OPTUS

10 October 2023

[redacted]

Re: Draft Digital Identity Bill and Rules

Optus welcomes the opportunity to provide its feedback on the *Draft Digital Identity Bill and Rules*. Expanding access to secure digital identity services for all Australians is a crucial task that will bring numerous economic and security benefits.

Overall, Optus is supportive of this critical initiative. It should not only support a significant productivity uplift for the delivery of digital services to Australians but, done correctly, also materially reduce the risks associated with the storage of identity data. Optus is already advanced with Digital ID in our business and believes that the Bill will provide an important legislative framework that will provide confidence for Australians in utilising digital ID technologies.

Optus also offers the following more specific points for the government's consideration:

1. Government should consider harmonising the regulatory obligations under the Bill with other relevant legislation (such as the Privacy Act and, for our industry, the Telecommunications Act and Telecommunications (Interception and Access) Act) to ensure businesses do not need to hold customers' personal ID document data as a result of other regulatory obligations. Specifically, this means that telecommunications providers would need relief from their various obligations to retain customers' ID document data.
    a. It should be made clear that retaining a record of the confirmation of the ID via a digital process and enabling law enforcement (or other similar bodies) to refer back to this transaction, where required for investigative purposes, would be sufficient to discharge the obligation of a telecommunications provider to properly identify its customers.
    b. An example in the Draft Bill is the section 28(2) requirement that an organisation deactivates a digital ID on request by the individual. This appears to conflict with obligations under both the Telecommunications Act and Mandatory Data Retention Regime that require telecommunications carriers to retain customer records for minimum periods (e.g. for investigating Telecommunications Industry Ombudsman complaints).
2. On a related note, Optus seeks clarification as to whether the Digital ID System will be aligned with those under the Security of Critical Infrastructure (SOCI) Act and, if so, how this might apply in practice? Specifically, could the system information (as defined in Section 10 (2) of the Draft Rules) that participating entities hold be considered a 'critical infrastructure asset' and therefore subject to the SOCI Act obligations?
3. In relation to the security breach reporting provisions of the Draft Bill, Optus seeks clarification as to whether a breach would also require reporting to other government agencies and/or regulators. There are currently a range of reporting obligations under various legislation such as the Privacy Act and Security of Critical Infrastructure Act as well as sector-specific laws (in our case the Telecommunications Act).

[redacted]

   a. It would be useful to clarify how these various obligations interact and whether there is an opportunity for streamlining these reporting processes to one body rather than multiple entities.

4. When conducting credit checks, the probability of a successful identity verification is increased if a unique identifier can be included (such as a driver's licence number), not just name, address and date of birth. When using Digital ID verification, there may be resistance from customers to sharing this additional data, even if the purpose and benefit are disclosed. We therefore recommend that the Digital ID mechanism cross-references back to credit agencies for appropriate transactions. This would ensure the current higher frequency matching benefit is maintained without customers having to share additional personal information.
5. Section 45 (2) (b) of the Draft Bill provides that you cannot use biometrics to test for the presence of multiple digital IDs.
   a. While the intent of this clause is clear and we are supportive of this intent, Optus suggests that the risk it generates could potentially outweigh the public benefit, specifically the risk of fraudulent activity through the use of multiple identities. The benefits of using biometric verification can range from customer benefit (e.g. multiple records can be consolidated for the benefit of the biometric owner) through to fraud prevention (as it will enable identification of a proliferation of IDs against one real identity, which is a common sign of fraud). Having appropriate safeguards would of course be crucial to enable this but we suggest that government consider allowing biometrics to be used to test for multiple IDs given the benefits for both customer experience and fraud prevention.
6. The requirement under section 48 (4) (4) (b) that organisations complete a fraud investigation in 14 days is unworkable. Based on our extensive experience with fraud investigations, Optus strongly recommends that a 180 day period would be more realistic.
7. Optus views the liability and redress framework in Section 79 as being much too broad. We recommend that there be more precision about the potential injury from which the section is providing protection (e.g. actions from an individual who is aggrieved by an entity confirming or failing to confirm their identity). This would help provide more regulatory certainty for participating entities.
8. We note that there is likely to be a transitional effort required to move to an arrangement where existing ID data must be deleted as we validate a new digital ID. We are unsure of the time and effort required to ensure this so, while we support the intention to move quickly, we recommend that the Bill stipulate an appropriate timeframe in which to implement this transition.

We appreciate the Australian Government's consideration of these issues and would be happy to discuss our submission further.

[END SUBMISSION]