Commonwealth Bank

Mr John Shepherd
First Assistant Secretary
Digital ID Taskforce
Department of Finance
One Canberra Avenue
FORREST ACT 2603

Uploaded via Portal: https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions

13 October 2023

Dear Mr Shepherd,

Subject: Exposure Draft of the Digital ID Bill and Draft Digital ID Rules

The CBA of Australia (CBA) welcomes the opportunity to make this submission in response to the consultation on the exposure draft of the *Digital ID Bill 2023* ('Exposure Draft') and the draft *Digital ID Rules 2024.*

CBA supports the development of a national digital identity framework to enable citizens to identify themselves safely online. Recent data-breaches, affecting millions of Australians, have shown that existing safeguards for protecting citizens' data online are "outdated"[1] and that the country's digital infrastructure needs to evolve to ensure that Australia remains a leading digital economy.

That is why CBA has helped launch the ConnectID digital identity network, a private digital identity scheme led by Australian Payments Plus, which is designed to be interoperable with Australian Government Digital Identity System ("**AGDIS**")[2].

CBA therefore supports the intent of the legislation in expanding the AGDIS, ensuring Australian citizens are protected online and are able to safely use their identity and minimise what they share in the process. As a key priority, citizens should have the freedom to use

[1] Shorten, B., (2022), "Medibank, Optus data breaches show Australia's online safeguards are outdated", opinion piece published in *The West Australian*. Accessed online at: https://ministers.dss.gov.au/editorial/9706

[2] See https://www.commbank.com.au/digital-banking/connect-id.html

their preferred service provider in interacting with both Government and private sector entities.

Principles

For a digital identity framework to deliver on its potential and enhance the privacy and security of Australia and Australians, CBA supports the following principles:

- *Citizen centric* – Australians should be able to have a choice of which service provider they wish to use to verify their identity. CBA strongly supports entrenching "choice and consent"[3] at the core of the system.
- *Voluntary* - Digital identity services should be made available for citizens to use on a voluntary basis, and entities who provision services through the system should also be able to do so on a voluntary basis.
- *Interoperable* – Flowing from the above points, the Government should go beyond consultation in setting rules and technical standards and set up structures that enable genuine co-design between public and private sector entities participating in the scheme and other rules-making bodies, such as the Open ID Foundation.
- *Technological neutrality* – To fully encourage innovation and foster consumer choice, rules and technical standards should focus on principles without entrenching prescriptive technological solutions.
- *Data minimisation* – Participants in the digital identity ecosystem should be appropriately incentivised to reduce the amount of customer data that needs to be shared in order to verify a citizen's identity.

Scope of accredited services

The current draft definition of 'accredited service' lacks the necessary clarity to determine how obligations in the Exposure Draft, Rules and Accreditation Rules will apply to accredited entities that provide products and services within and outside of the proposed AGDIS. Organisations such as CBA conduct a range of activities outside of the provision of digital identity services, but in its current form the legislation does not sufficiently ring-fence compliance obligations. The current drafting may unintentionally affect the other activities accredited organisations undertake.

CBA supports additional privacy safeguards listed in the legislation as applying "only to the extent the entity is providing its accredited services", but note that this section also creates ambiguity by stating that it will apply to entities "doing things that are incidental or ancillary to the provision of those services"[4].

Specific examples where there is a lack of clarity around the scope of activities captured by the legislation include:

- Deactivation of a digital ID[5] in CBA's systems (noting the 'identity' will be needed for a range of activities relating to other products and services provisioned by the bank);

[3] Gallagher, K., 2023, "Guide to the Digital ID legislation and Digital ID Rules – Minister's Foreword"
[4] Exposure Draft, s31
[5] Exposure Draft, s28

- Destruction of biometric information[6], noting that organisations may verify the identity of customers and maintain this information for the provision of products and services outside of digital identity;
- Restrictions on the collection of attributes about individuals outlined in section 41.

Obligations should only apply to accredited entities which are providing services *within* the AGDIS or when undertaking activities under which it has been explicitly accredited. The legislation must explicitly clarify that any obligations in the Exposure Draft and Rules will not apply in any other circumstances, including undertaking customer due diligence assessments outside the AGDIS, such as banks on-boarding customers (which is covered by separate regulation under the AML-CTF Act), or verifying customers data and credentials outside of AGDIS accredited services.

CBA recommends the Digital ID legislation and Digital ID Rules should not seek to regulate activities that are "incidental or ancillary to the provision" of digital identity services.

The Digital ID legislation and Digital ID Rules should clarify that the scope of regulated activities is limited to those within the AGDIS or for which an entity has been explicitly accredited.

Proposed phased expansion

CBA does not support the proposed phased approach of the AGDIS rollout. In keeping with the design principle of citizen choice, consumers should have the ability to choose their preferred trusted Identify Provider, and given there are existing and emerging market solutions, they may already have an existing relationship with an Identity Provider that they would prefer to leverage. Accreditation should be the barometer of an entity's maturity and applicability for joining the system – not an artificially constructed timeline which does not relate to an organisation's capability to satisfy the stated requirements.

One consideration for phasing should be the extent to which private sector solutions demonstrate an existing compliance with Australian laws and regulations, and are designed to accommodate the requirements of the AGDIS. Priority to join the AGDIS should be given for solutions designed by Australians, in order for Australians to use.

CBA recommends that the phased rollout of the AGDIS be based on the qualification of individual entities, rather than a phased roll-out to selected sectors of the economy.

In line with the requirement for service providers to be accredited under the TDIF, priority should be given to Australian entities who have designed their solutions for Australians to use.

