Australian Banking Association

Response to Digital Transformation Agency (DTA) digital identity legislation position papers

Summary

Australian Banking Association (ABA) welcomes the opportunity to respond to the DTA's digital identity legislation position papers. ABA agrees there is significant potential economic benefit in the government's digital identity initiative for consumers and businesses. ABA agrees with the foundational position that the government will not seek to implement a single 'Australian' digital identity, and instead will establish a government digital identity system that can co-exist and interoperate with other digital identity systems.

The field of digital identity is a rapidly evolving one. 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 (including interoperability with other digital identity systems), flexibility to innovate and incentive to participate, security of protections for data and privacy, and clarity and effectiveness of governance arrangements. ABA also highlights that in order to incentivise adoption, digital identity should be no more onerous to use than other methods of identity verification, provide a good user experience, and be adaptable to participants' and users' needs.

ABA's response elaborates on these issues.

Data, privacy, cyber security

ABA strongly reiterates our view that DTA should carefully consider what is necessary to be placed into digital identity legislation relating to privacy and protections. This point can affect user experience and potentially the adaptability of the regime, as much as implementation costs for participants.

ABA agrees that the digital identity system needs to have strong protections for privacy and data so as to maintain consumer confidence in digital identity and the digital economy more broadly. Cyber security is a critical component of privacy protections. Choice for users and inclusive web design are also welcomed. However, digital identity cannot be considered in isolation, a successful digital identity system will be used as an option to access other services and by broad sectors of the economy. As such digital identity privacy protections needs to align and not conflict with other Commonwealth, State and Territories legislation, or existing programs and services relating to privacy and cyber security.

Duplicative or conflicting requirements will add complexity for participants in the digital identity system without necessarily adding meaningful protection for consumers. Complexity – including the complexity from navigating overlapping privacy regimes – can disadvantage smaller participants who may not have the same resources to ensure compliance with the regime. Unnecessary complexity can deter businesses from relying on digital identity, if doing so becomes significantly more complex than relying on existing ways of verifying customers' identity. Complexity can also weaken consumers' ability to understand what protections apply to them, when they engage with the digital economy.

From this perspective, the ABA is concerned a number of proposals in the position papers relating to privacy:

- duplicate and in some instances conflict with existing legislation, particularly the *Privacy Act 1988* (Cth) (Privacy Act), the privacy protections under the consumer data right (CDR) regime, and anti-money laundering and counter-terrorism financing legislation.
- duplicate existing programs or regulatory obligations for some or all participants.

ABA asks the DTA to specifically consider, for each proposal, to what extent additional protections beyond the Privacy Act are required. Where specific protections are required, ABA recommends the digital identity legislation:

- contain a mechanism to fully harmonise with, cross-refer or otherwise rely on an existing privacy regime, and to provide exemptions from the digital identity legislation where participants are required by another legislative or regulatory obligation to treat data differently;
- clearly avoid duplicated functions between the Oversight Authority (OA) and other regulators, particularly the Office of the Australian Information Commissioner (OAIC) and Australian Cyber Security Centre (ACSC), and consequently minimise duplicative reporting obligations and the lack of clarity about OA and other agencies' mandate; and
- allow participants to meet obligations under the digital identity legislation by complying with substantively equivalent obligations in other regimes such as prudential regulation.

Right to deregister a digital identity

The DTA proposes to provide individuals with statutory rights to voluntarily create and use a digital identity, and subsequently opt out of the system (through deregistration of the individual's digital identities). ABA understands the legislation is not intended to override existing Commonwealth, state and territories legislation, and believes this means legislation needs a mechanism to avoid conflicts or duplicative obligations.

The right to deregister a digital identity may have implications for an entity's functions and activities that rely on the verification of individuals' identities. RPs may need to be able to continue to rely on, and retain information relating to, a deregistered digital identity. In particular, the ABA asks DTA to consult AUSTRAC and the Department of Home Affairs about the extent to which the subsequent deregistration of a digital identity used for know-your-customer purposes may impact ongoing customer due diligence processes contemplated by anti-money laundering and counter-terrorism financing legislation.

