20 May 2022

Secretariat
Statutory Review of the Consumer Data Right
The Treasury
Langton Crescent
PARKES ACT 2600

Classification Public

Via email to CDRstatutoryreview@treasury.gov.au

Re: Cuscal response to the Statutory review of the Consumer Data right
Cuscal Limited (Cuscal) welcomes the opportunity to provide feedback into the statutory review of the Consumer Data right (CDR).

We acknowledge that CDR has resulted in a fundamental change which could transform the entire economy. The consumers right on their data has the potential to improve an individual's life journey and is important the legislation adopts a balanced and long-term approach in setting requirements impacting all stakeholders.

Background to Cuscal
For over 40 years, Cuscal has leveraged our assets, licensing, and connectivity to provide intermediary and principal outsourcing activities on behalf of our clients. We are an end-to-end payments specialist that services more than 100 established ADI and challenger brand clients within Australia's financial system, including the majority of the mutual banking sector, and a growing number of FinTech and 'PayTech' enterprises. We enable their market connectivity so they may provide innovative products, business models, and drive improved customer outcomes.
We are an Authorised Deposit-taking Institution (ADI), the holder of an Australian Financial Services Licence, and an Australian Credit Licence for Securitisation purposes. Cuscal has Board representation with Australian Payments Plus, NPPA, BPAY, Eftpos, the Australian Payments Network and participates in numerous industry committees. We were the founder of 86400 (www.86400.com.au), a fully licenced mobile-led digitized bank, which we subsequently sold to National Australia Bank.
The services that we provide to our client institutions include card scheme sponsorship for issuing and acquiring, payment card issuing, card production services, digital banking applications, access to domestic payment services using direct entry, BPAY, the New Payments Platform (NPP) and Open Banking Data holder platform services. We also act as settlement agent for many of our clients through our Exchange Settlement Account with the Reserve Bank of Australia (RBA).
As a fully PCI-DSS accredited ADI, Cuscal is uniquely placed to provide secure and robust capabilities that facilitate access to markets that would otherwise be beyond the reach of some organisations.

Cuscal Role in Open Banking
To help our clients benefit from the CDR, while minimising their cost and risks, Cuscal has invested in a Collaborative Data Exchange.

This technology platform will position Cuscal as a CDR Intermediary that helps each of the three CDR participants obtain the most out of the CDR:

- Data Holders can manage compliance effectively.
- Consumers can share their banking data with best-practice simplicity, while remaining in control over the data they consent to share via their bank.
- Data Recipients can create better digital services, enabled by the data that consumers consent to share, but minimising the time, cost, and risk of doing it themselves.

Cuscal is working towards becoming an accredited data recipient soon, to enable a broad range of services for our CDR participants. For further information on Cuscal and our services please refer to our website at *www.cuscalpayments.com.au*

The issues paper has a list of five questions, and we have responded accordingly.

Q1: Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?
Response: The Part IV D of the Competition and Consumer Act 2010 focusses on standards and rules for the sectors designated by the Minister and has been developed in such a way that more sectors can be included as additional sections within the legislature. However, there are a few areas that Cuscal believes will become concerning as the CDR expands.

As CDR spreads across the economy encapsulating other sectors, it will be critical as to how **data protection** and privacy requirements are aligned for both Data holders and Data recipients. Currently the CDR has introduced Privacy safeguards that are mostly applicable for Data recipients. Data holders are deemed to be covered under the Privacy Act 1988. This is not contentious with respect to banking sector where the Data holders are approved deposit taking institutions that are highly regulated industries and covered by the Privacy Act together with prudential and capital requirements However, as the requirement becomes apparent to include other types of data holders such as non-bank lenders, BNPL services, retail, merchant services (which may have turnover less that the Privacy Act threshold of $3M) it is important that the levels of data protection and privacy standards are consistent across the industry irrespective of the sector they belong to. This will add a relevant regulatory requirement on these industries, as it is critical that all data holders are held to the same standards, if trust is to be fostered in the CDR. The Privacy Act 1988 will need to incorporate all designated entities that hold CDR data to the same standards and regulatory requirements. A suggestion would be to extend the same privacy safeguards to all Data holders that are not covered under the Australian privacy principles.

