Australian Banking Association

Australian Banking Association submission – digital identity legislation

Summary

Australian Banking Association (ABA) welcomes the further opportunity to provide input to the consultation on the exposure draft legislation and draft rules for the proposed government trusted digital identity system (the System). 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 welcomes the engagement from the Digital Transformation Agency (DTA) during the development of policy, and in particular thanks the DTA team for its engagement during this consultation.

ABA reiterates our view that there is significant potential economic benefit in the government's digital identity initiative for consumers and businesses. The development of both government and private sector digital identity systems is needed to achieve wider adoption, and therefore realise the potential economic benefits of this government policy. That will continue to depend on whether the proposed legislative framework provides clarity, ensures robust privacy safeguards for users, provides flexibility to innovate and incentives to participate, while minimising the potential for conflicting or inconsistent data and privacy obligations for participants.

The key issues addressed in this submission are:

- the scope of the legislation and its impact on a participant's use of digital identities outside of the System;
- privacy, access to data and data security, aligning obligations under the proposed legislation and the *Privacy Act 1988* (including changes proposed in the Privacy Act Review Discussion Paper, issued on 25 October 2021);
- the need for clarity on whether a bank can be a participating relying party in the System while complying with its obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF);
- the need for clarity of the legislation's requirements; and
- ensuring legislation does not prevent participants from offering a smooth user journey, especially when a user is moving between the System and other regimes such as the Consumer Data Right.

Detailed submissions

Scope of legislation

Issue	Comment
Impact on accredited participants	While section 14 of the exposure draft Bill states the Bill applies to the trusted digital identity system, the legislation can also be read as applying broadly to 'digital identity systems' of an accredited entity. A private sector entity may choose to become accredited to use the trustmark as a marketing initiative with consumers. The Bill will directly regulate private sector entities that choose to become accredited under the TDIF accreditation scheme. ABA seeks clarity whether the Bill will regulate the entity's provision of the accredited facility, including its provision within a private sector digital identity verification solution, and how the Bill may apply where the entity provides the accredited services within the TDIS or within another digital

	identity system. ABA understands the policy intent is that data collected on an accredited facility of an IDP would be governed by the legislation, however this distinction is not clear on the face of the Bill.
Impact on internal use of digital identity or participation in other systems	Subject to the clarification sought above, ABA is concerned the exposure draft Bill may have broader impact than intended and could be sufficiently broad as to apply to (for example) a bank's use of an identity verification system to provide online banking to its customers. If the exposure draft Bill is intended to allow a participant to distinguish the offering of a digital identity in the System, from an entity's own customer verification processes and/or its participation in another digital identity system, ABA would welcome clarification about how this could occur and governance requirements. Also refer comments immediately above.
Application to acts and omissions outside Australia; data sovereignty rule	The exposure draft Bill will apply extra-territorially to acts and omissions outside of Australia. Refer to comment below about TDIF Rule requirement to keep data in Australia.
Know-Your-Customer (KYC)	It may not be possible for a bank to rely on digital identities generated under the trusted digital identity system while complying with AML/CTF obligations. This means banks could be relying on digital identities generated through the TDIS as relying parties. Sections 37A and 38 of the AML/CTF Act allow entities to rely on customer identification procedures of third parties in certain circumstances. For ongoing reliance, the Act requires a written arrangement and reasonable grounds to believe that the third party has appropriate systems and controls to meet the requirements of Chapter 7 of the AML/CTF Rules. Some IDPs in the system, such as the MyGovID solution, are not covered by the AML/CTF regime and hence could not be relied on by banks. Given blinding of transactions within the TDIS, it would be difficult for banks to know when they would be able to rely on a digital identity provisioned through the TDIS for onboarding a customer. ABA understands this matter may go beyond the scope of the exposure draft Bill, and urges DTA to continue engagement with AUSTRAC and relevant policy agencies.

