. DATA enables sharing for the delivery of government services; informing government policy and programs; and research and development. The CDR and DATA share similarities, including an accreditation framework for data recipients, bespoke privacy safeguards and use cases to streamline service delivery for consumers. There are, however, clear differences between the two schemes. The objectives of the schemes are different – DATA aims to promote the availability of public sector data for prescribed purposes, while the CDR aims to promote consumer choice, innovation and competition through greater consumer, product and service data portability in designated sectors. DATA does not mandate data sharing, which is subject to the agreement of the data holder and accredited recipient rather than being consumer-initiated. As the CDR moves to increase government participation in the CDR as both a data holder and a data recipient, careful consideration should be given to how these systems can operate most effectively together and whether aspects of their implementation can be aligned, such as:

- facilitating the inclusion of government-held datasets, noting the differing objectives of the DATA and the CDR,
- recognition and alignment of accreditation frameworks (see Recommendation 2.7), and
- alignment of data standards, including terminology where possible.

The Digital Transformation Agency (DTA) has also been developing legislation for an Australian Government Digital Identity System, building on the infrastructure developed to deliver myGovID. Though focused on proving identity, this is, at core, a data sharing framework. Should the Government be inclined to continue this work, it is important for the CDR and Digital Identity framework to complement each other where possible to ensure a seamless digital experience for users and a navigable system for those delivering services.

The *Privacy Act 1988* was also raised by several submissions, with general concern that the *Privacy Act 1988* and the CDR create dual requirements for participants in the CDR. Participants noted that these dual requirements create significant and unnecessary complexity, particularly for smaller participants (without large legal teams) required to interpret their obligations under each of these frameworks.

“Placing privacy protections into legislation not related to privacy not only increases the complexity of that legislation but creates a risk that people seeking to understand how the privacy of their data transmitted through CDR channels is protected in the Privacy Act 1988 (Cth) will potentially consider that none exists.” – Joint submission CAANZ, CPA, IPA

The requirements on participants for data sharing and use under the privacy safeguards were, however, generally seen as being appropriate for participating in the CDR. It is difficult to see how these arrangements could be simplified while providing a high degree of consumer protection without making general changes to the *Privacy Act 1988*. The CDR should not be the mechanism through which changes to Australia’s general privacy landscape are achieved. Instead, the ongoing Privacy Act Review should consider what the appropriate privacy settings are for the wider economy. If this results in a lifting of standards to a level similar to the CDR privacy safeguards, then consideration should be given to amending the Act and the CDR rules, removing any duplicative obligations and providing a level of alignment.

“Simplicity and consistency in privacy obligations will benefit both businesses and consumers in understanding their rights and responsibilities and will also aide situations where businesses may operate internationally (and therefore be subject to a range of international privacy requirements as well).” – Telstra

Finding 3.4

Protections provided by the CDR are designed to ensure the integrity of the scheme is maintained as it moves across each sector working alongside the *Privacy Act 1988*. Where opportunities for alignment with the *Privacy Act 1988* are identified, the CDR protections should be reviewed to reduce duplication and increase alignment.

Although they impact only those in the financial services sector, the ongoing Review of the Legislative Framework for Corporations and Financial Services Regulation by the Australian Law Reform Commission are good examples cited in illion’s submission of ongoing processes that may provide some avenue for regulatory alignment.

A close eye should also be kept on any potential decisions and regulatory changes impacting payments systems, which include the nascent technologies of cryptocurrency and digital wallets. With the CDR poised to make the step into payment initiation, any changes to the payment ecosystem may have potential overlaps that should be considered. In particular, Scott Farrell recommended in the recent Review of the Australian Payments System “aligning the requirements under CDR accreditation with the payment services licence where appropriate. For example, the payment services licence should contain requirements that are built on top of the relevant information security requirements under the CDR.”⁴⁵

45 Payments System Review, June 2021, <https://treasury.gov.au/sites/default/files/2021-08/p2021-198587.pdf>

“We recommend government consider the cumulative regulatory burden associated with all of these reforms as it contemplates the CDR legislative framework. Moreover, any changes to the CDR should avoid confusion or tension between regulatory frameworks across portfolios. It would not be helpful for any proposed changes to the Privacy Act to be at odds with the legislative framework or rules underpinning the CDR, for example. Similarly the Payments System Review is also contemplating similar issues, including a right to action. We strongly encourage Treasury and all relevant portfolios work proactively together to ensure alignment between the various streams of related work.”

— Business Council of Australia

The CDR has also been specifically called out in the terms of reference for the ongoing Quality of Advice Review (QOAR). Given the CDR has the potential to streamline the provision of a data collection process for the digital tools used by financial advisers, reducing the time and effort to collect customer data and thus the cost for the consumer, there is high level of overlap between the two Reviews. Attention should be given to the final report for the QOAR, particularly as it relates to any findings or recommendations that specifically reference the CDR, such as potential use cases and the identification of new datasets.

It is important, as the CDR moves forward, that it remains cognisant of the both the existing and emerging regulatory landscape, keeping an eye on overlapping schemes, recognising the pre-existing regulatory burdens that have already been placed on certain sectors and seeking out opportunities for alignment and remove duplication where possible.

Finding 3.5

The regulatory environment that the CDR operates within is complex. Where possible, the CDR should seek opportunities for alignment with other regulatory schemes, limiting duplication and overlapping regulatory obligations to make the CDR easier to navigate, reducing additional compliance burdens and confusion for participants.

3.6 Alignment with other initiatives in the digital economy

The CDR has the potential to become a key driver of Australia’s digital economy. Data portability is a core capability that supports digital services, including streamlined and/or automated payment transfers and supporting capabilities for these services, such as digital identity.

The Review has discussed the importance of digital identity to enable CDR cross-sectoral use cases, a view supported by many participants who saw digital identity as important to future growth in the CDR system and a key dependency for the system, particularly in supporting payment and action initiation. The Future Directions Inquiry and Strategic Assessment also raised it as a recommendation.

Box 3.4 – What is digital identity?

Digital identity can help individuals verify their identity in a safe and secure way to access services online. This can include services provided by the Commonwealth, states and territories and the private sector. Digital identity can remove the need for individuals and businesses to visit a shopfront with their identity documents for some transactions but does not replace the foundational, typically government-originated documents that support identity proofing and verification.

“With the expansion of CDR into other sectors, CDR and Digital Identity ecosystems will require strong interoperability, particularly between private and public sector networks. Each system needs to maintain their own independence, as not all Digital Identity use cases will involve data sharing or have a link into CDR use cases, but CDR will become a very important user of an interoperable digital identity ecosystem, driving strong consumer choice and a more streamlined approach to customer verification and authentication requirements under CDR.” – NAB

Noting that there are various proposed solutions to provide digital identity for government and private sector services, many participants the Review spoke to saw a role for government in facilitating broader uptake and use of digital identity. This included providing channels for the market to leverage government biometrics databases to enable high-level identity verification for online transactions or actions where a high degree of identity assurance is needed.

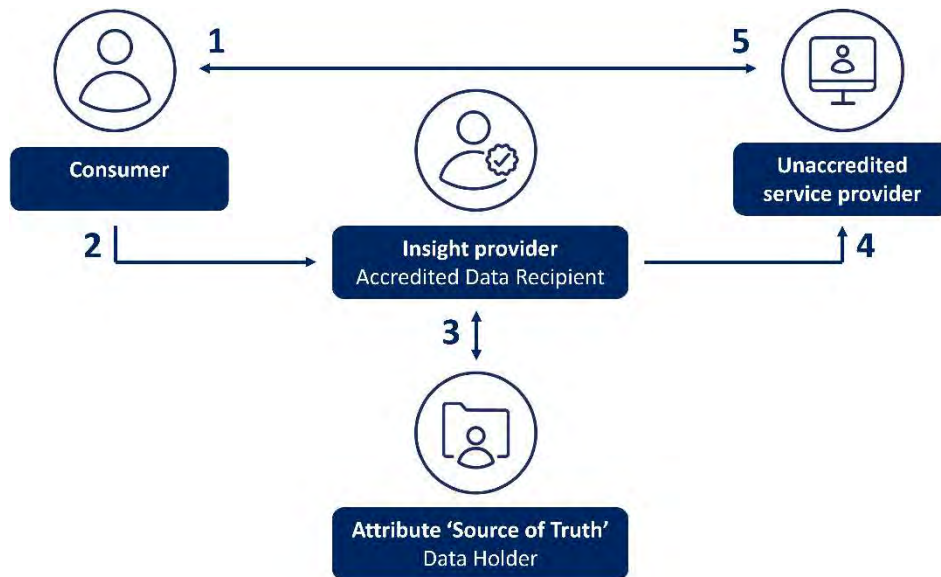
In considering any approach to digital identity, the Government should be careful not to provide potential solutions through the CDR that duplicate existing solutions or are disconnected from existing solutions under development. Noting the challenges of establishing an effective, economy-wide approach to digital identity, further work should be done to ensure any integration of digital identity in the CDR ecosystem is aligned with and supports existing regulatory and legal frameworks. Any approach should also align with and not duplicate existing regulatory obligations in the wider market or sectors where the CDR operates, such as Know Your Customer checks and *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) obligations that apply in the financial sector. Depending on what digital identity solution is used, some obligations such as AML/CTF may require the inclusion of additional data not currently covered by the CDR e.g. date of birth.

