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

Australian Payments Network
Connect Inspire Thrive

20 May 2022

By email only: CDRstatutoryreview@treasury.gov.au

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the Treasury's Issues Paper on the '*Statutory Review of the Consumer Data Right (CDR)*'.[1] AusPayNet supports the review's aims in ensuring the CDR initiative fulfills its potential by putting customers at the heart of innovation and contributes to the digital economy through data-enabled payments and excellent integrated customer experience.

AusPayNet Membership and Role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop procedures, policies and standards governing payments in Australia. Our purpose is to enable competition and innovation, promote efficiency, and control and manage risk in the Australian payments ecosystem. AusPayNet has 150 members, including financial institutions, operators of Australia's payment systems, merchants, and financial technology companies.

Context: Alignment with Real-Time Payments

As noted in the Issues Paper, both the Government's Digital Economy Strategy[2] and the final report of the Inquiry into the Future Directions of the Consumer Data Right[3] found benefits in connecting the CDR to the broader data economy to drive the digital economy. Since then, the final report on the Review of the Australian Payments System[4] reached a similar conclusion.

In line with promoting payments efficiency while controlling risks, AusPayNet collaborated with the payments industry on two relevant initiatives: real-time payments infrastructure, and a digital identity framework.

In 2012, AusPayNet, then known as Australian Payments Clearing Association, formed the Real-Time Payments Committee to develop a better customer experience by delivering fast, versatile, and data-rich payments. This collaborative industry initiative led to the formation of New Payments Platform Australia Ltd (NPPA) to deliver a central infrastructure and world-class platform for an efficient and secure customer payments experience.
In 2018, AusPayNet, the Secretariat of the then Australian Payments Council, established Digital Identity Working Groups to modernise payment streams and build trust in the payments ecosystem. It is now the caretaker of the resulting TrustID Framework. This industry-focussed framework is an open, contestable

[1] Commonwealth Treasury, March 2022, 'Statutory Review of the Consumer Data Right– Issues Paper.' (link)
[2] Commonwealth Treasury, 2021, 'Digital Economy Strategy.' (link)
[3] Commonwealth Treasury, 23 December 2020, 'Inquiry into the Future Directions of the Consumer Data Right – Final report' (link)
[4] Commonwealth Treasury, 30 August 2021, 'Review of the Australian Payments System – Final report', Accessed 11 May 2021 (link)

framework that when operational, can be used by different organisations to offer a range of interoperable identity services to individuals and private sector entities. In practice it would allow end users to establish their credentials online with an accredited preferred service provider and then to use those credentials to verify who they are when interacting online. The Framework is not a digital identification solution in and of itself; it comprises rules and guidelines for organisations (which meet certain accreditation requirements) to design, build and operate digital identity products and services.

In light of its experience in facilitating the above initiatives, AusPayNet welcomes the opportunity to offer its experience and insights to assist in the review so that the benefits of expanding CDR may be realised. AusPayNet is also keen to share its input on the timing of new designations so that the industry has sufficient time to comply with new requirements. In preparation for this submission, AusPayNet consulted extensively with its Members, other commercial and government organisations and stakeholders in a series of workshops and an industry survey. The input below represents their key feedback.

Responses to Consultation Questions

1 – Objects of CDR

Question One

Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?

AusPayNet proposes updates to the objects to ensure that they remain fit-for-purpose for the expansion of the CDR initiative.

According to s 56AA in Part IVD of the *Competition and Consumer Act*[5],

> "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 (c) as a result of paragraphs (a) and (b), to create more choice and competition, or to otherwise promote the public interest." (Emphasis added)

RECOMMENDATION: AusPayNet suggests a technical change in s 56AA(a) such that the word 'certain' be replaced with the term, 'designated', for consistency with the terms used while designating sectors in CDR.

[5] *Competition and Consumer Act 2010* (Cth) (link)

2 – Future Implementation of CDR

Question Two

Do the existing assessment, designation, rule-making and standards-setting statutory requirements support future implementation of the CDR, including to government-held datasets?