Secondly, the same issue exists with respect to the approach to **cybercrime** in these sectors. As industries are learning about the impacts and extent of cybercrime it is important that the required safety measures and reporting of cyber related incidents are aligned for all Data holders irrespective of the sector they are associated with. Currently under the CDR only Data recipients are required to report any cyber related instances to Australian Cyber Security centre (ACSC) under Schedule 2 subrule 1.7. It is understood that a Data holder in Banking and Energy will have their requirements under the license conditions to report cyber related incidents to specific regulators. As digitization and CDR touches each aspect of an individual's interaction in seeking and enabling services a standardised reporting for all cyber related incidents will support the ongoing resilience of the regime against cybercrime.

Currently the legislation does not cater for a comprehensive and cohesive framework for protecting consumer rights with respect to privacy or cyber related incidents.

The third area for improvement is the mechanism and channels for **raising consumer complaints**.
As the regime expands it will become difficult for consumers to ascertain which organisation, they are required to raise complaints and seek actions for redress. Thought should be given on defining a single agency for raising CDR complaints and for the agency to work internally among other government departments as required.

It is worth noting that the above items (and other ecosystem integrity matters) will also form part of considerations by Treasury regarding the graduated licencing regime for payments, which is a key part of the Government's response to the Farrell review of Australian Payments Regulation.
https://treasury.gov.au/sites/default/files/2021-12/p2021-231824_1.pdf

Q2: Do the existing assessment, designation, rulemaking, and standards-setting statutory requirements support future implementation of the CDR, including to government-held datasets?
Response: Cuscal **agrees with the current approach to designating sectors** which includes extended industry consultations and discussions with Treasury. This allows for informed and balanced discussion and relevant points of reference to be considered when approaching such complex pieces of legislation. Cuscal believes the industry has made substantial progress from when it commenced in 2019 and has now established an operating rhythm and understanding of implementing standards through the consultation process. This will need to continue as CDR considers Open Finance, action initiation and Government held datasets as future milestones to be achieved.

There are two aspects that we wish to highlight for consideration. Firstly, the **timeframes for consultation** through to implementation should be considered keeping in mind the broad range of participants at various levels of technological advancement. For example, the initial process of engaging the larger entities as part of rulemaking is simple and effective, however, care should be taken that the various distinctions within a sector are clearly understood by engaging the small to medium level participants to cater for relative regulation and compliance logistics.

Secondly, **CDR is principle-based legislation** and hence care should be taken that it is not too prescriptive in nature as it stagnates innovation and creates more friction. The Data recipient and Data holders are responsible for the management of consents and notifications to consumers. There are existing notification channels and so additional regulation prescribing the communication and contact channels for consumers can create complexity leading to confusion for consumers. An example highlighting this point will be the increasing number of consumer dashboards that an individual will need to maintain in the future when services become interconnected with payments.

For better and enriching outcomes, it is important that CDR allows regulated CDR intermediaries to build robust data driven tools for introducing innovative products and handling highly sensitive datasets. A fine balance needs to be achieved with respect to the number of screens and steps within the process to avoid becoming too prescriptive while at the same time achieving the desired compliance result with respect to privacy disclosures.

Q3: Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers?
Response: **The designation of CDR intermediaries** is a key aspect for growing the CDR ecosystem. As indicated in past consultations Cuscal believes that innovation is more likely to come from CDR intermediaries competing to build the best Data recipient experience for consumers.

This new segment of CDR participant is not currently recognised under the CDR rules. 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. This will allow CDR intermediaries to make investments in innovation as they have the legislative protection to build new services benefitting consumers.

CDR has the ability to not just impact a consumer's journey for a particular service or product but to enhance the life journey of a consumer. Hence CDR needs to be **interoperable with other services** that a consumer may use in their lifetime to help make the interaction simpler and meaningful. For example, sharing data is useful but the real impact is seen when a consumer can use their data to engage with multiple services and can receive better offer deals on products such as (data driven) increased credits, overdrafts, enhanced insurance cover, individualized services such as enrolling children in school, university etc. Additionally, to facilitate CDR scenarios like switching, date of birth should be added into a new *Identity* data cluster with name, and consideration be given as to how this could be assigned as an Identity Proofing Level and used for KYC.