Biometric information

The DTA proposes strong restrictions will be implemented on how biometric information can be used; when data profiling can occur; certain type of sensitive attributes. ABA supports strong consumer protection and privacy safeguards. However, given the existing protections in the Privacy Act, the ABA questions why additional restrictions are required.

If the digital identity legislation will contain specific requirements relating to biometrics, ABA provides further comments for DTA's consideration.

- The legislation should make it clear that any such enhanced rules apply only to the extent that the participants process biometric information for the purposes of the system, and not to any general processing of that information outside the scope of legislation.
- The legislation should provide a mechanism to address any conflict between the proposed requirement for identity providers and credential service providers to delete biometric information when the purpose for which it was provided has been fulfilled, and requirements under other legislation and regulatory regimes (existing or future) that may require participants to retain information about the authentication and use of a biometric. Under DTA's current proposal, the OA will be able to grant an exception where retention of such information is required for a longer period. ABA does not consider it be an efficient process for classes of entities to seek an exemption from the OA. A preferred approach may be that, as is the case under general privacy law, participants should be left to make their own assessments as to whether they are required or authorised by law to retain or destroy the biometric information, without the need to seek an exception from the OA. This would be consistent with the approach proposed in para 6.8 of the position paper (Record-keeping).
- The DTA's proposal to fix permitted and/or prohibited biometric modalities in primary legislation may stifle the development and uptake of emerging technology. If it is necessary to make rules as to what modalities can and cannot be used, these

permissions/prohibitions would be best dealt with in subordinate rules to allow for greater flexibility.

- The position paper references 'sensitive attributes'; The ABA seeks clarification is this is equivalent the management of sensitive information collection, storage, and disclosure under the Privacy Act.

Consent for use of biometric information

The DTA proposes that identity providers and credential service providers will be required to ask users for consent each time their biometric information is used. It will also be necessary to inform users as to the duration of the validity of their consent. It would be useful for the DTA or OA to provide guidance on the duration of consent validity, in consultation with participants, to provide participants with certainty as to their reliance on user consent.

In addition, ABA also proposes that legislation can provide for a better user experience if it allows users to set up time-bound ongoing consent (for example for 6-12 months, which could be withdrawn at any time) or a multiple use consent at their election (for example through a preference centre or when setting up their digital identity profile).

Restricted attributes

The DTA proposes to give the OA power to classify attributes as restricted attributes. Such yet-to-be-determined attributes will only be accessible to relying parties (RPs) who meet additional requirements. An RP may apply to the OA for access to restricted attributes, but only if a user first consents to such a disclosure. ABA provides two comments on this proposal:

- User consent to access a restricted attribute should not be a pre-condition to access. Giving users the choice to permit or refuse access to the restricted attribute would not be appropriate in circumstances where a participant is compelled by law to collect the relevant attribute.
- This proposal is likely conflict with existing law, if participants are required by another legislation or regulatory regime to collect information about restricted attributes. As such the digital identity legislation should not prevent participants from collecting restricted attributes where this is done in compliance with another legislative or regulatory requirement. In addition, the digital identity legislation should clarify any restrictions do not apply where participants collect restricted attributes outside of the digital identity system.

Requirement to conduct a Privacy Impact Assessment (PIA)

DTA proposes that accredited participants will be required to commission an independent assessor to conduct a PIA as a requirement of their accreditation. The requirement to commission an independent assessor to conduct the PIA should be optional, not mandatory. Sophisticated organisations, such as financial institutions, have the internal capability to conduct their own PIAs.

Acting on behalf of another

As a general principle, further detail is required on 'who owns identify' and on what basis can one individual validate the identify of another individual? Specifically, what are the requirements for acting on behalf of vulnerable persons?

Based on our experience with the CDR Rules, the ABA cautions against prescriptive rules which try to cater for every scenario – this is not possible and will likely create a 'laundry list'. The ABA recommends that legislation should be principles based and focused on prevention of consumer harm.

Specifically, the DTA proposes to provide a default minimum age of 15 years for use of a digital identity to obtain a service on the system. Consideration will need to be given to whether this aligns with banks' and other entities' own minimum age at which services can be acquired. If the legislation sets a default

minimum age, it should also 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.