AusPayNet notes that existing CDR statutory requirements need to be reviewed to support future implementation of the CDR. During our consultations, the overriding feedback is that the common elements of the CDR and other relevant frameworks need to be aligned to avoid duplication or confusion. These common elements include regulatory requirements, accreditation, technology standards and dispute resolution.

Alignment of Frameworks and Compliance Requirements – Licensing Requirements

As set out in the Review of the Australian Payments System, there is a need to have a "close link between the CDR and payments strategy to ensure that the strategic focus of each is aligned". Many participants in the payments ecosystem will be impacted by both CDR and payments initiatives, given many are involved in the facilitation of both transactions and underlying consumer data flows. Therefore, the alignment should extend to the proposed payments licensing regime once it is established (as the Review of the Australian Payments System envisages).

Alignment of Frameworks and Compliance Requirements – Liability Model

In general, AusPayNet would be supportive of more coordinated and consistent rule changes across regulators. There are good models for this approach elsewhere in the world, for example the UK's Regulatory Initiatives Grid.

The table below shows an example of the differing liability models – a commonly raised concern amongst our Members – used in the CDR, TDIF and *AML/CTF Act*. Applying a strict reading of the legal text quoted below, under CDR, an entity is not liable for poor provision of *data* if it follows the statutory requirements in good faith and has the evidence to prove its case. Under TDIF, an entity is not liable for the provision of the *service* for similar reasons. Under AML/CTF, an entity's liability for poor *identity verification* based on its *data* depends on a different measure i.e. whether the subject is of a low and medium risk or high risk. Such inconsistent requirements are a barrier to interoperability authentication solutions.

CCA s 56GC	**TDIF s 39**	**AML/CTF[6]**
Complying with requirements to provide CDR data: protection from liability (1) If: (a) a CDR participant, or designated gateway, for CDR data (the CDR entity): (i) provides the CDR data to another person; or (ii) otherwise allows another person access to the CDR data; and (b) the CDR entity does so, in good faith, in compliance with: (i) this Part; and	Accredited entities onboarded to the system protected from liability in certain circumstances (1) If, while onboarded to the trusted digital identity system, an accredited entity: (a) provides, or fails to provide, a service for which it is accredited; and (b) provides, or fails to provide, the service to another accredited entity onboarded to the trusted	'Safe harbour' customer verification procedures for medium or lower risk individuals You may use 'safe harbour' procedures to verify your customer's identity if they are an individual and you have assessed their money laundering and terrorism financing risk as medium or low. These checks are less stringent than those required for high risk customers. You must still verify their full name, and, depending on which you collected, either their date of birth or residential address.

[6] AUSTRAC, 'Customer Identification: Know Your Customer (KYC)', Accessed 11 May 2021 (link)

(ii) regulations made for the purposes of this Part; and (iii) the consumer data rules; the CDR entity is not liable to an action or other proceeding, whether civil or criminal, for or in relation to the matter in paragraph (a). Note: A defendant bears an evidential burden in relation to the matter in subsection (1) for a criminal action or criminal proceeding (see subsection 13.3(3) of the Criminal Code). (2) A person who wishes to rely on subsection (1) in relation to a civil action or civil proceeding bears an evidential burden in relation to that matter. (3) In this section: evidential burden, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.	digital identity system, or to a participating relying party; and (c) provides, or fails to provide, the service in good faith, in compliance with this Act and with the technical standards that apply to the entity; the entity is not liable to any action or other proceeding, whether civil or criminal, brought by an accredited entity or a participating relying party in relation to that service. (2) An entity that wishes to rely on subsection (1) in relation to an action or other proceeding bears an evidential burden (within the meaning of the Regulatory Powers Act) in relation to that matter.	You can use either reliable and independent documents or electronic data to verify the identity of your medium or low risk customer. For documents, you must use original or certified copies of primary or secondary documents. For electronic data, you must use at least two separate data sources to verify customer information. This can include records from credit reporting agencies.

<u>CDR Dataset and Technical Standards</u>

The CDR expansion to include more datasets will require further analysis on how data should be categorised according to the functions being performed instead of traditional sectoral boundaries.