“We recommend Treasury work with AUSTRAC and with the Digital Transformation Agency, which has developed the Trusted Digital Identity Framework, to better assess how account creation can be enabled digitally within a robust regulatory and legal framework to avoid regulatory duplication by attempting to solve for digital identity via the CDR” – Commonwealth Bank of Australia

Though the CDR cannot provide a framework for delivering an economy-wide digital identity solution, there is potential for the CDR to do more than just use digital identity. The CDR has the potential to enable or support digital identity by allowing consumers to share complementary datasets to strengthen authentication of their identity and/or attributes (e.g. that they hold qualifications or credentials they say they do).

For example, when a person is required to confirm their identity and attributes with an unaccredited third party provider (such as a real estate agent), that third party could ask the person to provide consent for an ADR to receive attribute data through the CDR from data holders (such as banking information or energy bills) so that the ADR can verify the identity and attribute information for the third party. This process could save consumers the onerous process of collecting, formatting and providing attribute information themselves and would be more secure than existing processes to share identity and attribute information with third parties.

Figure 3.1 – CDR and attribute verification



With the CDR providing the framework to support open banking and Open Finance, along with the former Government's agreement⁴⁶ to accept the Future Directions Inquiry recommendation to implement payment initiation, the CDR will interact with the New Payments Platform (NPP) (see Box 3.5). Submissions to the Review from the ABA and the Australian Payments Network highlighted the similarities between the NPP and its new PayTo service offering to support and streamline payment transfers, with many suggesting the CDR should be leveraging and aligned with this work, potentially achieving a 'quick win' for payment initiation. This alignment includes looking to minimise friction points where possible to improve the consumer experience (such as with the consents process), and reduce regulatory compliance for participants, with consideration to any potential risks that may undermine the integrity of the system. For example, the submission by Australian Payments Network noted that the CDR consent flow (in the Consumer Experience (CX) guidelines published by the DSB) currently requires consumer involvement in five distinct steps of the flow, whereas PayTo allows a consumer to authorise a third party to provide specific payments on their behalf, offering a streamlined interaction for the consumer.

46 The Government response to the Inquiry into Future Directions for the Consumer Data Right, December 2021, <https://treasury.gov.au/publication/p2021-225462>

Box 3.5 – New Payments Platform (NPP) and PayTo at a glance

Launched in 2018, the New Payments Platform (NPP) is Australia's real-time payments infrastructure that supports the transfer of funds on a 24/7 basis. The NPP's new PayTo service streamlines payments authorisations and supports a range of use cases from recurring or subscription payments, ecommerce and in-app payments, one-off payments, funding for other payment options such as digital wallets to third party payment services such as corporate payroll. For example a consumer could set up a recurring payment in their internet or mobile banking app as an alternative to direct debit, allowing them to see and control recurring payments, with the ability to stop them at any time. The rollout of PayTo by businesses participating in the NPP started in June 2022.

"The ABA supports greater alignment of these requirements now to ensure that as banks continue to build for both the CDR payments initiation and PayTo, they can do so in a manner that ensures interoperability between the two as this will ensure a better consumer experience" – Australian Banking Association

"As significant payments infrastructure with a fully developed rules framework and liability model, PayTo should be closely considered when the detailed design work is performed to extend the CDR framework to include payment initiation and when the accompanying legislation is developed" – New Payments Platform

Finding 3.6

There is significant enthusiasm for the delivery of action initiation under the CDR, with many submissions noting the opportunities for the CDR to capitalise on concurrent work being undertaken within payments systems, such as PayTo. Where possible, the CDR should work in conjunction with other initiatives to minimise potential friction points and reduce regulatory compliance for participants, with the objective to create more streamlined consumer experiences.

3.7 Role and importance of the consumer voice in the CDR

As flagged at the outset, a key theme encountered in this Review is consumer-centric utility as a core objective of the CDR. Some submissions have raised concerns that the consultation on CDR developments has favoured those deeply engaged with the CDR ecosystem (such as fintechs and businesses in designated sectors) with the resources to participate, and has lacked adequate consideration of consumer voices. Without a well-represented consumer perspective to balance the voices of other participants in the system, some are concerned the CDR will be driven from the core objects of the CDR for consumer benefit.

“The FinTech and financial services sector view of the consumer perspective is ... inevitably seen through a profit motive lens, rather than developing the CDR to address genuine consumer needs.” – Financial Rights Legal Centre

Consumer advocacy groups have been actively attempting to fill this void at personal cost; as noted by the Consumer Policy Research Centre, “the burden placed on consumer groups during consultation is extensive and excessive”. The CDR will need to continue to look to consumer advocacy groups because it is not feasible to expect ordinary consumers to engage directly in these processes. The Review was grateful to receive a submission from a private citizen with the time and knowledge required to effectively participate in a consultation process, but this participation is an exception rather than the rule. The issue of consumer representation is not isolated to the CDR, rather, it is endemic across many government consultation processes. This further compounds the realities faced by consumer advocacy groups on how to best allocate their limited resources and effectively participate in these processes.

“The ability for policymakers to fully consider the benefits and risks of a reform like CDR relies upon the ability for consumer organisations to effectively participate in such processes. CPRC strongly encourages the Australian Government to make provisions to adequately fund consumer representation to effectively participate in these processes.” – Consumer Policy Research Centre

The importance of consumer advocacy groups as representatives for consumers cannot be overstated, but it is not an issue solely for the CDR or its processes. Rather, Government must take a consolidated approach, which may include providing additional funding for consumer advocacy groups to meaningfully participate in processes with clear and direct impacts on consumer cohorts.

Recommendation 3.3

The consumer voice is amplified through consumer advocacy groups. These advocacy groups are generally under-resourced, inevitably diminishing the consumer input into the development of the CDR and other government consultation processes more broadly. Additional funding may be needed to support consumer advocacy groups to meaningfully participate in not just the development of the CDR but across government initiatives.

Part of amplifying the consumer voice is creating a CDR ecosystem that is easy and encourages consumers to raise complaints. A submission from Cuscal suggested that “[a]s the regime expands it will become difficult for consumers to ascertain which organisation, they are required to raise complaints and seek actions for redress”. Cuscal goes on to suggest that a single agency could be defined through which consumers raise complaints and which directs these complaints as required.

As a cross-sectoral scheme, the CDR was always designed to include multiple regulators to fulfil separate roles and responsibilities.⁴⁷ The Review recognises and supports that from the outset that, to be an effective consumer-facing policy, the CDR should have a ‘no wrong door’ approach (see section 2.3) to handling consumer complaints, so as to avoid, as the original Productivity Commission report put it, leaving “the consumer straddling in a regulator abyss”.

3.8 Beyond the Statutory Review

This Statutory Review takes place five years after the initial conception of the CDR in the Productivity Commission’s Data Availability and Use report. As previously stated, it comes at an important time for the CDR as it transitions from a build phase into a phase of maturing to develop its scope to deliver significant consumer benefits. This Review has offered a number of short to medium term changes to the statutory framework to support the maturation of the CDR. It also recognises that some of these changes may not be long term solutions and identifies a number of elements of the statutory framework that may need further consideration in the future, which could include:

- direct to consumer data sharing (section 1.6)
- implementation and governance arrangements of the CDR and other digital economy initiatives (section 2.3), and
- reciprocal data holder obligations (section 2.10).

The CDR has undergone substantial adjustments even in these early stages, and there should be an ongoing provision for considered review to ensure it remains agile and fit-for-purpose. Submissions from the Australian Energy Council and the OAIC recommended that a further statutory review of the CDR be conducted in the future, with the former suggesting repeating reviews every three years and the latter suggesting a further review within the next five years.

This Review supports a further statutory review occurring within the next five years, capturing the lessons from the next iterations of the economy-wide rollout and allowing an additional course check and design calibration as the system continues to mature. A future statutory review could address the considerations listed above if they remain pertinent along with any further issues that arise in the meantime, particularly in relation to the development of the CDR to include payment and action initiation and other developments in the wider digital economy.

⁴⁷ See *Data Availability and Use – Productivity Commission Inquiry Report*, No. 82, March 2017, <https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf>

Finding 3.7

Consider a future statutory review within the next five years. This review may consider direct-to-consumer data sharing, the implementation and governance arrangements of the CDR and other digital economy initiatives, reciprocal data holder obligations, as well as any other issues that arise.

3.9 Part Three – Conclusion

The Review encountered sincere enthusiasm and optimism from stakeholders around opportunities that will arise as the country continues its development as a digital economy. Australia has already made significant advances in areas including payments, e-invoicing and the digital delivery of government services. Stakeholders were confident that the CDR is an important part of the future Australian digital economy.

To capitalise on the opportunities of the digital economy, the CDR must be appropriately configured to facilitate the inclusion of different types of consumers like business, to grow the ecosystem, while ensuring the broader consumer voice isn't lost. Thought also needs to be given to how the CDR will operate across sectors and which components are needed to allow interoperability not just between sectors, but also internationally. Finally, the CDR needs to keep a finger on the pulse of other regulatory frameworks and initiatives within the digital economy, looking for alignment where possible and leveraging existing infrastructure.

Part Four: Other issues raised in submissions

As detailed throughout this Report, the Review has responded to stakeholder observations and suggestions that went to the functioning of the overall CDR framework and its continuing implementation. The Review also acknowledges additional suggestions from stakeholders that could be considered in the future development of the scheme (see table 4.1). Any further consideration of the issues identified in this section should be undertaken in the context of ongoing future legislative, rule-making and standard-setting updates, with a view to ensuring that the framework remains fit-for-purpose into the future. Some of these issues are relatively technical in nature, others extend beyond the scope of this review or require further consideration in the context of an evolving CDR system.