Any specific requirements under digital identity legislation will need to fully align with State/Territories requirements for documents like powers of attorney. This also reinforces the advantage of a principles-based approach to digital identity legislation.

Further questions about privacy protections

- Para 6.1 of the Privacy and other safeguards position paper refers to elements of the small business exemption in the Privacy Act, which may be used for determining exemptions from the proposed rule to provide alternative identity verification channels. ABA seeks assurance that DTA is consulting with the Attorney-General's Department to stay abreast of any potential repeal of the small business exemption as part of the Privacy Act reform process.
- ABA notes that accessible and inclusive web design is standard practice for good user experience outcomes. It is unclear why this is required to be legislated.

Record keeping and meta-data

The ABA suggests that this aspect of the DTA's proposal requires further detail:

- What meta data fields are considered requiring to be kept?
- What is an activity log (what is it meant to capture)?
- What is the purpose of keeping meta-data and an activity log?
- Regarding the 7-year requirement to retain non-biometric records, who is retaining this data?
- For individual history log: does the information to be held at the individual level include the meta-data?

The ABA notes the statement '…the record keeping requirements are not intended to override Commonwealth or state and territory laws which already apply to the information', and highlights that there are existing protections in the Privacy Act and associated guidelines, in addition to the myriad of regulatory obligations for record keeping that already apply to FIs. The proposal of a retention period specific to Digital ID appears to conflict with existing Commonwealth or State laws. It becomes complex to determine which data/information that forms part of the digital identity is unique from information already collected and requires a separate legislative retention period.

Given this context, ABA queries what is the purpose of the record-keeping and what gap it is intended to fill. Instead, ABA reiterates our proposal for the digital identity legislation to defer or cross refer to existing obligations. Digital identity legislation may be appropriate where the DTA identifies gaps that the government considers, as a matter of policy, needs to be filled.

In addition, the ABA seeks clarity on what access will government entities have to individual's digital identity records?

Disclosure of data, data breaches

Data breaches: under the new legislation, accredited participants will be required to give a copy of a data breach notice (to the extent that the breach applies to the system) to the OA, in addition to the OAIC.

FIs are subject to a number of existing, and anticipated, regulatory obligations that require them to notify various regulators of data breaches. Further notification obligations are contemplated under the security of critical infrastructure reforms. The proposal to also notify the OA will further complicate the effective and expeditious management of data breaches. If notification of the OA is to occur, then any exceptions to notification set out in Part IIIC of the Privacy Act should also apply to notification of the OA. Further, the legislation should also make it clear that only one regulator (in this case, the OAIC) is

permitted to investigate, and take enforcement action, in respect of a data breach that affects the system.

Disclosure of data: ABA seeks further information about how the proposed 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 seek further details about how much more data will be disclosed and captured in the proposed system, and what additional disclosure may be necessary to consumers in accordance with APP 5, Privacy Notices.

Cybersecurity

Cyber breaches: the DTA proposes that the OA will have a role in relation to cybersecurity breaches. The digital identity legislation should not result in the fragmentation of information and reports about cyber incidents away from ReportCyber and the ACSC. The proposed obligations of participants to provide support for cyber attacks also duplicates existing organisations such as IDCare.

DTA also proposes to impose obligations on participants relating to cyber security, which can duplicate obligations that financial institutions are subject to under prudential regulation. A similar issue of regulatory duplication is being addressed under the Security of Critical Infrastructure legislation by introducing a mechanism that allows the SOCI Act to defer to sector-specific regulations about cyber security. ABA recommends DTA consult with the Department of Home Affairs as well as relevant sectoral regulators.

Governance arrangements

Industry representation

ABA supports the proposal for industry to have representation in governance arrangements.

It will be critical for governance arrangements to be genuinely open to private sector expertise on matters including cyber security. Governance arrangements will need to ensure rules and other administrative decisions consider impact on user experience and adaptability, and potential impact on incentives to innovate, within robust privacy and other consumer protections.

