AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

26 October 2021

Digital Transformation Agency
PO Box 457
Canberra City ACT 2601

By upload: https://www.digitalidentity.gov.au/have-your-say/phase-3/submission-form

ARCA submission - Trusted Digital Identity Bill

Thank you for the opportunity to provide a submission on the Trusted Digital Identity Bill (**the Bill**) and related legislative instruments which were released on 1 October 2021, as part of Phase 3 of Australia's Digital Identity legislation.

ARCA is the peak industry association for businesses using consumer information for risk and credit management. Our Members include banks, mutual ADIs, finance companies and fintech credit providers, as well as credit reporting bodies and, through our Associate Members, many other types of related businesses providing services to the industry. Collectively, ARCA's Members account for well over 95% of all consumer lending in Australia.

ARCA's previous submission – the Digital Identity Legislation Position Paper

ARCA has previously provided a submission dated 13 July 2021, in relation to the Digital Identity Legislation Position Paper (**Previous Submission**).

In the Previous Submission, ARCA has set out its views in relation to the Digital Identity Legislation Position Paper under four separate topic headings (as referred to below).

ARCA's submission – the Bill

As stated in the Previous Submission, ARCA welcomes the proposal to expand the availability of the Digital Identity System (**the System**) to the private sector (including companies such as banks and utility providers) and to state, territory and local governments.

Having reviewed the Bill and ancillary materials, ARCA is broadly supportive of the Bill and related legislative instruments (apart from those issues and concerns specified below) and we are of the view that these instruments will greatly assist the Government to achieve its stated intention to:

- Enable the expansion of the System and in particular, to enable greater participation by state and territory governments and the private sector:
- Enshrine in law various privacy and consumer protections, so that Australians can have confidence in the System and feel that their personal information is safe and secure, and
- Establish permanent governance arrangements and a strong regulatory regime.

We consider that the Bill and the ancillary documentation, address a number of the matters raised within the Previous Submission. In particular, the concerns raised within the Previous Submission under the topic headings *'1 - The creation of new privacy laws and regulation within the Proposed Legislation'* and *'4 -Security of personal information'*.

However, we consider that the Bill and the ancillary materials do not address all of the issues raised in the Previous Submission, and in particular those set out under the headings *'2 - The scope of the Oversight Authority'* and '*3 - The potential interoperability of the System with other systems or services'*, as well as giving rise to the following new issues:

- Potential for legal uncertainty and regulatory overlap - incident notification requirements, and
- Uncertainty in relation to the visibility and impact of advice provided by the Information Commissioner.

We have set out in detail below ARCA's concerns in relation to the Bill.

1. The scope of the Oversight Authority

In the Previous Submission, ARCA put forward the position that:

- Enforcement activity by the Oversight Authority should be limited to breaches, or potential breaches, of obligations or requirements contained within the relevant legislation regulating the System and which are specific to the operation of the System, and
- The legislation regulating the System should contain an explicit exclusion from the jurisdiction of the Oversight Authority, any breaches or suspected breaches, of privacy related laws or regulations which are referred to, or contained within, external legislation or regulation.

In light of the operation of section 64 of the Bill, it is our understanding that the laws within the Privacy Act relating to the collecting, using and disclosing of 'personal information' (as defined by the Privacy Act), will apply to the information of individuals who elect to participate in the System (that is, information which falls within the description of 'attributes', 'restricted attributes' or 'biometric information' will be deemed 'personal information' under the Privacy Act).

In this context, we note that section 87 of the Bill confers upon the Oversight Authority a number of functions including, but not limited to, the following:

- To advise and assist entities in relation to their obligations under the Bill:
- To promote compliance with the Bill, and

- To do anything that is incidental or conducive to the performance of any of the specified functions of the Oversight Authority.

We also note that under section 88 of the Bill, the Oversight Authority has the power to do "…*all things necessary or convenient to be done for or in connection with the performance of its functions*."

While the drafting of the provisions referred to above, indicate an intention for the authorised functions and actions of the Oversight Authority to be limited to activities in connection with the Bill, the operation of section 64 of the Bill means that there may be situations where action taken by the Oversight Authority extends to the interpretation and application of laws arising under the Privacy Act.

For example, if the Oversight Authority advises an accredited entity that it considers that entity to have breached a requirement of the Privacy Act in connection with their handling of the 'personal information' of an individual utilising a service under the System, there is potential for the Oversight Authority to;

- indirectly create new expectations as to the operation of that particular Privacy Act clause(s), and/or
- create legal uncertainty in the event that the view of the Oversight Authority conflicts with, or is contrary to, previously established legal principles or expectations.

