Australian Banking Association

ABA submission: Digital identity legislation position paper

The Australian Banking Association (**ABA**) welcomes the opportunity to provide a response to the Digital Transformation Agency (**DTA**)'s consultation on phase 2 of Australia's digital identity legislation. The ABA advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

ABA reiterates our view that there is significant potential economic benefit in the government's digital identity initiative for consumers and businesses. ABA also reiterates that the ability of a government digital identity system to achieve wider adoption, and therefore realise the potential economic benefits of this government policy, will likely depend on factors such as clarity of legislative framework, flexibility to innovate and incentive to participate, implementation of data and privacy safeguards, and clarity and effectiveness of governance arrangements.

Scope of legislation and disincentive to accredit or participate

ABA understands the key change in this position paper is how the legislation would apply to transactions and entities, set out in chapter 5 of the position paper.

Previous stages of consultation indicated the legislation would apply to transactions conducted within the government digital identity system. Chapter 5 of the position paper now indicates the legislation would apply a digital identity created by an entity that is accredited (refer to Figure 4). ABA also understands that, if an identity provider (**IDP**) and exchange are both accredited, and the two entities undertake a digital identity transaction, the transaction would be subject to legislation *even if the two entities intend to conduct the transaction under another digital identity scheme* (refer to Figure 8).

ABA considers this application of the proposed digital identity legislation is too broad. In particular, this proposal would be likely to disincentivise the private sector from becoming accredited or participating in the government identity system because:

- The proposed digital identity legislation would apply to digital identity transactions that are intended to be done under a private digital identity scheme, even if this is not the outcome intended by the user, IDP, relying party (**RP**) or exchange.
- The proposed legislation may impose requirements that are incompatible with a private scheme. Even if there is no immediate inconsistency, this outcome creates the risk of inconsistency or conflicting requirements in the future.

An IDP, RP or exchange can mitigate the risk of legal inconsistency if the entity does not apply for TDIF accreditation or participate in the government digital identity system. In other words, choose between participating in the government system, or participating in any other private digital identity scheme.

ABA believes this would be a sub-optimal outcome. It is likely to create fragmentation between government and private sector digital identity schemes, and may reduce the widespread adoption of the government digital identity system.

Proposed amendment

ABA asks the DTA to consider including a mechanism in legislation that would ensure the legislation does not apply to digital identity transactions that are intended to be conducted under another digital identity scheme and not under the government digital identity system.

The scope of legislation should be as set out in the table below. The legislation currently applies to scenario 3 but should be amended so it does not apply.

Scenario	Accreditation/participation	Transaction	Subject to legislation
1	IDP and exchange are participants in government system.	A transaction is intended to be conducted under the rules of the government system.	Yes
2	IDP and exchange are accredited and participating in government system. These entities are also part of a private digital identity scheme. RP has been accredited to the TDIF and understands that it will be subject to TDIF rules and liability approach.	A transaction is intended to be conducted under the rules of the government system.	Yes
3	IDP and exchange are accredited and participating in government system. These entities are also part of a private digital identity scheme. RP has been onboarded to the private scheme and understands that rules and liability will be defined by that private scheme.	A transaction is intended to be conducted under the rules of the private scheme.	No
4	IDP is accredited and participating in government system. Exchange is not accredited in government system. These entities are also part of a private digital scheme.	A transaction is intended to be conducted under the rules of the private scheme.	No
5	Exchange is accredited and participating in government system. IDP is not accredited in government system. These entities are also part of a private scheme.	A transaction is intended to be conducted under the rules of the private scheme.	No

Legislation could, for example, expressly provide that legislation does not apply if a transaction is conducted under another digital identity scheme, or allow participants to 'opt out' of the legislation for individual transactions or a class of transactions, on the basis that the transaction will be conducted under another digital identity scheme.

This proposed change is likely to require consequential changes to definitions and subsidiary instruments. For example, the definition of a digital identity (as an identity that is generated by an accredited participant) is too broad, as is the proposed definition of a digital identity system. The provisions about use of trustmarks may need to be reviewed.

Additional comments

Technology neutrality

ABA strongly recommends ensuring the legislation is technology neutral and principles-based as much as possible, to allow for flexibility and future proofing. This means, for example, avoiding describing the

digital identity system by reference to technology components and elements (as this may anchor the system to a particular technology approach) or by reference to a government exchange (as this could anchor the provision of identity to one exchange). It also means ensuring legislation describes the regulatory outcomes that government is seeking to achieve, rather than prescribe the use of particular technology or a technology or operational process for achieving the outcome.

Oversight authority having class exemption powers

In a number of places in the position paper, the Oversight Authority (**OA**) is proposed to have the power to exempt a participant from specific obligations.