Establishing the rules and standards is only the first step in building a digital identity system. Since participation and use of the government digital identity system will be voluntary, the success or otherwise of the digital identity system will depend on whether consumers, businesses and other organisations have incentive to use and participate. This means ensuring, over the long term:

- the services delivering value: being easy to use, with capacity to improve and innovate to and respond to changes in technology and user demand
- consumer and businesses having confidence in security and protection of personal information and data, including from cyber attacks
- for RPs, the services being easy to integrate and use
- for identity service provider (IDP), the commercial returns from providing digital identity services being commensurate to the cost of building, integration and compliance. As indicated in the previous section, this will be in absolute terms and relative to other business opportunities including under other digital identity systems

These outcomes are more likely to be achieved if the governance arrangements and decision-making genuinely give due weight to private sector expertise, and have an objective of promoting commercial interests and incentives in a way that is consistent with government policy objectives.

Clarifications about OA

We also seek clarification about the role and liability of the OA. Note these issues can also impact on entities' assessment of the system's liability regime as a whole:

- the OA's proposed function of "approving the information made available through the system" – ABA seeks clarification on what information can be made available, whether to government or third parties, impact on consumer privacy and participants' privacy obligations.
- Whether there is an appropriate role for the OA to deal with incorrect or 'dirty' data, and whether this will be part of the OA's role to 'improve the system' as proposed in the liability position paper. If not how will liability to correct data be allocated?
- The OA's liability and role when it determines what information is made available through the system (as proposed in the liability position paper).

Also refer to comment below about the OA's role in relation to RPs and state/territories participants.

Clarity of legislative framework: interoperability and liability

ABA supports the overarching position that the government digital identity system will interoperate with other digital identity systems. The ABA understands the policy intention is that an entity may be a participant in the government digital identity system and in other digital identity systems.

Clarity about scope

It will be vital for the legislation to provide maximum clarity about when an entity and a transaction is subject to the digital identity legislation. The descriptions and diagrams in the position paper about scope and interoperability demonstrate the complexity that can face participants and consumers. ABA asks DTA to consider the issues below and consider conducting further targeted consultation on scope:

- Having a fail-safe way to determine whether a transaction is subject to the digital identity legislation will be crucial. If there will be 'blinding' of transactions, it will not be possible for participants to assess whether a transaction is subject to the legislation unless they can rely on information from the exchange or OA. Pushing uncertainty onto participants would create undue regulatory risk and can be a disincentive to participate. If the intention is for the status of the transaction to be made clear at the exchange level, this requirement should be imposed on exchanges under legislation or legally binding standards.
- If the register can be taken as proof that an entity is registered and a transaction is subject to the legislation, the register will need to be updated in a timely way. Since digital identity services can be provided 24/7, updating the register periodically (ie, weekly) or even at end of day can create a real risk that transactions will be performed on the wrong basis. Instead, a register may need to be updated as close to real time as possible following an OA decision to register or deregister.
- A related question is how liability will be allocated (including to the OA) if parties rely on the published register which contains incorrect information, and whether the allocation of liability would differ if the error came from the entity or was introduced by the OA. Similar questions may arise if an error is due to reliance on information from an exchange about the status of a transaction.
- ABA welcomes clarification from DTA that obligations under legislation would continue to apply to transactions conducted within the system, after an entity ceases to be registered with the OA. ABA also welcomes the clarification that the register will also provide historical records of which entities have been registered in the past but have had their registration revoked or they have sought removal themselves. These proposals should be made clear in the legislation.

ABA understands discussion are ongoing between DTA and state/territories governments about participation. ABA sees strong benefit in consistent adoption across jurisdictions and minimising differences in legislative and technological requirements. Banks have a strong track record of working with governments to deliver services or implement policy initiatives, and would welcome similar partnership and collaboration with governments on the next steps of this initiative.

Relying parties, state/territories participants

The Scope and Interoperability position paper states that RPs would not have to become accredited under the TDIF (p.10). Further clarity is needed around when a non-accredited RP would be able to access customer verifications from a TDIF-accredited provider.

Given there will be some obligations imposed on RPs (such as having to offer a choice of Identity Providers and minimum information security standards), an accreditation process, including annual review or attestation, is the best method to drive ongoing compliance with the regime. In addition, in the event of a data breach, ABA recommends that the OA should have the authority to remove an RP from the register, to prevent data being sent to the entity on an ongoing basis.

