DATA STANDARDS BODY

10 October 2023

Department of Finance
1 Canberra Avenue
FORREST ACT 2603

Submission to the Digital Identity Bill 2023 consultation

I have been the Data Standards Chair for the Consumer Data Right (the CDR), responsible for making and reviewing the CDR data standards, since 2018. In this role, I am supported by the Data Standards Body (the DSB). I have overseen the development of the CDR data standards in the banking and energy sectors, where CDR is currently operating, and the non-bank lending sector, where implementation is under way.

I have gained unique insight into the opportunities and challenges associated with standards development in Australia's digital economy. Two lessons are particularly relevant.

- A complex ecosystem like the Digital ID data standards will not be based on a single standard but a family of inter-related standards drawn from many sources. The CDR data standards, for example, incorporate international standards, national standards and specially developed standards which give effect to the CDR rules. Many of these overlap with other government and private initiatives, including Digital ID.

- The management of security, trust and risk is a major concern in the development of digital standards. In my experience, creating a safe and secure ecosystem requires a single line of accountability for risk management. When that accountability is distributed across multiple people or organisations it is difficult to ensure risks are properly identified and mitigated. In the case of both CDR and Digital ID, this can have a direct impact on Australian consumers.

The exposure draft of the Digital Identity Bill 2023 (the Bill) marks an important step towards the creation of a world-class digital economy in Australia. I strongly support the commitment to secure, inclusive, and convenient online identity verification. This submission outlines my feedback to further strengthen this initiative. My primary recommendation is for Digital ID and CDR data standards to be made by the same Data Standards Chair, advised by a single DSB.

- Digital ID and CDR naturally overlap and there are significant efficiencies to be gained from developing them together. CDR stakeholders have repeatedly raised the need for digital identity to be addressed and have highlighted the opportunities for convergence and consolidation.[1]
- Consumers, too, will be interacting with both Digital ID and CDR. Divergent ecosystems and requirements risk impacting consumers' experience of both ecosystems, undermining their trust and affecting their perception of Government.

[1]See selected Data Standards Advisory Committee minutes relating to digital identity and TDIF in December 2019, March 2020, February 2023, and June 2023.

- The security of Australians' data is paramount for both initiatives. Cyber security is a national priority, as illustrated through recent reforms to the *Security of Critical Infrastructure Act 2018*. The rapid increase in cyber attacks and cybercrime means it is imperative that the CDR and Digital ID are in lock-step in responding to online threats, including implementing a common set of security standards. The alternative risks security divergence that will open up additional surfaces for cybercriminals to attack.
- The CDR is a world-leading digital reform and the data standards have international recognition[2] and influence.[3] The DSB is actively engaged in international standards development and collaboration. Developing the CDR and Digital ID data standards in isolation would have significant implications for this work. Notably, divergence of these two reforms may impair interoperability both nationally and globally, increase implementation costs and could affect trans-Tasman interoperability, which is important given the many organisations who operate in both Australia and New Zealand.

A secondary, and subordinate, recommendation is that the scope of the data standards, for both reforms, should cover all technical aspects that contribute to the management of security and trust. This will ensure both a clear line of accountability for these concerns but will also ensure a single avenue for security related issues to be raised and consulted on. As part of this, it is important that the Digital ID Data Standards Chair has the authority to make standards in relation to the matters for which they are accountable under the Bill.

In summary, Digital ID and CDR should not be developed in silos. Even with the best intentions for collaboration, separate standards-making processes will increase the risk of duplicated or conflicting requirements. This could compromise the success of both initiatives, while also undermining data security and public trust in the Government. Conversely, if developed together, Digital ID and the CDR can hasten the development of a world-class digital Australian economy, with consumers at its centre.

Further feedback, including more detailed comments on the Bill, is attached.

Yours sincerely

[redacted]

Andrew Stevens
CDR Data Standards Chair

Attachment A: Benefits of the Digital ID and CDR data standards being made by the same Chair, supported by a single Data Standards Body

Attachment B: Detailed comments on the draft Bill

[2]Financial Conduct Authority, "Call for input: open finance".
[3]Draft Customer and Product Data Bill (NZ), s 89, and Office of the Minister of Commerce and Consumer Affairs, "Establishing a Consumer Data Right" (June 2021).