ABA reiterates our view that some privacy safeguards and data protection proposals can conflict with existing legislative requirements, which may apply more broadly to a class of participants and not just to individual participants. As such we seek confirmation that the OA will have the ability to provide exemptions to a class of entities, and not just provide individual exemptions. ABA also proposes that the digital identity legislation create a presumption in favour of an exemption being granted where the applicant can demonstrate a possible conflict with other legislation, for example, potential requirements relating to suspicious transactions or fraud prevention.

ABA also reiterates our proposal that the OA should be able to give an exemption from the requirement to seek user consent to access restricted attributes, if a participant can demonstrate that they are required or authorised by law to collect this information for a particular purpose. This exemption can be written in the Rules.

Role of OA

ABA refers to our previous submissions and asks the following questions.

- The OA is proposed to have the function of 'approving the information made available through the system'. We seek clarification on what information can be made available and whether information can be made available to government or non-government third parties. We also ask for the details of any assessments of this proposal's impact on consumer privacy and participants' privacy obligations. We also seek further information on the OA's liability if data is made available through the system when it should not be, and whether this could give rise to any liability for participants.
- We believe there may be an appropriate role for the OA to deal with incorrect or 'dirty' data. We would appreciate DTA considering this issue further, and consider whether this could be part of the OA's role to 'improve the system'. If the OA will not have such a role, we seek further information about how the liability framework may apply and which entity would have responsibility to correct 'dirty' data.
- The proposed legislation would permit the OA to coordinate the sharing of information between participants to support each other in managing cyber security and fraud incidents. We agree that robust cyber security will play a crucial part in ensuring the system is sound and retains consumer confidence and encourage the DTA to work closely with the Australian Cyber Security Centre on this issue. We seek further information about the way in which data will be shared and used amongst participants, as this can also have an impact on users' privacy and the privacy obligations of participants.
- We would like to seek clarity on the OA's role in complaints handling: will the OA have a centralised complaints handling mechanism, and will data about complaints be shared so participants and users have visibility over common themes and volumes?

Investigation of data breaches

The legislation will build upon the notifiable data breach scheme in the *Privacy Act 1988* (**Privacy Act**) and require accredited participants to provide a copy of any data breach relating to the digital identity system given to the Office of the Australian Information Commissioner (**OAIC**) to the OA as well. While

the Position Paper explains that the OAIC alone will have sole investigative power in relation to a data breach, it also notes that the OA will have the power to take administrative action against an Accredited Participant in response to a notifiable data breach.

To avoid duplication, the legislation will need to make it clear that any investigation of a data breach, including breaches relating to the digital identity system, is a matter for the OAIC alone. Further clarity is needed on the difference between the administrative action that the OA can take against an accredit participant in relation a data breach, and enforcement action the OAIC may take.

In relation to a data breach that affects multiple accredited participants, the legislation will need to be clear as to which of the entities is required to notify the OA. The legislation should also specify that any exceptions to notification under Part IIIC of the Privacy Act also apply to notification of the OA. Given these questions, ABA continues to see merit in the OAIC being the OA.

Accreditation

ABA notes the legislation will now apply to entities that are accredited to TDIF or participate in the government digital identity system. Under this proposed arrangement, ABA still believes that participants will and should be required to check that an RP is accredited, before sharing data. This would still require the OA to ensure the accreditation register is kept up-to-date as close to real time as possible, to minimise the risk of a transaction being undertaken after a participant has been offboarded but before the register is updated. For example, if a participant is offboarded on Friday evening but the register is not updated until Monday, a number of transactions may occur over the weekend with participants being put in an adverse position.

ABA also seeks clarity on whether exemptions granted to participants will be able to be viewed on the register.

Pricing

ABA supports the proposed pricing principles allowing providers to set prices for non-standardised services based on market principles (for example, provision of certain credentials).

Liability

ABA seeks more information about the implications and/or details of the following proposals.

- Certain rules may be designated as enforceable rules and subject to civil penalties. We ask the DTA to conduct more detailed consultation on which provisions may be designated as such.
- The proposal that, where an accredited participant fails to comply with the rules and has failed to act in good faith, the participant would be liable for loss and damage suffered by all participants flowing from that non-compliance. This proposed regime has the prospect of imposing unlimited liability on the accredited participant who fails to comply. ABA believes further work is needed on the liability regime, including whether it may be preferable to leave the allocation and quantification of loss and damage to general contract law.
- The proposal that some obligations under legislation will continue to apply to an offboarded participant, and the participant would continue to be subject to the OA's directions and powers in connection with its role so long as it holds information in connection with the system. We ask legislation and/or rules to specify which obligations will apply when a participant is offboarding and after a participant has offboarded. Specifically, whether the offboarded participant would continue to be subject to civil penalties and the liability framework for events that happened while they were an accredited participant.
- ABA also seeks clarity on the interplay between civil penalties and the liabilities framework.