Q4: Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?
Response: The CDR is based on the core principle of Consent that is voluntarily expressed, explicit, time bound and easily revokable. The direct-to-consumer service is seen as a service between the Data holder and the consumer which currently exists prior to the inception and evolution of the CDR. As such the **direct-to-consumer scenario can be well managed within the current framework** as Data holders are required to arrange the data sets in the CDR standards and will have the ability to share with consumers via the Consumer dashboard.

It is important to also acknowledge that there will be certain sectors that are not digitally advanced, and CDR has identified solutions such as concept of an "offline consumer" in the energy sector. Hence it is expected that without adding more legislative requirements there already exists a solution for consumers that require CDR data directly from their data holders via the existing CDR consumer dashboard.

Q5: Are further legislative changes required to support the policy aims of CDR and the delivery of its functions?
Response: As CDR expands the legislative framework would **require constant review** for policy desirability. Some of the identified areas that have been highlighted in other related consultations are:

- A critical requirement for CDR to be more effective will be its ability to be **interoperable across other multiple services** such as Digital identity, Payment processing, Centrelink services, Medicare services, ATO Superstream ecosystem, ASX trading systems etc.

- Since CDR is a fundamental change to how data ownership has moved from businesses into the hands of the consumer it is important that CDR is recognised as a **fundamental and broad piece of legislation** similar to Privacy in state and federal laws.

- As other countries embark on the Open banking journey similar to Australia and the United Kingdom, it is important to **understand the intersections** that needs to be catered for under the CDR. For example, the GDPR has a right to erasure - the CDR currently does not have a similar clause that can be applied under such circumstances. Instead, the CDR has a rule around de-identification or deletion of redundant data. There is difference in definitions and applications of such concepts hence there is a need for legal clarity for businesses that are captured under both Australian and international obligations.

Below are some additional points that Cuscal considers important for making CDR more effective in preparation for the future expansion.

- The introduction of Consumer Data right in Australia has paved the way for sharing data in a **secure and lawful manner**.

  To build on this high standard of data protection and increase in consumer confidence traditional, insecure practises of screen scraping should be (at some stage) prohibited under the legislation.

- An increase in **consumer participation and awareness** can only be achieved through planned educational and marketing programmes. There is a need for industry and Governments to work together to raise awareness among consumers to apply their consumer data right for better, competitive products and services.

- Organisations continue and will always need to **invest in CDR compliance**, however the constant nature of changes to standards and rules results in CDR participants focussing mainly on compliance first, hindering their capacity to work on innovative ideas and solutions. As compliance takes priority, organisations are focussed on meeting ongoing legislative requirements while balancing competing strategic priorities. Hence the current cadence of **ongoing standard changes should be re-considered**, and focus should be on making updates to CDR standards annually as part of sector implementation. For example: In the six months since October 2021 until now, we have seen the standards move four times. Even though there may be only a few minor changes in this standard release it requires resources to perform analysis and development effort to maintain compliance impacting existing project deliveries and increased pressure on capacity. The banking sector commenced CDR discussions in 2019 and changes to the banking standards are still ongoing resulting in changing priorities for businesses.

- For a data economy to function effectively the **data ingestion process** should be of a very high standard. The quality of data can heavily impact the level of services consumed and can lead to trust issues. Hence it is vital to ensure data quality is always met and any complaints in this area should be investigated and compliance measures applied.

- The **complaint resolution framework** in place for Banking, Energy and in future Telecommunications are designed with a siloed view of the interaction with a consumer. As CDR moves towards an economy wide implementation, considering public sector information and consumers seeking value across multiple producers i.e., a "horizontal model" we question whether the current complaint and resolution model is fit for purpose to support the future strategy?

- The **application of CDR banking data** for the purpose of identifying individuals would be valuable for certain use cases such as opening new accounts and onboarding consumers.

- As the economy is transforming to digital, one of the emerging issues is the threat of **cybercrime**. As the CDR expands an industry led cyber response plan should be reviewed and considered given the increased levels of interconnectivity resulting from interoperability. And the question remains whether the current regulatory model sufficiently captures management of cyber related crimes and is there a place for an independent regulator or area with a focus on Cyber.

We trust that our above responses help Treasury in its review and make recommendations that supports an economy wide implementation of CDR.

If we can be of any further assistance in the interim, please feel free to contact me at kmckenna@cuscal.com.au or (02) 8299 9000.

Yours sincerely,

Kieran McKenna
Chief Risk Officer