



27 October 2021

Mr Jonathon Thorpe
General Manager
Digital Identity
Australia

Submission method: By upload

Dear Mr Thorpe

Re: Exposure draft of the Trusted Digital Identity Bill and related legislative instruments

The Australian Financial Markets Association (AFMA) welcomes the opportunity to comment on the Exposure draft of the Trusted Digital Identity Bill and related legislative instruments. AFMA's membership of over 110 financial market participants delivers the whole range of financial services, including identity management services, to both the public and private sectors.

AFMA works with our members to promote efficiency, integrity, and consistency in financial market practices. We thus welcome the expansion of the digital identity system to the private sector and states and territories that encourages standardised approaches to identity verification.

We suggest reading our comments below in conjunction with our submission in July 2021 to the Positions Paper as we restate some of our outstanding concerns.

AFMA Comments

Privacy Safeguards

We note and support the intention of the legislation not to capture all digital identity frameworks. In such cases, the Privacy Act will provide a standardised set of expectations around privacy safeguards for all entities across the economy.

More generally we are cautious about fragmenting privacy legislation across multiple Acts. The additional privacy safeguards proposed for the scheme in the draft legislation, particularly in relation

to consent requirements and biometric information should align with the potential changes to broader privacy protections following the government's review of the Privacy Act.

The Bill should also seek alignment with the Privacy Act in other areas as noted below.

The Bill should require Identity Service Providers and Credential Service Providers to take adequate steps to make sure the user information is collected promptly and is correct, up-to-date, and complete, after a user request.

Further, the recently released discussion paper on the government's Review of the Privacy Act considers individuals' right to erasure of their personal information¹. We note that given competing stakeholder views about the benefits and challenges of introducing such a right, the Review is seeking further feedback on the most appropriate means of introducing it that would provide individuals with greater control over their personal information without negatively impacting other public interests (such as the obligation to retain data for legal or business-related purposes). While such erasure rights could be introduced as a safeguard in addition to strengthened consent requirements, in line with our comments above, the DTA should align these considerations with the outcome of the Review.

Cyber security

AFMA suggests the DTA reconsider the requirement under the TDIF Accreditation Rules for accredited parties to provide their security policies to the Oversight Authority for review on an annual basis. In support of consistency and efficiency, there may be an opportunity for the DTA to align this requirement with assurance requirements already in place under other data sharing regimes.

We also note that financial institutions undertake several information security compliance reviews and audits both as good practice and in response to existing regulatory requirements. The Bill should consider cross-referencing these prevalent regulatory obligations where appropriate and ensure it is not creating inefficient burdens by placing duplicative requirements on entities.

To increase knowledge sharing, AFMA would encourage the establishment of a forum whereby participants of the Digital Identity system can better understand and monitor evolving cyber threats. We note the Department of Home Affairs has established a renewed Trusted Information Sharing Network (TISN) engagement platform under the Cyber and Infrastructure Security centre and a similar platform could be formed for the Digital Identity system.

Relying Parties

In our previous submission, AFMA had noted that it does not support the legislation allowing relying parties to apply to the Oversight Authority to on-board to the system without TDIF accreditation. This

¹ Privacy Act Review – [Discussion paper](#), October 2021

was so that relying parties are subject to the same standards around data management and preventing misuse of data since they will have access to users' sensitive personal information.

The same data should have the same protections. We have previously raised similar concerns in relation to the Consumer Data Right (CDR). Schemes such as CDR and TDIF should not create potentially lower security points of potential data exposure as this could result in challenges to scheme confidence in the event of a leak from the weaker security points.

We suggest that relying parties be subject to the information security requirements in the Accreditation Rules. This will ensure there is standardised treatment when it comes to information security requirements for all participants in the Digital Identity system. The additional privacy safeguards that the Bill introduces for all accredited entities should also apply to relying parties.

Liability and Redress frameworks

We note that the Oversight Authority will have the ability to potentially direct Accredited participants to have adequate insurance arrangements in place as part of their accreditation requirements. This is so they have appropriate protection from identity fraud and cyber security incidents. AFMA supports that all participants that apply to be on-boarded to the Digital Identity system should maintain sufficient capacity to cover potential liabilities that might arise under the scheme, this could include coverage via insurance or by having sufficient reserve capital etc.

Access to Data

The Bill provides the Oversight Authority with the ability to allow a participant to access restricted attributes. AFMA suggests that as a condition for granting that access, the Oversight Authority should also require participants to expressly provide the precise business need for requesting a restricted attribute. If a business need to access the actual data of a restricted attribute is not deemed appropriate, the Oversight Authority should consider establishing an ability for participants to query a user's identity (i.e. their age), rather than accessing specific details of a restricted attribute (such as date of birth).

Trusted Digital Identity Advisory Board

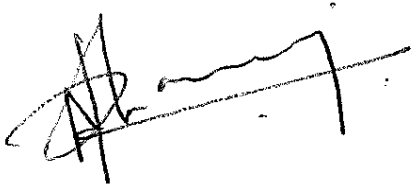
AFMA supports the establishment of an Advisory Board to advise the Oversight Authority on its exercise of powers under the Act. We highlight that the Board should seek to consider and balance various industry issues and concerns when providing advice to the Oversight Authority.

To support transparency, AFMA considers that decisions of the Advisory Board should be published, including occasions where the board fails to reach consensus on specific matters. Particularly, participants in the digital identity system should have visibility of any recommendations that relate to new rules and standards that may rise over time due to technological developments.

Additionally, AFMA supports that the decisions of the Oversight Authority should reference advice provided by the Advisory Board, and where decisions contradict that advice, the Oversight Authority should provide a rationale for departing from the advice provided.

Please feel free to contact us for more information via the Secretariat.

Yours sincerely

A handwritten signature in black ink, appearing to be 'Nikita Dhanraj', written over a horizontal line.

Nikita Dhanraj
Policy Manager