Table 4.1 – Other issues raised in submissions

| Issues that could be adopted in the context of future CDR updates | |
|--|---|
| Aligning consent processes across the payments and digital ecosystem | Section 3.6 of the Report finds that the CDR should look at opportunities to align and interface with PayTo and other payment initiatives to deliver action initiation. In addition, and to achieve this, consent flows across payments and CDR need further separate consideration. Multiple submissions suggested that work needs to be done to align the consent flows under the CDR with those for PayTo where possible. In particular, the Australian Payments Network recommended that a review of rules 4.11(1)(c), 4.13(1), 4.22 and 4.25(1) will be necessary to facilitate this. The Review encourages further assessment of the necessary rule changes once the primary legislation has been amended to enable action initiation, which go to Finding 3.6, that consideration could be given to aligning the CDR and PayTo consent requirements where appropriate. |
| Better defining sectors | Submissions from the Australian Payments Network and Australian Energy Council noted that the language of the objects in s56AA(a) in the Act could be sharpened. Notably, the objects refer to <i>certain</i> sectors being covered by the CDR, where it could instead refer to <i>designated</i> sectors. The Review supports such a change to improve focus in the language and meaning of the part's application to designated sectors. |
| Clarifying 'accredited persons' | The Financial Rights Legal Centre and Rajbhandari and Burden noted that s56AA(a)(ii) refers to accredited persons as the only ones able to access data through the CDR. Under existing data sharing arrangements, data can be shared with unaccredited persons such as Trusted Advisers or CDR Representatives. To reflect these arrangements, s56AA(a)(ii) in the Act may need to be clarified. |

| | |
|--|--|
| <p>Enabling direct to consumer data sharing</p> | <p>The legislative framework is broadly suitable to support direct-to-consumer data sharing. Part 3 of the CDR rules outlines requirements for data holders and direct to consumer data sharing.</p> <p>Whether it is timely to ‘switch on’ direct-to-consumer data sharing is a separate matter, and the Review has found that it is not timely to do so (Finding 1.3). Consumer data sharing at this stage would not offer significant benefits to consumers and poses apparent risks. These risks may change as the CDR system matures, and the nature of consumers’ engagement with data changes, at which point safely enabling direct-to-consumer data sharing may be worthwhile.</p> <p>When conditions have reached a point that risks around direct-to-consumer data sharing have decreased on balance, the functionality and obligations can be enabled through a rule change to the relevant schedules.</p> <p>Data holders are not restricted from enabling direct-to-consumer data sharing of their own volition. The CDR supports data holders making that available without waiting for rules requiring them to share it. This would be the case for the banking sector and any data holders electing to disclose ahead of being required to (Rules Schedule 3, Clause 6.5) according to the commencement table (Schedule 3, Clause 6.6 – which is silent on Part 3 obligations – effectively leaving them switched off). There are caveats to this in that there is a requirement to adhere to CDR standards in making this disclosure – standards which don’t currently exist – and for it to be provided in a human-readable form. Any attempts to develop a CDR-compliant data sharing mechanism ‘through CDR’ in this context will potentially need to be revised if these settings change, and banks already often have existing methods for sharing data with customers outside of CDR.</p> <p>In the energy sector, obligations around Part 3 of the rules are explicitly referenced as not applying (Schedule 4, Clause 8.5), so any disclosures made by data holders to requests from consumers would be outside the CDR, unless that obligation is revised in rules updates.</p> |
|--|--|

| | |
|---|--|
| <p>Expanding CDR rules to support the use of CDR data in credit assessments</p> | <p>The Australian Banking Association, Australian Retail Credit Association and the Commonwealth Bank of Australia suggested amending Clause 7.2 of Schedule 3 of the rules to expand the condition of data sharing to include circumstances where a consumer applies for and/or acquires a product. The current rules limit the use of CDR data for the purposes of credit decisions by allowing the data to be retained only if the consumer acquires this product, in the circumstance a product is not acquired the data must be deleted. This suggestion could enable further use cases to be developed in credit assessments, potentially allowing consumers to more easily switch providers or access products.</p> |
| <p>Rules changes to improve user experience, potentially through allowing bundling of consents</p> | <p>The Australian Payments Network submission suggested a rules change was necessary to support payment initiation and consent bundling. Notably, rule 4.10(b)(ii) explicitly prohibits the bundling of consents with other directions, permissions, consents or agreements. Further attention could be given to allowing consent bundling in certain circumstances with a view to where the benefits of a simplified consumer interface can outweigh the potential risks, noting this is only part solution as mentioned in section 2.7. If such an assessment concludes in favour of consent bundling, then r4.10(b)(ii) may need to be amended, noting that r4.9(d) suggests that consents are required to be 'specific to a purpose' which, as pointed out by the Australian Payments Network, may be sufficient to protect against inappropriate use of bundled consents. Such amendments should be considered in light of Finding 2.2.</p> |

| Other issues raised in submissions | |
|--|---|
| Adopting a stronger commitment to expanding CDR based on cost-benefit analysis | Submissions to the Review suggested that the Government should adopt a stronger cost-benefit approach to decision making in the CDR statutory framework. This includes framework features such as designation, privacy and security requirements in producing the Regulatory Impact Statements (RIS), and accreditation requirements. Submissions from the Australian Banking Association, Australian Energy Council, Consumer Policy Research Centre, Financial Rights Legal Centre and Telstra noted a need to undertake cost benefit analyses at various stages to inform decision making. The Review recognises the importance of appropriate cost-benefit analyses, but also notes that a careful balance is required so as not to duplicate existing processes, introduce further barriers and complexity to the system, or add further burden to participants. |
| Increasing consideration for a wider range of consumers, particularly vulnerable consumers | <p>As noted in section 3.7, the elevation of consumer interests should be considered to ensure the CDR continues to deliver its objectives. These considerations should be made across the various elements of system design. The Future Directions Inquiry similarly has made recommendations to support the participation and protection of vulnerable consumers in the CDR (particularly through Chapter 7).</p> <p>In a submission from the Financial Rights Legal Centre, it was suggested that some CX testing to date did not include a statistically significant sample,⁴⁸ and it was also suggested that this testing has failed to adequately capture the voice of a number of groups of vulnerable Australians.</p> <p>Through consultation for this review, it was clear that attention hasn't been given to actively incorporating the voice of vulnerable consumers in the rollout of the CDR, particularly to culturally and linguistically diverse communities. The Review encourages further work to attend to vulnerable consumer needs as a priority, and to be cognisant of cohorts who might be particularly at risk from new developments from the CDR (for example, older Australians). Consideration should also be given to how CDR sector assessment processes can best identify any unintended consequences for vulnerable groups, as raised by Bednarz et al in their submission on the inclusion of insurance data. Greater attention should also be given in providing opportunities where vulnerable consumers can be assisted to better engage with the CDR.</p> |

48 For example, see Consumer Experience Research Phase 3: Round 3, https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/05/CX-Report_-_Phase-3_-_Round-3.pdf

| | |
|--|---|
| Introducing a fiduciary obligation for data holders | <p>Submissions, including from the Financial Rights Legal Centre, Consumer Action Law Centre and the ACCC, recommended establishing a fiduciary duty for CDR participants (ADRs and data holders) to use data in the best interests of consumers. It is suggested that these duties can increase consumer confidence in the CDR system, in a similar way that these duties have been established in other realms where consumers are dependent on another party completing a service for them (such as doctors, lawyers and accountants). The Review notes that such a duty would likely increase the regulatory burden for CDR participants, however, submissions note this may be offset by increased trust from consumers and willingness to participate in the CDR.⁴⁹ As a general principle, the Review notes that the CDR framework should not seek to impose additional regulatory obligations outside of those that are required to successfully operate the system. Where other regulatory frameworks are better placed to address a potential harm or issue, they should be relied upon. It is not clear that the potential benefits of bringing in these obligations outweigh the additional regulatory burden on CDR participants.</p> |
| Joint accounts and consent rules | <p>The joint submission by the Australian Banking Association, Financial Rights Legal Centre, Consumer Action Law Centre and the Consumer Policy Research Centre also raised concern over the current opt-out model for joint accounts and noted they had previously recommended it be implemented as an opt-in model to ensure the safety of users. Their joint submission recommended the model should be reconsidered in the context of the rollout of payments initiation to allow time to evaluate the model and to determine whether sufficient protections are in place for consumers, particularly in relation to privacy, complaints handling and liability. The Review recognises the potential risks identified in submissions by the opt-out model and also sees the potential frictions an opt-in would present to the consumer. It is noted that the current model was subject to consultation and only recently implemented by major banks on 1 July 2022. It has yet to be implemented by non-major banks (compliance date 1 October 2022). At this point in time the Review finds an insufficient basis to reassess the model, and suggests time should be given to allow the system to mature and develop, before further considering a change.</p> |

49 See: Isabelle Guevara, *Digital fiduciaries and privacy protection in the digital age*, August 2021, https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2021/PrivacyEssayWinner2021#_edn24; cited in submission from Financial Rights Legal Centre.

| | |
|------------------|---|
| Safety-by-design | In their joint submission the Australian Banking Association, Financial Rights Legal Centre, Consumer Action Law Centre and the Consumer Policy Research Centre proposed the adoption of safety-by-design principles developed by the eSafety Commissioner to prevent products and services from being misused to cause detriment to customers or third parties. The Review notes that many participants support the current privacy and security settings and yet other participants find them to be overly complex. Further enhancements to protect consumers should be considered in this context and the system should be allowed to mature before adding further complexity. |
|------------------|---|

Recommendation 4.1

Further consideration should be given to other issues raised during the Statutory Review in the context of ongoing future legislative, rule-making and standard-setting updates to ensure that the CDR remains fit-for-purpose.