Obligation of relying parties

ABA considers RPs should be subject to an adequate set of minimum obligations that protect users' data and the security of the digital identity system, while respecting the need to ensure RPs do not face unnecessary hurdles to participate in the system.

We propose that RPs should be required to undergo TDIF accreditation, and breach of obligations should lead to deregistration and de-accreditation, and potentially civil penalties depending on the nature and severity of the breach. We also ask DTA to consider whether RPs should be subject to obligations relating to data retention and protection, and cyber security insurance. This would protect users' data and maintain user confidence in the system.

We also propose that the OA should ask RPs to identify what data they need to meet regulatory or commercial obligations. Consistent with the data minimisation principle, RPs should not be able to access data they do not need.

Deregistered ID

ABA reiterates our comment from a previous submission that RPs may need to be able to continue to rely on, and retain information relating to, a deregistered digital identity. We ask that the legislation accommodate such reliance and retention or for the OA to have the ability to grant an exemption in such circumstances.

Privacy Act / biometrics / digital identity information

ABA supports robust privacy and consumer safeguards in the digital identity system.

ABA continues to highlight the need for harmonisation between digital ID legislation and the amended Privacy Act, and the digital identity legislation relying on existing legislation as much as possible. ABA welcomes the feedback that DTA and the Attorney-General's Department are in discussions about the proposed digital identity legislation and the Privacy Act review.

In addition ABA:

- Seeks further clarification about how biometrics will be dealt with under Privacy Act and the digital identity legislation. We also note that financial institutions may have obligations that require the financial institution to retain information about the authentication and use of a biometric.
- Seeks clarification whether 'sensitive attributes' will align with requirements for sensitive information under Privacy Act.

The definition of Digital Identity Information in legislation will not be exhaustive, and further detail would be set out in the rules. ABA highlights that the rules do need to be specific and exhaustive about the personal information attributes that constitute Digital Identity Information, so participants have certainty about what is subject to legislation. This is particularly important given the introductions of civil penalties for contraventions of various safeguards in the proposed Bill. Consideration should be given to other exhaustive definitions in the Privacy Act, including for 'sensitive information' and 'credit information'.

ABA has previously provided submissions about how the digital identity system may change how large organisations validate identity within the digital identity system: currently an organisation may conduct validation of identity internally with limited disclosure to an external provider (for example to verify a drivers licence number). We would welcome clarification from the DTA or OAIC about how much more data will be disclosed and captured in the proposed system, and what additional notification may be necessary to consumers in accordance with APP 5, Privacy Notices.

Consent and restrictions on data profiling

ABA seeks clarification that the policy relating to consent, as described in the position paper, would allow participants to seek time bound ongoing consent or multiple use consent. We also seek clarity which of the accredited participants involved in the authentication of an individual's digital identity

attributes is required to obtain and manage consent, which may also include enabling an individual to withdraw consent.

ABA expresses concern that the description given in the position paper, that a user can tick a 'do not display next time' box and provide non-time bound ongoing consent, is not best practice.

The legislation would also prohibit accredited participants from using attributes and other information obtained from the digital identity system for prohibited purposes, even with an individual's consent. The prohibited purposes will include 'unrelated marketing'. The meaning of unrelated marketing as explained in the Position Paper is not clear. Given a contravention of these rules is punishable by civil penalties, further clarity as to the meaning and scope of the prohibited purposes is needed.

ABA also queries whether users should be able to consent or opt in to share data for marketing.

Default minimum age (15 years)

ABA has previously indicated that the proposed minimum age for using a digital identity does not align with the minimum age for providing certain services or purchasing certain goods (for example, a minimum age of 16 for opening a bank account; minimum age of 18 to purchase alcohol). As such, ABA asks legislation to clarify that the minimum age for using a digital identity does not require any entity to provide another services, if the entity has specific rules about the minimum age for accessing that service or are subject to legislation about minimum age. ABA also asks legislation to clarify that a 15 year old has capacity to consent in their own right to the processing of their personal information for the purposes of the system.

Meta-data and activity logs

ABA has previously raised questions about the definition of metadata and activity log, and reiterate those questions. We also ask DTA to consider whether these terms should be consistent with existing legislation that may impose requirements relating to meta-data. ABA also asks legislation to avoid, or in the alternative resolve, inconsistencies that may be identified in record keeping obligations, for example, whether the digital identity legislation would overrides Privacy Act record keeping obligations for biometric information, metadata and activity logs. Any differences in definition and/or record keeping requirements would be suboptimal and should be clearly set out in subordinate rules.