Privacy and access to data

Issue	Comment
Alignment with Privacy Act Review	ABA notes the Government has released a further discussion paper as part of its review of the Privacy Act. In the time available, ABA has not been able to compare the exposure draft Bill and the proposals of the Privacy Act Review Discussion Paper. ABA urges the DTA to continue close engagement with the Privacy Act review to ensure alignment between the privacy safeguards in the exposure draft Bill, and amendments that may be considered to the Privacy Act, to the maximum extent possible.
Existing obligations under Privacy Act	ABA also notes the following existing obligations under the Privacy Act and/or Consumer Data Right:

and/or Consumer Data Right	○ Obligation to take reasonable steps to ensure user information is accurate, up to date and complete, and also correct data in a timely manner following a user request. Refer the credit reporting framework in Part IIIA of the Privacy Act and Privacy Safeguards 11 and 13 under the Consumer Data Right. ○ Obligation for recipients of unsolicited user data to destroy the data as soon as practicable. Refer Privacy Safeguard 4 under the Consumer Data Right.
Retention of information	Section 132 of the exposure draft Bill requires an entity to destroy or de-identity personal information obtained through the trusted digital identity system that it is not required to retain under the Bill or another law. The Bill does not appear to expressly permit retention of personal information for any purpose. Further clarification is needed: ○ When an entity is permitted to retain personal information; ○ whether a digital identity is personal information; ○ whether a participating relying entity can continue to rely on a digital identity that has been deactivated or deleted. If not, how will the entity know the identity has been deleted or deactivated? Further, section 61 of the exposure draft Bill requires the deactivation of a digital identity on request of the individual. Does this require the entity to delete the digital identity?
Retaining data for testing	We propose that the power in the Bill to retain data for the purposes of testing should only be applicable if it is accompanied by a requirement for the affected individual's express consent.
Expansion of the concept of personal information	The expansion of personal information adds significant complexity to the privacy related requirements in the exposure draft Bill. For example, the requirement to seek consent to handle the personal information of deceased individuals can create practical difficulties for the participant and for the family or estate of the deceased. Also refer 'Notifiable data breaches', below. ABA reiterates our call for alignment between the exposure draft Bill and the Privacy Act. To the extent differences remain, ABA asks DTA to consider whether legislation can be clearer about the differences between the concept of 'personal information' in the exposure draft Bill and under the Privacy Act, how each concept applies and the impact on the scope of regulatory obligations. This is particularly important given the crossovers between the two pieces of legislation.
Notifiable data breaches	The requirement to provide notification of data breaches is an area where the expanded meaning of personal information, and additional requirements under draft rules, adds complexity. ABA asks DTA to consider the scope to align with the Privacy Act where possible. The expanded meaning of personal will require participants to consider additional categories of information when assessing whether an eligible data breach has occurred. The TDI rules and TDIF accreditation rules may require the notification of additional types of incidents (such as a cyber security incident). ABA asks the exposure draft Bill to clarify whether existing exceptions to the notification of data breaches, which exist in the Privacy Act, apply to the notification of data breaches under the exposure draft Bill.