Glossary

| | |
|--|--|
| Accredited Data Recipient (ADR) | Accredited Data Recipient (ADR) under section 56AK of the <i>Competition and Consumer Act 2010</i> . An ADR can receive CDR data after being accredited by the Data Recipient Accreditor (the ACCC). |
| Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) | The <i>Anti-Money Laundering/Counter Terrorism Financing Act 2006</i> (AML/CTF Act), and the AML/CTF Rules aim to prevent money laundering and the financing of terrorism. |
| 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 <i>Competition and Consumer Act 2010</i> and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians. The ACCC is a co-regulator of the CDR with the OAIC. |
| Consumer Data Right (CDR) | Australia's data portability initiative. Allowing consumers to consent to disclosures of their data to third parties. |
| Consumer Data Right (CDR) agencies | CDR agencies are the ACCC, OAIC, DSB and the Treasury. |
| Consumer Data Right (CDR) consumer | The 'CDR consumer' is the person who has the right to access the CDR data held by a data holder, and direct that the CDR data be disclosed to them (not currently enabled) or to an accredited or trusted person. For the purposes of the CDR a 'person' can be an individual or a business. |
| Consumer Data Right (CDR) data | Information within a class specified in a CDR designation instrument, or information wholly or partly derived from such information. |
| CDR Rules | The <i>Competition and Consumer (Consumer Data Right) Rules 2020</i> (the CDR rules) provides the framework for how the CDR it is to be implemented and operated. |
| Consent | Communication to an accredited person of the datasets 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. |
| CX | Consumer Experience |
| Data Availability and Transparency Act 2022 (DATA 2022) | The <i>Data Availability and Transparency Act 2022</i> (DATA 2022) enables sharing for the delivery of government services; informing government policy and programs; and research and development. |

| | |
|---|---|
| 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 / Datasets | Data is information translated into a form for efficient storage, transport or processing, and is increasingly synonymous with digital information. It includes product data (data related to the product/service advertised for example: descriptions, prices, terms, and conditions) and consumer data (data related to the consumer of the product/service for example: consumer contact details, or information relevant to their eligibility for a service). |
| Data portability | The ability to move data from one place to another. |
| 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 making data standards for the CDR, supported by the DSB. |
| Derived data | Under Section 56AI(2) of the <i>Competition and Consumer Act 2010</i> . ‘Derived CDR data’ is data that has been wholly or partly derived from CDR data, or data derived from previously derived data. This means data derived from ‘derived CDR data’ is also ‘derived CDR data’. |
| Designation | The designation instrument enlivens the Rule making power by designating a sector of the economy as a sector to which the CDR applies. |
| 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. |
| New Payments Platform (NPP) | Australia’s real-time payments infrastructure, introduced in 2018, which allows consumers and businesses to make and receive fast payments which are secure and data-rich. |
| Office of the Australian Information Commissioner (OAIC) | The independent national regulator for privacy and freedom of information. The OAIC is a co-regulator of the CDR with the ACCC. |
| Open Banking | The CDR based system giving customers access to and control over their banking data and data on banks’ products and services. |

| | |
|--|---|
| 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 in order to assist the accredited person to provide goods and services to CDR consumers. |
| PayTo | PayTo is a new, digital way for merchants and businesses to initiate real-time payments from their customers' bank accounts. |
| Participant | CDR participants include ADRs, Data Holders, Representatives, Affiliates, Trusted Advisers. |
| <i>Privacy Act 1998</i> | 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. |
| 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. |
| Standard/s | The technical and consumer experience data standards made by the Data Standards Chair for the purpose of the Consumer Data Right to inform participants on how to comply with the rules. |
| Strategic Assessment | A three-month assessment to inform an economy-wide Consumer Data Right, as announced as part of the former Government's Digital Economy Strategy announced in the 2021-22 Budget. |
| Trusted Adviser | A person who can be nominated by a consumer and with consent receive that consumer's data from an ADR. Trusted advisers must belong to one of the specified professions listed in CDR Rule 1.10C(2). For example, accountants, registered tax agents, BAS agents. |
| Unique identifiers | A unique identifier is an identifier that marks that particular record as unique from every other record. |
| Use case | Where a particular dataset has a current and demonstrable application to the provision of a product or service. |
| Vertical and horizontal integration | Vertical integration is the capacity for innovators to engage consumer within their industry. Horizontal integration is the connectedness between sectors particularly such that cross-sectoral use cases are enabled. |

Appendix A – Context of the Review

Background to the Review

This Review was undertaken in the context of significant policy and governance developments in the CDR. This includes the roll out of the CDR to the banking sector, the introduction of rules to bring the energy sector into the CDR from late 2022, and the finalisation of the sectoral assessment and designation process for the telecommunications sector. The practical application of the CDR initiative to these three sectors provides a good opportunity to reflect on the efficacy of the statutory framework as the CDR grows.

The CDR is a multi-year, complex initiative that will continue to grow and evolve over the next decade. As such the Review will need to consider the policy, governance and any other relevant recent developments in the CDR in responding to the Terms of Reference, including:

- The former Government’s response⁵⁰ to the final report⁵¹ of the Future Directions Inquiry, which provides options to expand and enhance the functionality of the CDR.
- The release of the former Government’s Digital Economy Strategy⁵² (announced as part of the 2021-22 Budget), which sets out a roadmap of initiatives to ensure Australia is a world-leading Digital Economy by 2030 – including the Australian Data Strategy,⁵³ and the expansion of the Digital Identity System.
- The CDR Strategic Assessment to inform the future expansion of the CDR, with a relevant consultation paper released by Treasury in July 2021.⁵⁴
- Updates to CDR rules to support greater participation within the CDR ecosystem.
- International developments in consumer-initiated data portability.

50 The Government response to the *Inquiry into Future Directions for the Consumer Data Right*, December 2021, <https://treasury.gov.au/publication/p2021-225462>

51 The final report of the *Inquiry into Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

52 Further content concerning the *Digital Economy Strategy* can be found here: <https://digitaleconomy.pmc.gov.au/>

53 Further content concerning the *Australian Data Strategy* can be found here: <https://ausdatastrategy.pmc.gov.au/>

54 The consultation paper and *Strategic Assessment Outcomes* report can be found here: <https://treasury.gov.au/publication/p2022-242997>

Terms of Reference

- Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?
- Do the existing assessment, designation, rule-making and standard-setting requirements of the CDR framework support future implementation of the CDR, including to government-held datasets?
- Does the current operation of the statutory settings enable the development of CDR-powered products and services to benefit consumers?
- Could the CDR statutory framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?
- Are further statutory changes required to support the policy aims of CDR and the delivery of its functions?

Objects of 56AA of the Act

The object of this Part is:

- a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently
 - i) to themselves for use as they see fit; or
 - ii) to accredited persons for use subject to privacy safeguards; and
- b) to enable any person to efficiently and conveniently access information in those sectors that:
 - i) is about goods (such as products) or services; and
 - ii) does not relate to any identifiable, or reasonably identifiable, consumers; and
 - iii) as a result of paragraphs (a) and (b), to create more choice and competition, or to otherwise promote the public interest.

CDR rules discussed in the review

- 4.9 Object – The object of this Division is to ensure that a consent given by a CDR consumer to collect and use CDR data is:
- a) voluntary; and
 - b) express; and
 - c) informed; and
 - d) specific as to purpose; and
 - e) time limited; and
 - f) easily withdrawn.

4.10 Requirements relating to accredited person's processes for seeking consent

An accredited person's processes for asking a CDR consumer to give consent:

a) must:

- i) accord with the data standards; and
- ii) having regard to any consumer experience guidelines developed by the Data Standards Body, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids; and

b) must not:

- i) include or refer to other documents so as to reduce comprehensibility; or
- ii) bundle consents with other directions, permissions, consents or agreements.

4.11 Asking CDR consumer to give consent to collect and use CDR data

a) ask for the CDR consumer's express consent:

- i) for the accredited person to collect those types of CDR data over that period of time; and
- ii) for those uses of the collected CDR data; and
- iii) to any direct marketing the accredited person intends to undertake;

4.13 Withdrawal of consent to collect and use CDR data and notification

(1) The CDR consumer who gave a consent to collect and use particular CDR data may withdraw the consent at any time:

- a) by communicating the withdrawal to the accredited person in writing; or
- b) by using the accredited person's consumer dashboard.

4.22 Requirements relating to data holder's processes for seeking authorisation

A data holder's processes for asking a CDR consumer to give an authorisation must:

- a) accord with the data standards; and
- b) having regard to any consumer experience guidelines developed by the Data Standards Body, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids.

4.25 Withdrawal of authorisation to disclose CDR data and notification

(1) The CDR consumer who gave, to a data holder, an authorisation to disclose particular CDR data to an accredited person may withdraw the authorisation at any time:

- a) by communicating the withdrawal to the data holder in writing; or
- b) by using the data holder's consumer dashboard.

Appendix B – List of Submissions

The Review received 44 written submissions. The organisations and individuals that made public submissions are included in Table B.1.