Questions also arise in relation to the OA's role in relation to state and territories participants that are permitted to comply with State and Territories privacy laws. For example, this means a rule prohibiting data profiling would not apply to these participants. If a state entity does not comply, it seems there will be little or limited recourse for the OA to take action and consumers would be required to navigate the different remedies that may be available under state/territories law. ABA asks the DTA to further consider how to ensure remedies for non-compliance are consistent, to help to give users confidence. These scope decisions can also have implications for the liability of other participants under the digital identity system.

Liability

ABA seeks further detail about the proposed liability regime for the digital identity system. The Liability position paper remains at high level and does not provide sufficient detail to fully assess the implications for IDPs and RPs. Assessment of liability will also depend on some of the questions raised above about the OA or exchange's liability. ABA recommends the DTA undertake specific consultation on the drafting of provisions setting out the liability regime. In addition, some worked examples covering a range of scenarios would be helpful, e.g. liability for a fraud or cyber attack.

Flexibility to innovate and incentive to participate

ABA highlights the digital identity system needs to provide sufficient commercial incentive to participate, both at launch and going into the future as consumer demands, technology, costs and charges evolve.

Technological neutrality in Commonwealth, state and territories legislation

To incentivise and support adoption of digital identity, legislation at all levels of government needs to be technology neutral. This means, in addition to the digital identity legislation, other Commonwealth, state and territories legislation will need to be reviewed to remove or amend requirements that presume face-to-face identity verification or paper-based processes. This work is underway as part of the Commonwealth government's deregulation taskforce, but more may need to be done at all levels of government and by Commonwealth, state and territories regulators.

Commercial incentives

It will be costly for IDPs to build new systems to offer new services and products, integrate with other RP / IDP systems, and establish systems and controls to comply with the rules and standards that apply to the digital identity system. These steps require significant human and technological investment. Entities that consider becoming IDPs will need to establish a business case to make the initial investment, and will review over time whether the business case for participating remains.

These will be commercial decisions including profitability of the services that may be offered through the system, both in absolute terms and relative to other commercial opportunities (for example under other competing digital identity systems).

The pricing principles should recognise this commercial reality, in order to maximise the likely success of the government's digital identity initaitive.

Incentives for adoption

The ABA agrees with the pricing principle that pricing should foster inclusion, promote affordability and adoption. Since users will not be charged under the proposed system, assessment of inclusion and affordability for RPs should consider the cost of existing identity verification procedures (including staff cost and time taken for manual procedures), systems and the costs arising human error, delays or abandoned/lost transactions. The regulatory impact assessment for the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 estimated the cost of identity verification using third parties to be around $15. The Financial System Inquiry final report also highlighted the cost and fragmentation of existing identity services as a reason for a national digital identity strategy.

In addition to pricing of transactions, two other crucial factors will influence adoption:

- Cost of set up: this includes the technology cost of systems that will allow an entity to become an RP, including any integration required under the rules and standards
- Ongoing compliance: if privacy protections will apply to RPs, then it will be crucial for the privacy obligations to be clear and simple to understand and implement. Otherwise this will be a significant disincentive to adoption, particularly for small businesses or entities with little or no compliance resources.
- Ease of use: this includes how easy it will be for RPs to use the services. This will depend on the technology, complexity of rules and standards, and is related to the cost of compliance above.

Pricing principles

Based on these observations, the ABA provides the following proposals about the pricing principles:

- Pricing principles should also seek to provide incentives for entities to participate. This could be an additional element of principle 4.
- Principle 7 should be implemented in a way that gives appropriate flexibility on pricing (ie, allow bundled services)

ABA also makes two further proposals:

- Pricing principle 1 means the government will be subsidising the design and build costs of a government system which will compete against other services. For transparency, the government should make clear the basis and amount of the subsidy.
- Legislation should allow RP being charged a cost to utilise data assets, and the system, intermediary and IDP being compensated for the transaction. Without an economic mechanism private sector activity and commercial adoption will be hindered as there is no incentive to provide solutions for existing and/or prospective data needs (such as use of multiple data points to provide higher levels of assurance).