3 – Development of CDR-Powered Products and Services

Question Three

Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers?

A broad range of stakeholders has raised the current operation of the consent flow as a detriment to the consumer experience. According to the Customer Experience guidelines set by the Data Standards Body,[7] the consent flow is an eight-step process that can be conducted through back-and-forth writing or a consumer dashboard. The consumer largely plays a respondent role and is subject to the initiative and servicing times of the data recipient and especially of the data holder. In the consent flow, the consumer is involved in six of the eight steps while the data holder is involved in five of the eight.

1. *Consumer* waits for a data recipient to contact him/her.
2. *Consumer* gives consent to data recipient to request his/her data from the data holder.
3. Data recipient contacts and requests data from data holder.
4. **Data holder** contacts *consumer* and asks consumer to authenticate him/herself.
5. *Consumer* authenticate him/herself by sending a One-Time-Password (OTP) to the **data holder.**
6. **Data holder** requests *consumer* to authorise the disclosure of their CDR data to the data recipient.
7. *Consumer* provides authorisation to the **data holder.**

[7] Data Standards Body, 21 Jan 2022, 'Consent Flow: Consumer Data Standards and Guidelines' (link)

8. **Data holder** shares *consumer*'s data with the data recipient.

The current multi-step consent flow and passive nature of the role the consumer plays are counterproductive to the intended introduction of action initiation to CDR by the final report of the Inquiry into the Future Directions of the Consumer Data Right.[8] Comparatively, NPPA's PayTo will have a streamlined consent process whereby the consumer can authorise third parties to make payments on his/her behalf directly through the smartphone so that the consumer has greater visibility and control over their mandate payment arrangements.[9]

RECOMMENDATION: AusPayNet recommends harmonising the CDR consent flow and PayTo consent flow to benefit consumers.

4 – Direct to Consumer Data Sharing

Question Four

Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?

The CDR legislative framework could be revised to improve consent management.

Consent mechanism

The current consent flow is derived from legislative requirements in r 4.11(1)(c), 4.13(1), 4.22 and 4.25(1) of the Competition and Consumer (Consumer Data Right) Rules (CDR Rules).[10] The rules work together such that the consumers are bound to work through data holders and recipients and cannot initiate payment actions.

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

(1) When asking a CDR consumer to consent to the collection and use of their CDR data, an **accredited person must: …**

(c) **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

[8] Commonwealth Treasury, 23 December 2020, 'Inquiry into the Future Directions of the Consumer Data Right – Final report' (link)

[9] New Payments Platform Australia, November 2021, 'PayTo: Service Overview.' (link)

[10] Competition and Consumer (Consumer Data Right) Rules 2020 (link)

(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.**"

(emphasis added)

RECOMMENDATION: AusPayNet recommends a review of r 4.11(1)(c), 4.13(1), 4.22 and 4.25(1) to enable consumer payment initiation and harmonisation with the PayTo consent flow.

Consent Bundling

The restriction against consent bundling in r 4.10(1)(b)(ii) of the CDR Rule does not follow technology trends and is not fit-for-purpose. It is not aligned with the direction of current discussions in creating digital identity solutions to provide convenient and secure processes (including in payments), without the need for consumers to repeat their information and consent and thus, suffer from consent fatigue. Consent bundling is required to process increasingly complex or ongoing digital/data activities (including payments).

Notwithstanding the above, AusPayNet is of the view that r 4.9(d) alone should suffice to ensure that the bundled consent provided will not be misused. This is because while there may be consent bundling of multiple (payment) activities, the consent in its totality is still provided in the context of a specific purpose.

"4.9 Object

The object of this Division is to ensure that a consent 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: ...
(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.

(emphasis added)

RECOMMENDATION: AusPayNet proposes Rules 4.10(1)(b)(ii) be repealed.

Conclusion

AusPayNet appreciates the opportunity to respond to the review and to contribute our insights from the perspective of the payments industry. We would also welcome the opportunity to engage further with the Treasury on the issues raised in this submission.

[redacted]

Yours sincerely

Andy White
CEO, Australian Payments Network