Table B.1 – Public Submissions

| Organisations and individuals |
|---|
| Australian Banking Association |
| Australian Banking Association, Consumer Action Law Centre, Consumer Policy Research Centre, Financial Rights Legal Centre (joint submission) |
| Australian Communications Consumer Action Network (ACCAN) |
| Australian Competition & Consumer Commission |
| Australian Energy Council |
| Australian Payments Network |
| Australian Retail Credit Association |
| Australian Small Business and Family Enterprise Ombudsman |
| Basiq |
| Business Council of Australia |
| Mr Bikalpa Rajbhandari and Associate Professor Mark Burden |
| Chartered Accountants ANZ, CPA Australia & Institute of Public Accountants Australia |
| Communications Alliance Ltd |
| Commonwealth Bank of Australia |
| Customer Owned Banking Association |
| Consumer Action Law Centre |
| Consumer Policy Research Centre |
| Cuscal |
| Digital Service Providers Australia New Zealand |
| Dr Zofia Bednarz, Mr Chris Dolman FIAA, and Prof Kimberlee Weatherall |

| |
|---|
| EML Payments Ltd (EML) |
| EnergyAustralia |
| Energy Queensland |
| Envestnet Yodlee |
| Ernst & Young (EY) |
| Financial Data and Technology Association (FDATA) |
| Financial Rights Legal Centre |
| Finder |
| illion |
| Internet Association of Australia |
| Intuit |
| National Australia Bank |
| Office of the Australian Information Commissioner |
| Origin Energy |
| Mr James Mackie |
| PEXA |
| Public Interest Advocacy Centre |
| Red Energy and Lumo Energy |
| Scientia Professor Ross P Buckley & Dr. Natalia Jevglevskaja, University of New South Wales |
| Tech Council of Australia |
| Telstra |
| TrueLayer |
| Verifier |
| Xero |

Appendix C – Overview of the Consumer Data Right

The Consumer Data Right (CDR) is Australia's national data portability initiative. It is a significant, economy-wide reform designed to empower consumers to benefit from the data Australian businesses hold about them and in doing so strengthen innovation, competition and productivity. The CDR was conceived of as a right by the Productivity Commission in March 2017,⁵⁵ based on the benefits it could provide to consumers and businesses and its potential to enhance competition. The Productivity Commission identified that creating a right of this kind would fundamentally reform Australia's competition policy in a digital world.

In July 2017, the *Review into Open Banking* was commissioned to recommend the most appropriate model for an Open Banking initiative in Australia. Giving regard to the earlier work of the Productivity Commission, the final report of this review positioned Open Banking as a component of a more general right for consumers to control their data in Australia – the CDR. The final report of the *Review into Open Banking* set out four key principles, which have guided the implementation of the CDR in Australia.⁵⁶ These are that the CDR should:

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

55 Refer: *Data Availability and Use – Productivity Commission Inquiry Report*, No. 82, March 2017, <https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf>

56 Final report of the *Review into Open Banking*, <https://treasury.gov.au/consultation/c2018-t247313>

CDR statutory framework

The CDR statutory framework originated with the Treasury Laws Amendment (Consumer Data Right) Bill 2019, which received Royal Assent in August 2019. The statutory framework comprises four components:

- Part IVD of the *Competition and Consumer Act 2010* (the Act), which contains the primary CDR legislation, and establishes all other components of the legislative framework,
- CDR Designation Instruments made by the Minister pursuant to Part IVD of the Act, which designate sectors of the Australian economy for the purposes of the CDR,
- the Consumer Data Right rules (the rules) made by the Minister responsible for the CDR. Among other things, the rules set out the circumstances in which data holders are required to disclose data, and to whom, in response to a valid consumer request. They also set out consent requirements, how data may be used and privacy safeguards.
- the Consumer Data Standards (the standards), which set the technical requirements by which data needs to be provided to consumers and accredited data recipients (ADRs) within the CDR system – ensuring safe, efficient, convenient, and interoperable systems to share data are implemented. Where the rules require compliance with the standards, a breach of the standards may constitute a breach of the rules, and standards have a contractual effect between data holders and recipients in certain instances.

Oversight of the CDR

The Minister

The Assistant Treasurer is the responsible Minister and sets the overall strategic direction and expectations for the CDR program. The Minister is directly advised by the Treasury who leads CDR policy, including the development of rules and on which sectors the CDR should apply to in the future.

The CDR Agencies

The Treasury leads CDR policy, including development of rules and advice to Government on which sectors the CDR should apply to in the future.

Treasury works closely with the Australian Competition and Consumer Commission (ACCC), which is responsible for the accreditation process, including managing the Consumer Data Right Register, and ensures providers are complying with the rules and takes enforcement action where necessary; and the Office of the Australian Information Commission (OAIC), which regulates privacy and confidentiality under the CDR, enforces the privacy safeguards and privacy-related CDR rules where necessary, handles complaints and notifications of eligible data breaches relating to CDR data. The Data Standards Body develops the technical and consumer experience standards, which are made by the Data Standards Chair.

CDR Board

The Consumer Data Right Board (the Board) was established under the authority of the Secretary of the Treasury in February 2020. It provides senior leadership and strategic oversight by CDR agencies to deliver a complex, multi-year and multi-function policy, regulatory and ICT program. The Board is advisory in nature and not intended to supersede or otherwise interfere with the roles and responsibilities, or independence of any agency or individual member. Decision making is undertaken by a consensus of its Members who consist of the following:

- Deputy Secretary, Markets Group, Treasury (Chair)
- Commissioner, ACCC
- Data Standards Chair
- Australian Information Commissioner and Privacy Commissioner, OAIC

Evolution of governance

These responsibilities evolved with the rollout of the CDR. In the 2017 Productivity Commission Report *Data Availability and Use* it was suggested that the proposed data sharing framework should be established with the ACCC responsible for regulatory work including handling complaints from data holders, educating consumers, and assessing applications to participate in data sharing.

The Open Banking Review chaired by Mr Scott Farrell was published in 2018. This Review included several recommendations regarding governance of Open Banking, including that the initiative be supported by a multiple regulator model where the ACCC be responsible for competition and consumer issues and standards-setting, while the OAIC be responsible for privacy protection. The Review also recommended a Data Standards Body work with the regulators to develop standards. The Government at the time accepted these recommendations.⁵⁷

With the launch of Open Banking under the CDR in 2019, the multiple regulator model was adopted with the ACCC responsible for compliance, enforcement and accreditation as well as establishing the rules for participation in the CDR framework. The OAIC was responsible for enforcing the privacy safeguards and privacy-related CDR rules where necessary, handling complaints and notifications of eligible data breaches relating to CDR data, for investigating privacy breaches, and providing advice to the Minister and CDR agencies on the privacy implications of the CDR rules and data standards. During this time Treasury provided guidance on policy implementation for the CDR. The Data Standards Body was part of the Commonwealth Scientific and Industrial Research Organisation (CSIRO).

From 28 February 2021, the then responsible Minister for the CDR, Senator the Hon Jane Hume took over from the ACCC as CDR rule-maker. This change meant that accountability for development and advice on the rules, and for assessing future sectors, moved from the ACCC to Treasury, along with overarching leadership and responsibility for the CDR program. The functional reallocation also included the transfer of the Data Standards Body (DSB) from CSIRO to Treasury. These changes were intended to support a streamlined and unified approach to the development and implementation of CDR policy, rules and standards.

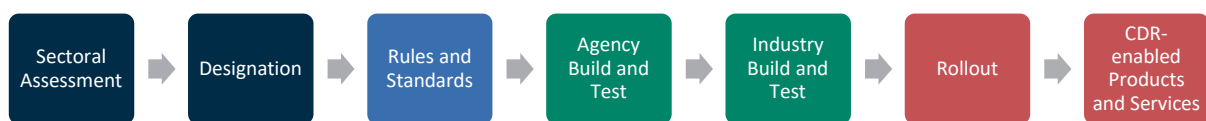
⁵⁷ See Recommendations 2.2, 2.4, 2.6, 2.7, and 2.9 of the final report of the *Inquiry into the Future Directions for the Consumer Data Right*, December 2020, <https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report>

The ACCC retains responsibility for accreditation of data recipients, registration and on-boarding of data holders and data recipients, compliance and enforcement (together with the OAIC), for designing, developing and running the Register & Accreditation Application Platform (RAAP) that supports secure sharing of data between participants, and for the Conformance Test Suite for participants.

Sectoral assessment and designation processes

The CDR statutory framework includes requirements related to the expansion of the CDR through a sectoral assessment and designation process, as well as how the CDR is designed through rules and standards to support engagement that evolves with technological developments.

Figure C.1: Summary of CDR sector implementation steps



Designation process

The Act provides that before a dataset or sector can be included in the CDR system, a detailed assessment must be undertaken for the sector or dataset designated by a legislative instrument made by the Minister.

The Minister may designate a sector of the Australian economy to be subject to the CDR under section 56AC of the Act. A sector is designated by legislative instrument, which specifies the classes of information (data) designated for the purposes of the CDR and the class or classes of persons who hold the designated information (data holders).