	Finally, ABA asks for guidance or further information about how the reporting of such breaches will be operationalised, and the approach of the Oversight Authority to responding to these notices.
Enforcement under two privacy regimes	If an entity breaches an additional privacy safeguard under the TDI Bill, or a privacy related requirement in the TDIF accreditation rules, the entity may face investigation and enforcement action under both the TDI Bill and the Privacy Act. ABA seeks clarification: ◦ Whether individuals could make a complaint about the breach under the complaint procedures in the Privacy Act. ◦ Whether representative complaints that may be made under the *Privacy Act* cannot be made in relation to a breach of the additional privacy safeguards in the exposure draft Bill. ◦ Dual or overlapping investigations and enforcement actions cannot be carried out in respect of the same contravention under the draft Bill and the Privacy Act (including the power to seek civil penalties of up to $2.2m per contravention for serious or repeated interferences with an individual's privacy). In the interests of regulatory certainty, ABA: ◦ proposes that a breach should be dealt with under one, not both, of these regimes. ◦ seeks clarity whether breaches of the additional privacy safeguards in the Bill should be dealt with using the compliance and enforcement powers under the Bill, and not also the powers available to the Information Commissioner under the Privacy Act. ◦ Also seeks confirmation the Oversight Authority would enforce compliance with the privacy rules in the TDIF accreditation rules.
Prohibition on certain marketing purposes	ABA asks for further clarification in legislation or rules, supported by guidance, about what is covered by the definition of 'marketing' at section 82(1) of the exposure draft Bill. Greater clarity is needed as to the scope of the prohibition under section 82 and how it applies to arrangements and activities in various sectors. ABA also understands accredited entities can use data to promote the services for which they are accredited if the individual has consented to this. We ask legislation or the Oversight Authority to clarify how this may apply in the case where the individual has given consent to an accredited data recipient in order to receive recommendations on suitable services.
Deletion of biometric information	Query if section 79 of the exposure draft Bill applies to biometric data templates. These templates are used to verify biometric information or authenticate an individual's digital identity. It is unclear how an entity can authenticate a digital identity after it has deleted biometric templates. If *retention* is permitted in order to allow an individual to *authenticate* to their digital identity account, ABA asks legislation to state that retention for this purpose is permitted and under what circumstances it can occur.
Express consent	ABA asks for confirmation that the concept of express consent is the same as the concept under the Privacy Act. ABA also asks the Oversight Authority to release guidance or examples on obtaining express consent for verifying or authenticating an individual, including where mechanisms for consent may already exist.
Reportable incidents	Outside of its information sharing powers under section 17 of the Rules, greater clarity would assist regarding whether the Oversight Authority has the power to determine whether an eligible data breach has occurred in relation to certain reportable incidents. Does the Oversight Authority have a

definition or guidance on its approach to determining ‘awareness’ of reportable incidents?

Access to data and Relying Parties

Issue	Comment
Access to verification of data instead of raw data	Under the draft legislation, the Oversight Authority is given the authority to allow a participant to access restricted attributes (after considering the matters at s 23(2) of the Bill). In making its determination, the Oversight Authority should also develop objective conditions on which a participating relying entity would be approved for accessing these restricted attributes. The development of these criteria should be done in consultation with the OAIC, which is the regulator for privacy-related matters under the legislation The Oversight Authority should create an ability for participating relying entities to request assertions about a user’s identity, as opposed to requesting the user’s full identity details (including name, date of birth and address). A current example is the Service NSW COVID-19 check-in app: when a vaccination certificate is linked to the app, upon checking in the app can show that a certificate has been provided (ie, a yes/no answer) without further information about the customer. This is an example of digital ID being used in a way that is privacy-preserving.
Obligations of relying parties	As participants in the digital identity ecosystem, relying parties will have access to and handle sensitive personal information. For example, a merchant could have access to and handle personal information about bank customers. To maintain system security, and to maintain consumers’ trust in using digital identities, we ask the Government to consider applying consistent information security requirements to all participants in the ecosystem. This means relying parties should be required to comply with the information security requirements contained in the Accreditation Rules. As the Bill introduces additional privacy safeguards for participants in the digital identity system, also consider applying restrictions on data profiling and the disclosure of data for marketing purposes to relying parties.

Cyber security, liability insurance, notification

Issue	Comment
Audit	The Accreditation Rules place a requirement on the Oversight Authority to annually review the security policies of accredited parties to ensure they are compliant with the Rules. Rather than an annual review of paper-based policies by the Authority, it is recommended that the same approach as the Consumer Data Right be adopted. That is, allowing accredited parties to provide an assurance report, in accordance with ASAE 3150 (Standard Assurance Engagements, Assurance Engagements on Controls) or a similar industry-specific standard (e.g. Australian Prudential Regulation Authority’s Information Security Prudential Standard CPS 234).