DATA STANDARDS BODY

Attachment A: Benefits of the Digital ID and CDR data standards being made by the same Chair, supported by a single Data Standards Body

The CDR gives consumers the right to share their data between service providers to get a better offer or access new services. It is intended to apply sector by sector across the whole economy, having begun in the banking and energy sectors. Work is currently under way to extend the CDR to the non-bank lending sector. Participants in these sectors include banks, energy retailers, non-bank lenders and accredited data recipients (including a variety of fintechs). The CDR is now well-established[4] with very active consumer usage.[5]

The CDR data standards make it easier and safer for consumers to access data held about them by businesses, and to share this data via application programming interfaces (APIs) with trusted, accredited third parties. They are made up of:

- technical standards for participants, including REST APIs, data schemas and security measures
- consumer experience standards, dealing with requirements for consumer-facing interactions, such as data language, authentication, and accessibility. [6]

Benefits of aligning technical standards

The CDR and Digital ID are both cross-economy initiatives, meaning they will have common participants who must understand and comply with the requirements of both. Developing standards in isolation would risk duplication of effort and unintended conflicts, with participants in both schemes subject to overlapping but contradictory regulation.

Unified and aligned standards could simplify implementation and compliance for organisations likely to participate in both regimes.[7] Examples of requirements and standards that should be aligned across both Digital ID and CDR include the Trusted Digital Identity Framework (TDIF)[8] and CDR standards setting out consent, information security, accessibility, and usability requirements.

The CDR data standards already refer to external requirements, such as TDIF and the Web Content Accessibility Guidelines (WCAG), and are subject to ongoing review and enhancement. This allows new functionality to be incorporated and new sectors to be accommodated, while also maintaining alignment with evolving technologies, security postures, and consumer behaviour and expectations. A single Data Standards Chair for both the CDR and Digital ID would build on this already effective process for data standards development and implementation. The incorporation of Digital ID could be further enhanced with standardised access to CDR data, including the potential introduction of verified credentials, which could further facilitate online identity verification.

---

[4]As at September 2023, there were 113 participating Data Holders brands across banking and energy sectors, 45 active Accredited Data Recipients, 88 CDR Representatives, and 118 software products in market.
[5]Over 54 million API calls in September 2023 and over 564 million API calls in the last 12 months, current at October 2023.
[6]See the CDR Data Standards v1.26.0; 24 August 2023.
[7]Mastercard, for example, is an active accredited data recipient (ADR) in CDR with an active TDIF accreditation status, while all four major banks are both ConnectID members and ADRs.
[8]See TDIF Release 4.8 Feb 2023

Aligning the standards could also support efficiency by leveraging commonalities and consolidating expertise. This is particularly critical when the technical skills required to develop world-leading data standards are in high demand and short supply.

Benefits of aligning consumer experience standards

The CDR consumer experience is reviewed and improved on an iterative basis. Stakeholders have pointed to the value of applying the CDR's consent model to other initiatives, including digital identity. Approaching consent and data access consistently would simplify implementation and compliance but also, importantly, support consumer experience and trustworthiness. Consumer experience research conducted by the CDR Data Standards Body has repeatedly shown the importance of trust and consistency to support willing and informed consent.

The value of a single Data Standards Chair and body for providing consistency could extend beyond Digital ID and CDR. The Privacy Act Review, for example, recommend the development of guidance for designing consent. Any such guidance should consider existing consent processes in CDR and Digital ID.

Benefits of consolidating consultation processes

Many stakeholders will be impacted by both the CDR and Digital ID. Consolidated consultation processes, with oversight from a unified Data Standards Body and Data Standards Chair, would provide greater certainty and would allow consultations to be appropriately sequenced in recognition of their relative priority and complexity. These consolidated processes could draw on CDR's established community of practice and lessons learned since 2018. This would mitigate the risk of consultation fatigue, lead to more effective engagement and support efficient use of community and Government resources.

Benefits of aligning other aspects of the framework

While my focus is data standards, there are other opportunities for alignment between the CDR and Digital ID, for example in relation to trustmarks, where there is an opportunity for both CDR and Digital ID to be indicated consistently and, by extension, reflect consistency in consumer expectations.

The importance of alignment extends to the broader ecosystem requirements for Digital ID. This includes the requirements set out in the draft Bill and rules, where there are already notable points of divergence from the CDR, such as in relation to the deletion of data and the processes and requirements for seeking consent. This is likely to result in some participants being accredited to participate in both Digital ID and the CDR but having conflicting obligations in relation to the use and disclosure of personal information.

DATA STANDARDS BODY

Attachment B: Detailed comments on the draft Bill

1. Importance of supporting an agile and responsive standards-making process

The Bill diverges from the *Competition and Consumer Act 2010* (the CCA) in ways that could impact on the agility of the data standards making process, including:

- the fact that no provision has been made for minor or urgent standards to be made without the consultation requirements (both public and Ministerial) applying
- the requirement for the Digital ID Data Standards Chair to consult the Minister before making or amending standards
- the fact that the Digital ID data standards will be a legislative instrument.