The Act provides that, before a sector can be designated, certain matters under section 56AD(1) (collectively, the statutory factors) must be considered by the Minister. These include:

Figure C.2: Sectoral assessment criteria

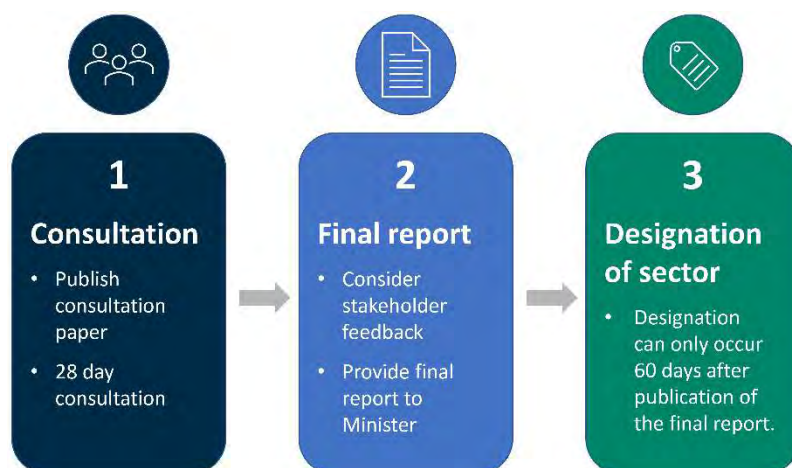


The Act also requires that, before designating a sector, the Minister must be satisfied that the Secretary of the Department (the Treasury) has arranged for consultation and analysis about designation and published a report about that analysis and consultation. As part of its consultation, the Treasury is required to consult the ACCC, the Information Commissioner, and the primary regulator of the relevant sector (section 56AE(1)(c)). Making a designation instrument cannot occur until 60 days after the publication of the report. Before making a designation instrument, the Minister must also consult the Information Commissioner about the likely effect of the instrument on the privacy and confidentiality of consumers' information (section 56AD(3)).

The sectoral assessment considers the type of data that should be designated (it may include datasets used in other sectors) and who holds the data in the sector, to inform which data holders and what data should be designated and shared in a secure way, upon a consumer's request.

A final report on the sectoral assessment, incorporating stakeholder feedback, will inform the decision about whether to designate a particular sector and any datasets and entities to be designated.

Figure C.3: Sectoral assessment process



A designation instrument specifies the parameters for classes of information that may be shared under the CDR in a particular sector, as well as who is required to share it. Once a sector has been designated, CDR rules and standards for that sector can be made in accordance with statutory processes, including extensive consultation requirements.

Designation involves specifying 'classes of information' or data to be designated but designating a sector does not in itself impose substantive obligations. Rather, the requirement to disclose particular data emanates from the CDR rules, which establish what is 'required' CDR data that must be shared in response to a valid request, as well as what information data holders, accredited data recipients and representatives are 'authorised' to share on a voluntary basis.

Rules and standards

The rules have been developed to apply universally across sectors to the extent possible, however, sector-specific provisions and modifications are catered for in sector-specific schedules, and will be iteratively updated as the CDR evolves and expands. Once designation of a sector occurs, sector-specific issues (for example, external dispute resolution arrangements specific to that sector) are considered, as well as the development of sector-specific data standards. The rules are made under the Act and set out the framework to facilitate data sharing.

The rules mandate how data holders disclose consumer and product data to consumers, and how data holders disclose consumer data on behalf of consumers and product data to accredited data recipients on behalf of the consumer. The first version of the rules was published in February 2020 and since then there have been several iterations of the rules.

The standards provide guidance to participants in the CDR on technical and consumer experience. Non-compliance with standards may constitute a breach of the rules where the rules require compliance with the standards. The Data Standards Body provides frequent updates to the standards in consultation with stakeholders.

CDR roll-out to date

Banking

The CDR was first implemented in the banking sector launching on 1 July 2020, where it is known as Open Banking. The majority of Australian banking consumers are now able to access the CDR to securely and conveniently share their banking data to access better-value products and services tailored to their individual circumstances.

As of 26 July 2022, 114 data holder brands are now live in the CDR system, with 76 designated data holders and an additional 38 brands. The number of ADRs has also been steadily growing, with 32 ADRs, 20 of which are active. This represents a market share of more than 99 per cent of Australian household deposits being covered by CDR data-sharing. As of 7 July 2022, there are also 3 ADRs who are principals for 31 representatives. ADRs are already and expected to use CDR data to provide services to consumers, such as budgeting, bill payment and financial management apps, streamlined credit approval processes, and the creation of in-depth financial overviews to assist consumers on their home-buying journey.

Energy

The expansion of the CDR to the energy sector is well advanced. On 12 November 2021, the Hon Jane Hume, the then Minister for Superannuation, Financial Services, and the Digital Economy, made energy-specific CDR rules that include phased compliance dates. Introducing the CDR in the energy sector will provide Australian households and businesses with more accurate information about their energy use and plans.

Commencing in November 2022, energy consumers will start to benefit from secure and easy sharing of data about their own energy use and connection. For example, this could include supporting informed decisions and greater insights on consumers' energy usage and expenditure to identify better value products and service offerings.

Telecommunications

In January 2022, the telecommunications sector was designated as the third CDR sector, following banking and energy. Introducing the CDR into the telecommunications sector will enable information about telecommunications product and consumer data to be shared in a safe and efficient manner. Consumers will be empowered to access better-value and personalised products and services, such as more accurate information about their internet consumption, phone usage and product plans so they can more easily compare and switch between providers.

The rollout of the CDR in the telecommunications sector is expected to create many benefits for consumers, including better product comparison, tailored product recommendations, and services that help consumers save time and money in accessing telecommunications related products, as well as supporting more informed financial decision making when telecommunications datasets are combined with other CDR data.

Recent developments and future directions

A more consumer-centric and agile approach to economy-wide expansion

In the second half of 2021, to inform the prioritisation and sequencing of future expansion of the CDR, Treasury undertook a rapid, whole of economy strategic assessment. The process involved significant domestic and international consultation and provided significant insights into the broad scope of potential CDR use cases and consumer outcomes. The findings from this process were made publicly available in the *Strategic Assessment Outcomes* report that was published on 24 January 2022 and informed the former Government's announcement of 'Open Finance' as the next priority area for expansion.

Strategic Assessment Report: key factors to support prioritise and sequence CDR expansion

Prioritise datasets that build on existing dataset(s) or are highly complementary to support faster ecosystem growth.

Prioritise datasets that support multiple use cases, broad innovation, and user journeys rather than simple switching use cases.

Focus on friction points for consumers that can be addressed through data driven innovation and standardisation.

Consider how the CDR might interact with any existing data sharing mechanisms already operating in a sector.

Consider maturity of ICT infrastructure and digital capability of sector, as well as the proprietary nature of datasets.

Open Finance

Open Finance expansion will see the CDR expand in an agile and use case focussed approach – bringing datasets from across general insurance, superannuation, merchant acquiring and non-bank lending service providers into the CDR.

The announcement of Open Finance followed the completion of the CDR Strategic Assessment, which found there were clear and immediate benefits in expanding the CDR to Open Finance by building upon data already contemplated to be shared under the framework. Open Finance will also support multiple use cases beyond provider switching, alleviate friction points for consumers through data driven innovation and standardisation, and potentially enhance existing data sharing practices in the related sectors.

Consultation also highlighted that unlocking public sector data, with consumer consent, could drive private sector innovation and improve how consumers can more seamlessly use data services across the public and private sectors.

Treasury consulted on expansion to non-bank lending services from 15 March to 15 April 2022. By expanding the CDR through Open Finance, consumers will be empowered to make the best financial judgments for their needs when choosing a superannuation strategy, general insurance product or credit provider.

Future Directions for the CDR

The *Inquiry into Future Directions for the Consumer Data Right* final report, released in December 2020, made 100 recommendations to expand the CDR by enabling greater consumer data empowerment and deeper functionality such as implementing third party action and payment initiation, an economy-wide foundation, a more integrated data ecosystem, and realising international digital opportunities.

Payment and action initiation will particularly be a game-changer for the CDR, and it is expected to drive greater participation and innovation in the scheme. These developments will require legislative amendments and will be the subject of a separate process of consultation to inform the Bill. Relevant findings from the CDR Statutory Review will also inform the design of the legislation.

Data Standards Body August 2022 Update

Table of Contents

| | | |
|-----|---|---|
| 1 | Working Group Update..... | 1 |
| 1.1 | Technical Working Group Update | 1 |
| 1.2 | Consumer Experience (CX) Working Group Update | 1 |
| 2 | Stakeholder Engagement..... | 4 |
| 2.1 | CDR Implementation Calls..... | 4 |
| 2.2 | Maintenance Iteration..... | 5 |
| 2.3 | CDR Support Portal..... | 5 |
| 2.4 | DSB Video Channel | 6 |
| 2.5 | DSB LinkedIn | 6 |
| 2.6 | DSB Newsletter..... | 6 |
| 2.7 | Workshops..... | 7 |
| 2.8 | Service Provider Directory..... | 7 |

1 Working Group Update

1.1 Technical Working Group Update

The technical working has had a big month in July. The key highlights of the work undertaken is as follows:

- Maintenance Iteration 11 has completed with the final decisions approved. This iteration was very large and addressed 38 distinct change requests as well as a number of minor documentation updates. The team is very appreciative of the work done by Hemang Rathod to lead the iteration.
- Following the completion of MI 11, version 1.18.0 of the Standards were published on the 11 August 2022.
- Maintenance Iteration 12 is underway and is in the backlog grooming phase. The intent is for this iteration to be much smaller in scope and size due to the upcoming implementation dates in both the banking and energy sector. The intent is that the changes included in Maintenance Iteration 12 will not be required to be implemented until well after the November implementation dates.
- The independent information security review report was completed and published. Work has progressed on the DSB response and is intended to be published shortly.
- Another Decision Proposal for the Telco sector has been published with the first two material consultations being completed. A meeting was also held with the Telco industry participants facilitated by Comms Alliance. Discussions are underway to establish regular meetings as was done previously with the ABA and AEC. Currently we are on track to have candidate standards published during November.
- Significant work went into resolving the issues surrounding the publishing of PRD for the energy sector. It is understood that this issue is now resolved for the time being.
- Work on the test documentation is ongoing with additional test cases being published on a regular basis.
- In addition, the team has been supporting the Treasury in assessing new sectors, action initiation, the development of v5 of the rules and rules for the Telco sector

1.2 Consumer Experience (CX) Working Group Update

Since the last update in July, the Consumer Experience (CX) Working Group has continued to engage with the community, progress the development of CX standards and guidelines, and has worked closely with Treasury, OAIC, and ACCC on CX developments and guidance related to the rules and incoming sectors.