In our view, both of these outcomes would further contribute to the fragmentation (and at times, uncertainty) which affects certain areas of privacy law and regulation in Australia.

We therefore re-iterate our position as expressed within the Previous Submission that:

> *"The form, content and outcome of any enforcement activity by the Oversight Authority should therefore be considered against any potential unintended consequences which it may have on a participant's compliance (or perceived compliance) with privacy legal and/ or regulatory requirements."*

2. The potential operability of the System with other systems or services

In the Previous Submission ARCA put forward its view that it considers that the legislation regulating the System should:

> "…*contain sufficient flexibility so that the System and an individual's Digital Identity can interface with, and potentially look to be utilised in conjunction with, other identity systems and services*."

The Bill, and in particular section 33 of the Bill, clearly contemplate and support the interoperability of services *within* the System. However, the Bill does not appear to contemplate operability with other regulated systems such as those utilised by participants within Open Banking.

For example, the Bill does not provide for;

- the potential ability for participants (either individuals or entities) within the System, to be able to utilise any aspect of an individual's Digital Identity

(including any consent(s) provided by an individual in connection with the System), or

- the potential ability for entities to ustilise any aspect of the processes and procedures implemented by the entity in connection with the System, with any other systems or services.

We note that the Regulatory Impact Statement contemplates the long-term benefits of adoption of the System across the economy and the potential benefits associated with the eventual connection of state, territory and private sector services as well as Federal Government services. However, the omission from the Bill of any mechanism to support the potential operability of the System with other external systems and services, may potentially reduce or remove the possibility of adoption of the System across the economy.

We maintain our view that operability with other systems and services is highly desirable and that where a potential participant within the System is a financial services provider, the ability to utilise or rely upon a single identity system when providing various online services may be a relevant consideration in respect of participating in the System.

3. Potential for legal uncertainty and regulatory overlap - incident notification requirements

Legal uncertainty

In the event of a cyber security incident or a digital identity fraud incident, section 43 and 44 of the Bill impose an obligation upon the relevant entity to make all reasonable efforts to contact any individuals '*affected by the incident'* as soon as practicable after becoming aware of the incident.

Precisely what it means for a person to be *'affected'* by an incident is not qualified or explained within the Bill.

This can be contrasted with the approach adopted in relation to the relevant Notifiable Data Breach (**NDB**) obligations contained within Part IIIC of the Privacy Act, which clarifies that the obligation to notify individuals about a data security incident arises in circumstances '*likely to result in serious harm'* to the individual.

We consider that by failing to specify the circumstances in which an individual is deemed to be '*affected*' by an incident, there is the potential for uncertainty and inconsistent interpretation of the incident notification requirements. On this basis, we suggest that the Bill and/or related legislative instrument, be amended to incorporate clarification and specificity as to the application of the incident reporting obligations, including in relation to when an individual will be deemed *'affected'* by an incident.

Potential regulatory overlap

It is our understanding that in the event of a cyber security or digital identity fraud incident, there is the potential that a relevant entity may, in certain instances, be required to simultaneously comply with both the NDB obligations as set out in the Privacy Act and the notification obligations set out in the Bill.

We consider that the imposition of two sets of notification requirements, under two different sets of legislation in relation to the same incident should be avoided, as this has the potential to:

- lead to legal and regulatory uncertainty on the part of the entity, in relation to their notification obligations;
- cause duplication of works and resources on the part of the entity; and,
- may result in an impacted individual being provided two different notices in relation to the same incident.

4. Uncertainty in relation to the visibility and impact of advice provided by the Information Commissioner

Under section 70 of the Bill, at the request of the Oversight Authority, the Information Commissioner is required to provide advice upon matters relating to the operation of the Bill. For the reasons referred to above under the section titled '*1 The scope of the Oversight Authority'*, the Oversight Authority may be able to seek advice on matters relating to operation or requirements of the Privacy Act.

In light of the potential for advice provided by the Information Commissioner to impact upon and/or relate to Privacy Act requirements, ARCA is of the view that it is in the public interest for such advice to be made publicly available.

We also consider that in discharging its functions the Oversight Authority should act in a manner which is consistent with the views of the Information Commissioner and believe that the Bill should contain an explicit requirement upon the Oversight Authority to do so.

If you have any questions about this submission, please feel free to contact me on 0414 446 240 or at mlaing@arca.asn.au, or Mary Vancea on 0403 137 435 or at mvancea@arca.asn.au.

Yours sincerely,

Mike Laing
Chief Executive Officer
Australian Retail Credit Association