Transparency and open consultation are key components of the standards-making process. It is important that the Bill's requirements to consult do not unduly restrict the Digital ID Data Standards Chair's ability to openly and transparently, but swiftly, respond to significant issues or community requests for change. In particular:

- the Digital ID Data Standards Chair should be able to make minor or urgent standards without the consultation requirements (both public and Ministerial) applying. This power is available to me under the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules) in relation to the CDR data standards. While I have not used it frequently, it is an important power that allows me to swiftly respond to critical issues in the standards, without causing undue disruption to participants. This is essential for standards, where relatively small discrepancies can disrupt the effective functioning of the system.

- the process for consulting the Minister before making or amending standards should be no more onerous than the requirement to consult the Data Standards Advisory Committee, the Information Commissioner and the Australian Competition and Consumer Commission (ACCC) about changes to the CDR data standards under the CDR rules.

2. Need for a dedicated body to assist the Digital ID Data Standards Chair

Under the draft Bill there is no body whose function is to assist the Chair, in contrast to the DSB's role under Part IVD of the CCA.[9]

The provisions of the CCA related to the DSB have allowed appropriate flexibility for contractors to be engaged, and to work closely with APS staff, without unduly restricting the DSB's structure. Flexibility in these matters is desirable, as demonstrated by machinery of Government changes which transferred the DSB from the Commonwealth Scientific and Industrial Research Organisation to Treasury in 2020.

Based on my experience receiving assistance from the DSB, I am concerned that the alternative arrangements set out in the Bill, where the Chair is supported by APS staff but able to engage consultants, may lead to inflexibility and lack of clarity about the respective roles and responsibilities of those APS staff and consultants.

[9]sections 56FJ and 56FK.

It would be preferable to replicate the provisions of the CCA, including:

- explicitly creating a body whose function is to assist the Chair
- clarifying that the body has the power to do all other things necessary or convenient to be done for or in connection with the performance of that function.

3. Need for an advisory committee to advise the Digital ID Data Standards Chair

The draft Bill allows the Minister to establish an advisory committee to provide advice to the Digital ID Data Standards Chair in relation to the performance of the Digital ID Regulator's functions and exercise of the Regulator's powers under the Act.

This is in contrast to the CCA, which gives me the power to establish committees, advisory panels and consultative groups, and the CDR Rules, which require me to establish and maintain a committee to advise the Chair about data standards in relation to each designated sector.

This has led to the establishment of the Data Standards Advisory Committee (the DSAC), with a membership made up of industry experts, privacy and consumer representatives and academics. Over the years, DSAC members have provided me with valuable insights and support. I consider my ability to select and appoint members, which has allowed me to ensure the Committee represents a diversity of industry and community views, critical to the effective functioning of the DSAC.

Separately, during my tenure, I have established focused, short-term consultative advisory groups to deal with specific topics and problems. This has been an effective and efficient mechanism to assist me in developing robust, best-practice data standards.

The Bill should:

- clearly allow the Digital ID Data Standards Chair to establish committees, advisory panels and consultative groups, separate to the Minister's power set out in the Bill
- be clear that the purpose of any advisory panel to be established by the Minister is to advise the Digital ID Data Standards Chair on Digital ID data standards
- allow the Minister's power to establish such a committee to be delegated to the Digital ID Data Standards Chair (with early consideration given to delegating the power).

4. Providing flexibility on where draft standards are published

The proposal to require draft Digital ID data standards to be published on the Department's website is restrictive. For consultations on new or amended CDR data standards, I publish drafts on collaborative platforms that allow stakeholders to submit feedback in an open and transparent manner. This establishes trust in the process for making standards and ensures there is public accountability and auditability. Providing flexibility on where standards consultations are published would allow draft standards to be published on a website dedicated to Digital ID standards or a common website for both CDR and Digital ID standards.

It should be left to the judgment of the Digital ID Data Standards Chair where to publish draft standards (provided they are available on the internet). Alternatively, requirements should be set out in delegated legislation so they can be more easily adjusted to suit stakeholder needs.

5. Matters that can be dealt with in the Digital ID data standards

The Digital ID data standards are currently referred to in terms that include technical, design, data, and test standards. The scope of Digital ID data standards should not preclude the Chair from making:

- consumer experience standards beyond those relating to usability and accessibility in the accreditation rules
- standards related to data security and deletion
- standards related to de-identification of data
- standards relating to deleting or anonymising an online identity.

6. Digital ID Regulator's ability to enforce the standards

Currently there is no ability for the Digital ID Regulator to enforce non-compliance with the Digital ID data standards. An enforcement mechanism is critical to the effective functioning of the system and the Bill should be amended to include one.