1.2.1 Customer data language standards

To conclude Maintenance Iteration 11 (MI11), the Data Standards Chair approved changes to the CX data language standards to treat customer data as sector-agnostic. These changes were incorporated into the v1.18.0 release. It will not alter any banking obligations but will require energy DHs to adopt language standards that are consistent with the language currently used in banking.

This change will make the customer data language sector agnostic, and as such will relate to the banking and energy sectors as well as future sectors, beginning with telco.

MI11 highlighted issues with the existing energy data language standards that will be consulted on as part of MI12. Change Request 529 ([CR529](#)) has been published for this consultation, which proposes that incorrect references to 'NMI' be removed, and the language for the payment schedule cluster be amended to more accurately reflect the data that will be accessible. The DSB welcomes views on these changes and if they need to be proposed as a future dated obligation or can take effect in November for energy DHs.

1.2.2 Telecommunications

Decision Proposal 267 (DP267) will consult on data language standards specific to the telco sector. This consultation will define standards for the telco sector and will be subject to further rules and technical standards refinement.

This consultation is intended to be conducted in two rounds. The incoming decision proposal (DP) will initiate the first round, which will run for 28 days. The second consultation will initiate the finalisation of the data language standards, which is expected to be run soon after the conclusion of the first round.

The CX working group is planning CX research to test comprehension of the proposed data language standards, which will inform the development of the descriptions to be used.

1.2.3 Decision Proposal 229

A path has been assessed for [DP229](#), which will consult on appropriate and consistent ways to represent various CDR participants in the CDR ecosystem, particularly in DH authorisation flows and dashboards. The paper is expected to include:

- A recommendation for ADRs to onboard a unique brand (and brandName) and software product (and softwareProductName) per client, such as an CDR Rep, Affiliate, or subsidiary etc.
- A proposal for DHs to display the brandName in the authorisation flow, in addition to the legalEntityName as required by the rules.
- A proposal for DHs to display the brandName, softwareProductName, and legalEntityName in DH dashboards
- Consideration for additional fields to pass metadata to facilitate authorisation management, particularly where concurrent consents are established using a single software product

1.2.4 Accessibility Analysis

The first [accessibility analysis](#) report from DSB's work with [PwC's Indigenous Consulting](#) (PIC) and the [Centre for Inclusive Design](#) was published in the [CX Reports section on accessibility](#). The coded prototype tested in accessibility research has been made available in a new [Open Source Assets](#) section of the CX Guidelines.

The findings of this research, further CX and accessibility analysis, and a complete list of recommendations will be made public in an accessibility improvement plan. The recommendations from this research are expected to trigger a review of the accessibility standards and artefacts, as well as propose increased DSB capability. The DSB will provide a public

response to this report and consult on these recommendations as part of ongoing standards and artefact development.

1.2.5 Authentication

Research on the [CX of Authentication](#) is underway to facilitate uplift and evolution. As suggested at the previous advisory committee, a related Noting Paper is being developed to share our approach with the community, as well as CX metrics we are using to assess a range of authentication approaches, which will ultimately inform standards development.

1.2.6 CX Artefact Development

The CX working group continues to iteratively develop and release CX artefacts to facilitate CDR implementation in response to an evolving ecosystem and community requests. In July, this included a new [CX Checklist](#) was published to reflect v1.17.0 changes, which is available as downloadable xlsx and csv files.

For more details, refer to the [change log](#).

1.2.7 Forward View

As noted in the [DSB's quarterly plan](#), a range of other activities are planned for the CX Working Group. The CX Working Group is also conducting internal work relating to new sectors, new rules, reviews of existing requirements, and future developments such as action initiation and recommendations from the Future Directions inquiry.

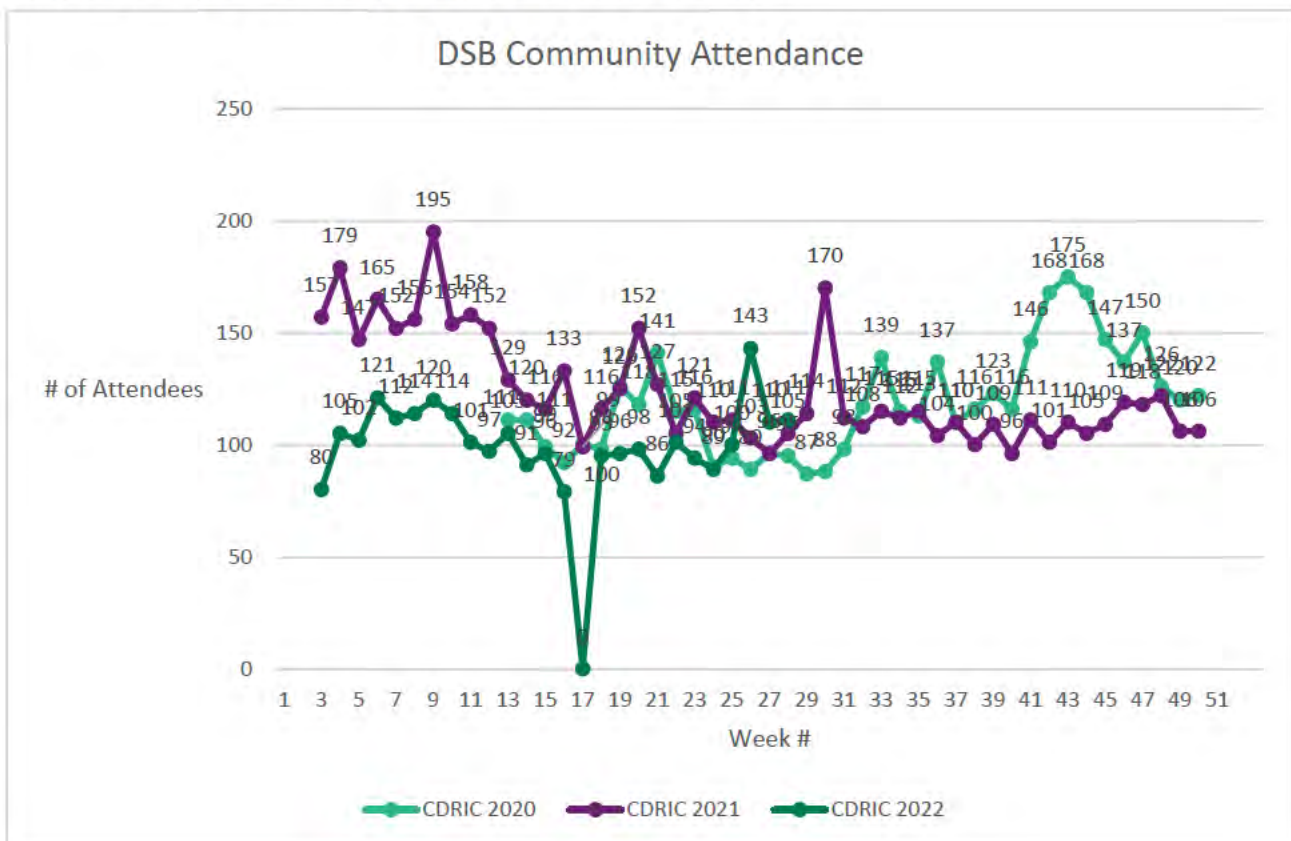
2 Stakeholder Engagement

Stakeholder engagement remains strong with the DSB conducting regular CDR Implementation calls, Maintenance Iteration cycle meetings and circulation of newsletters over the last month. A summary is provided below.

2.1 CDR Implementation Calls

The DSB & ACCC co-facilitate the CDR Implementation calls which are held weekly. The purpose of these calls is to provide a forum that is accessible to all and offers CDR participants undertaking implementation activities, a way to raise questions for clarification whilst getting access to important updates on the CDR and standards changes. These meetings offer an opportunity for data holders and their providers to better understand how to interpret and implement the rules, CX and standards.

Provided below is a summary of attendees at the meetings.



Provided below are details of the weekly meeting, including connection details.

| MEETING | DSB & ACCC WEEKLY CONSUMER DATA RIGHT IMPLEMENTATION CALL |
|--------------------|---|
| DATE TIMING: | Every Thursday 15:00 – 16:30 |
| LOCATION | Online via WebEx |
| CONNECTION DETAILS | Please click here for connection details |

2.2 Maintenance Iteration

The CDS Maintenance Iteration (MI) is an 8 week cycle where new change requests are prioritised in consultation with the community to form the implementation backlog recommended to the DSB Chair for the next release cycle. The changes resulting to the specification are made after review and input from the community. You can find more information on the process and stages of the Maintenance Iterations [here](#) or in the short introduction video [here](#).

Maintenance Iteration # 12 commenced on 20 July 2022 and is due to complete in mid-September.

Provided below is a summary of attendees at recent meetings.

| MEETING | DATE | ATTENDEES |
|--|---------------|-----------|
| MI # 12: Kick-off and backlog review and MII retro | 20 July 2022 | 35 |
| MI # 12: Consultation | 3 August 2022 | 32 |

If you would like to participate in the Maintenance meetings and contribute to the discussion, send a request via email to contact@consumerdatastandards.gov.au.