Incident reporting	Incident reporting requirements should be aligned with (to the extent possible) existing regulatory and industry obligations such as the Notifiable Data Breaches Scheme provisioned within the Privacy Act and CPS 234.
Enhanced collaboration	The Trusted Digital Identity Rules should provide for more collaboration amongst participants on the monitoring of cyber threats through the creation of forums, whereby participants can share in real-time threat activity and information. Also consideration should be given as to whether this can be done in conjunction with other government cybersecurity initiatives to avoid duplication of regulation, for example, any work undertaken by the Department of Home Affairs Cyber and Infrastructure Security Centre.
Liability insurance	Consider whether all participants seeking to be onboarded to the digital identity system should be required to maintain adequate liability insurance. The current proposal is that the Oversight Authority has the ability to direct an accredited entity to have adequate liability insurance in place; however, a preferable approach is to extend this to relying parties. This is because, as participants in the System, there is a case that relying parties should have adequate insurance against potential liabilities to give other participants confidence to participate.
Duplicate notification	Sections 43 and 44 of the Bill may act together to require multiple notifications to an individual relating to the same incident, which may be undesirable from that individual's perspective. Enabling one notice to meet the requirements under both sections would be preferable.

Definitions

Issue	Comment
Clarification of key terms	There are areas of the proposed legislation that may benefit from further definition, for example, digital support, deactivation, support services, acceptable service levels/NFRs, and interactions with other participating members. Several terms used in the legislation are not defined, or have a definition which is unclear for some purposes. For example: ○ A digital identity does not appear to be an 'attribute', but this isn't expressly stated. ○ 'Verification' and 'authentication' are not defined. ○ It is unclear whether 'point of contact' (s 43 of the Bill) includes a channel. ○ 'Unique identifier' (s 75) is not defined. ○ 'Credential' is not defined. ○ 'Valid terms' (rule 2.1 of Chapter 5 of the Accreditation Rules) is vague.
Interoperability	This term can have specific meaning in terms of technology/systems. ABA seeks confirmation that this term is intended to refer to the requirement that accredited participants and relying parties must not refuse to provide services to other participants or relying parties, and there is no additional technical meaning or requirement for interoperability (ie, interoperability between this ID system and other ID systems).

Draft TDIF Rules

Issue	Comment
Storage and handling of digital identity information outside Australia	The policy rationale for prohibiting an entity from storing or handling digital identity information outside Australia is not clear. Entities presently store and handle information of a sensitive nature outside of Australia and do so securely. On a technology level, this requirement can cause problems for entities that seek to use cloud service providers, as our understanding is that many commonly used cloud service providers (including those that will be regulated under proposed amendments to the Security of Critical Infrastructure Act 2008) are able to ensure resilience of their cloud services by maintaining servers in different regions, so that client data can move between servers if there is an outage or other issues with a server in Australia. If this rule is retained, suggest the exposure draft Bill can enables the Oversight Authority to make exemptions to this general rule on a class basis where reasonable controls can be implemented to protect the data.
Reportable incidents	ABA asks DTA to consider streamlining and aligning the reporting requirements under this proposed regime, with those of other regimes. One approach would be to limit reporting to fraud and security incidents only, or to provide an exemption where the Oversight Authority can obtain information from other regulators and thus maintain visibility.

Draft Accreditation Rules

Issue	Comment
Penetration testing	It is unclear how entities should conduct penetration testing (required by clause 7.5 of Chapter 4 the Accreditation Rules) in a way consistent with the requirements of the legislation.
Duplication with prudential obligations	It is likely that the TDIF Accreditation Rules will overlap with some prudential requirements, including the rules relating to protective security (which will likely overlap with elements of CPS234). ABA would welcome a clear mechanism for the Oversight Authority to accept documents produced for other purposes in legislation or guidance.
Privacy	The privacy compliance requirements in the TDIF Accreditation Rules are specific to accredited digital identity services and will need to be designed specifically to cater for the expanded scope of personal information under the TDI Bill. ABA reiterates earlier comments about aligning and streamlining privacy obligations under this regime.