2.3 CDR Support Portal

The CDR Support Portal continues to grow with over 84 live knowledge articles, guides and FAQs published, 2000 unique users over the last month and 600 over the last week. The Portal can be viewed [here](#).

We have a number of knowledge articles that have been recently added or changed in the Portal over the last 7 days. They are:

- [Secondary user instruction and vulnerability implications for Joint Accounts](#)
- [Expiry of Access Token for expired consent](#)
- [Clarification on transaction times](#)
- [CORS support with access-control-expose-headers](#)
- [Internal routing and sharing international payee data](#)
- [OTP and international phone numbers](#)
- [Data unavailable for BankingTransactionDetail fields](#)
- [Handling transaction details extendedData when NPP not supported](#)

We also list below our most viewed articles since the last committee meeting:

- [Calculating Average TPS and Peak TPS metrics](#)
- [CTS Guidance Materials](#)
- [Conformance Test Suite: version history and scenarios](#)
- [Guidance for data holders – assessing whether a product is in scope for CDR](#)
- [Brands in the Consumer Data Right Ecosystem](#)
- [Guidance for Profile Scope and Standard Claims](#)
- [Vulnerable customers](#)
- [Secondary users and Closed accounts](#)
- [Revised joint account implementation guidance](#)

2.4 DSB Video Channel

The DSB have recently published the following documentation in video form to further support the Consumer Data Right community:

- [Decision Proposal 257 – narrated by Neale Morison \(8/7/22\)](#)
- [Decision Proposal 256 – narrated by Neale Morison \(6/7/22\)](#)
- [Decision Proposal 255 Executive Summary – narrated by Neale Morison \(17/6/22\)](#)

You can view the video channel [here](#).

2.5 DSB LinkedIn

The DSB have recently added the following posts to their DSB LinkedIn account:

- Come to #DSB Video Channel for the drama, the romance, the excitement of the #ConsumerDataStandards.
- Tapped out trying to test your #CDR implementation, Faucet to behave. Tap into our development resources, and go with the flow
- Have you missed one of our newsletters? Here is a link to the repository of #DSB newsletter and blog posts published since 2019.

You can view the LinkedIn account [here](#).

2.6 DSB Newsletter

The DSB circulates a weekly newsletter that includes a collection of DSB and Consumer Data Standards tools, platforms, publications, and knowledge bases. We currently have over 1220 subscribers. A summary of our performance over the last months is:

| EMAILS SENT | OPEN RATE | CLICK RATE | UNSUBSCRIBE RATE |
|-------------|-----------|------------|------------------|
| 5163 | 25.1% | 1.5% | 0.1% |

To subscribe to the weekly DSB newsletter please click [here](#).

2.7 Workshops

We are currently in the planning stages for future workshops. Our future events can be found on the Consumer Data Standards website [here](#).

2.7.1 Recent Workshops

Since the last committee meeting, we have held a workshop on Historical Data Sharing for the Energy Sector. Below are further details:

| WORKSHOP | HOSTED BY | DATE | ATTENDEES |
|---|-----------|--------------|-----------|
| Energy Sector: Historical Data Sharing Workshop | DSB | 27 July 2022 | 60 |

2.8 Service Provider Directory

The Service Provider (SP) Directory provides a free-browsable catalogue of CDR solutions available in the market. The list is not exhaustive and the DSB do not endorse or certify the SP's. The Directory can be found [here](#).

The following entities are listed in the Directory:

| COMPANY | BUSINESS SERVICE PROVIDERS | TECHNICAL SERVICE PROVIDERS | IDENTITY, ACCESS & CONSENT MNG PROVIDERS | TESTING, DEV SUPPORT & DEPLOY TOOLS |
|---|----------------------------|-----------------------------|--|-------------------------------------|
| Adatree | | ✓ | ✓ | |
| AssuranceLab | ✓ | | | |
| Basiq | ✓ | | | |
| Biza.io | | ✓ | ✓ | |
| Fintech Solutions Services (Global) Pty Ltd | | | | |
| Frollo | ✓ | ✓ | ✓ | ✓ |
| Greater Than X | | | | |
| Innovo Technology Solutions | | ✓ | | |
| MinterEllison | ✓ | | | |
| Mountain Pass Pty Ltd | | ✓ | | |
| ProductCloud | | ✓ | | |
| Quill Peak Consulting | ✓ | | | |
| Regional Australia Bank | | | | ✓ |
| RSM | ✓ | | | |
| Tic Toc Enterprises | | ✓ | | |

For Noting

FOR FURTHER INFORMATION

Andrew Stevens

Data Standards Chair

e andrew.stevens@iisa.gov.au

w www.consumerdatastandards.gov.au

Barry Thomas

Data Standards Body General Manager

e barry.thomas@consumerdatastandards.gov.au

w www.consumerdatastandards.gov.au

CONSUMER DATA RIGHT BOARD: 23 August 2022

AGENDA ITEM 4.1

Accessibility Review update

Lead: Andrew Stevens, Data Standards Chair

Recommendations

That the CDR Board:

1. **Note** the ongoing work by the DSB, in support of the Data Standards Chair, to ensure Data Standards development reflects their legal obligations for Accessibility;
2. **Note** the legal obligations identified in the Accessibility Obligations and Conventions Framework for the Data Standards Chair; including those for Accessibility, Usability and Inclusion;
3. **Note** that these legal obligations are universal and relevant beyond the Data Standards and the remit of the Data Standards Chair.

Background

The consumer experience (CX) Data Standards and related artefacts outline accessibility requirements and guidance for CDR participants, which include references to external accessibility standards such as the Web Content Accessibility Guidelines (WCAG).

Accessibility requirements and conventions are constantly evolving. Therefore, periodic reviews of the data standards and CX artefacts are necessary to maintain their alignment with external standards such as WCAG. An Accessibility Review began in May 2022 for this purpose, as well as to identify relevant future directions and developments for accessibility, usability, and inclusivity.

PWC's Indigenous Consulting and the Centre for Inclusive Design were engaged as suppliers to carry out this work and provide the Data Standards Chair with insights relating to accessibility obligations and conventions. The activities and outputs of the review included a Background Report, Consumer Testing, and an Accessibility Improvement Plan.

The Background Report has now been published.¹ The Accessibility Improvement Plan is currently being finalised as the last output of the review, which will include the results of Consumer Testing and an extended list of recommendations covering obligations, opportunities, and considerations for the data standards and CX artefacts. Upon completion, the Data Standards Body (DSB) will publish a response to the Accessibility Improvement Plan, which will initiate public consultation on the scope and appropriateness of the proposals.

Key Issues

The Background Report identifies key obligations and conventions relating to accessibility, which emanate from:

- The Convention on the Rights of Persons with Disabilities

¹ <https://consumerdatastandards.gov.au/engagement/reports/reports-cx/accessibility>

CONSUMER DATA RIGHT BOARD: 23 August 2022

- The Disability Discrimination Act 1992 (DDA)
- The Web Content Accessibility Guidelines (WCAG)
- The Australian Government Digital Service Standards (DSS)
- Australian and International Standards

The pragmatic response for the Data Standards Chair to these legal obligations is to support data standards that provide *equal access of use*^{2 3}. This means:

1. Enabling any user to locate, identify, operate functions, and to access the information provided, regardless of their physical, cognitive, or sensory abilities; and
2. Maintaining the privacy and security of any user at the same level regardless of the accessibility features of the content or service.

The Background Report indicates that a failure to provide equal access of use could exclude and discriminate against people with a disability, which would breach the DDA. Risks for not complying include:

- **Negative publicity and public perception of the CDR:** This includes the creation of reputational, program, and implementation risk for officials and the government, as well as negatively impacting businesses and consumers.
- **Legal action:** Including the risk of legal action related to the legislative obligations under the DDA in relation to a failure to provide equal access. The AHRC keeps a register of similar decisions under DDA.⁴
- **Secondary effects for sector organisations:** Resources being provided for others to use may result in acquired liability. Organisations may expect that the Chair and DSB have considered accessibility before producing and releases resources for others to use.

The review noted that research would be required to develop a Usability and Inclusivity framework with regard for vulnerable consumers. The review also suggests that such an approach would align with priorities previously raised by the Assistant Treasurer Jones, Minister for the CDR, who noted in 2019 that the potential impact of the CDR on vulnerable consumers needed to be monitored,⁵ and that more needed to be done to ensure vulnerable CDR consumers were not discriminated against.⁶

While the Background Report identifies obligations and opportunities for the Chair that the DSB will respond to and consult on, the review also outlines the benefits of complying with accessibility obligations, which include:

- **Increased innovation:** Accessibility features in products and services often solve unanticipated problems for a broader group of users, not just those with identified accessibility needs;
- **Improved Usability:** Accessibility features are essential for some and useful for all; and
- **Higher adoption:** With greater accessibility, a greater number of people can benefit from the CDR

The Accessibility Review will soon conclude with the finalisation of the Accessibility Improvement Plan, which is its final output. This report will include an extended list of recommendations for the

² ETSI EN 301 549 - V3.2.1 - Accessibility requirements for ICT products and services

³ AS EN 301 549:2020 - Accessibility requirements for ICT products and services

⁴ DDA: Register of Court decisions <https://humanrights.gov.au/our-work/disability-rights/dda-court-decisions>

⁵ Mr Stephen Jones (2019) [Treasury Laws Amendment \(Consumer Data Right\) Bill 2019, Second Reading](#) (13:20)

⁶ Mr Stephen Jones (2019) [Treasury Laws Amendment \(Consumer Data Right\) Bill 2019, Second Reading](#) (17:01)