[6] Exposure Draft, s48

Relying parties

CBA would welcome additional obligations applying to Relying Parties. Currently, there is a lack of due diligence of entities wishing to become relying parties, other than proving they are an Australian entity or a registered foreign company[7] and undergoing approval from the Digital ID Regulator[8]. While relying parties must submit a risk assessment for managing cyber security incidents and a written policy for investigating fraud incidents[9], they do not have any obligations to notify other participants of such incidents or Service Level Agreements in responding to these incidents.

In general, there are few ongoing obligations on relying parties participating in the AGDIS, and the burden of enforcing requirements in the legislation falls on Identity Providers. For instance, accredited participants are taken to enter into a statutory contract with relying parties for activities undertaken under the AGDIS, but only accredited entities are liable for any loss or damage as a breach of that contract[10].

Additionally, only accredited parties (i.e. not relying parties) must maintain insurance for any liabilities that arise out of participation in the AGDIS[11], and only accredited parties (i.e. not relying parties) are subject to the redress framework[12].

CBA recommends the legislation imposes the following obligations on relying parties:

a. Restrictions on how relying parties maintain, treat, store and use information received within AGDIS;
b. Liability for breaches of a statutory contract that they enter into as part of their participation in the AGDIS;
c. A requirement to maintain insurance (as the Digital ID Regulator deems appropriate) for breaches of the statutory contract;
d. Service Level Agreements for responding to customer complaints, fraud investigations and cyber security incidents, as well as obligations to inform the regulator and other participants of any incidents that may affect the security or resilience of the AGDIS.

CBA recommends s.80(3) be amended to include relying parties as well as accredited entities as having liability for breaches of contract.

Standards & Interoperability

A successful Digital ID system will require a principle-based, technology agnostic approach.

CBA recommends that wherever possible the AGDIS references industry standards rather than creating bespoke standards. Overly prescriptive requirements may result in

[7] Exposure Draft, s58(1)(b)
[8] Exposure Draft, s59
[9] Digital ID Rules, s7
[10] Exposure Draft, s80
[11] Exposure Draft, s81
[12] Exposure Draft, s83

organisations deciding that the cost of compliance is too great, which is a particular risk in a voluntary scheme, and finding that it is not possible to meet requirements in an innovative way. Ideally, standards should incentivise participants to make forward-looking investments to facilitate a dynamic, interoperable ecosystem that can respond to evolving cyber threats.

Ensuring appropriate standards for the digital ID landscape is particularly difficult as not only are technologies fast-evolving, but there is an imperative to ensure interoperability with the private sector and other comparable jurisdictions (such as States and Territories within Australia, as well as global economies such as Europe, UK and Singapore).

For Australia's digital identity framework to evolve in response to the cyber security threat landscape, while remaining open to innovation, the Government must embrace standards governance that considers input from the technology sector and other global standards-bodies. This means the Government should go beyond mere 'consultation' and should engage in genuine co-design on standards with AGDIS participants and other subject matter experts.

Co-design should involve appropriate representation on standards-setting bodies, suitable consultation durations and structured mechanisms, such as voting, to align on outcomes. An important principle in a co-design framework should be that participants who bear the costs of meeting future standards changes or enhancements should have the greatest weight in voting. This will ensure the standards adequately balances the costs and benefits future roadmap items, while allowing participants to innovate in how new standards or requirements are met.

Examples of successful models that could be leveraged are numerous – in Canada, the Digital Identity and Authentication Council of Canada (DIACC)[13] has driven widespread adoption of digital identity solutions and helped to inform consumers; the National Institute of Standards and Technology (NIST) in the U.S. regularly invites independent experts and representatives from standards-bodies to develop standards and guidelines.

The current structure envisaged by the legislation falls short of these models with the standards entrusted to a Data Standards Chair, requiring them to "consult" for a period of 28 days.[14] The method and requirements governing consultation are otherwise at the discretion of the Data Standards Chair. Greater structure needs to be given to the consultation process, to ensure formal mechanisms for incorporating feedback from affected parties and subject matter experts, including voting on proposals, and adequate change management processes for ensuring that Participants have adequate lead-time to comply with future changes.

Following industry best practice rather than designing bespoke standards will allow the AGDIS to more nimbly address threats from malicious actors as attack vectors change. It will further ensure the AGDIS can continue to evolve with emerging technologies, preventing technical debt and avoiding risk of obsolescence.

[13] See www.diacc.ca

[14] Exposure Draft, s94

CBA recommends that the legislation create a standards setting body comprised of representatives from the Government and private sectors, including appropriate international standards-bodies and experts. In setting standards, the body should have regard to the following principles:

1. Be principles based rather than prescriptive in how standards are set, so that entities may innovate in how they meet the requirements of the framework;
2. Seek alignment with existing standards to the extent possible, particularly in regards to comparable international jurisdictions, and avoid bespoke arrangements at all costs;
3. Incorporate formal mechanisms for feedback, such as voting on new proposals
4. Provide greater weight to existing service providers when it comes to voting on standards, given that they will disproportionately bear the cost of compliance;
5. Allow adequate time for implementing any changes.

The standards setting body should also ensure that any changes take into account a cost-benefit analysis of the expense and complexity imposed on existing participants in the AGDIS.

Cyber resilience

The current proposed provisions regarding the definition of cyber security incidents is too broad, as it includes attempts to gain access to systems, even if those attempts are blocked and unsuccessful. As one of Australia's most trusted financial institutions, CBA prevents a surfeit of such attempts each day. Reporting failed attempts is unlikely to be of utility to the regulator and would impose significant cost and operational complexity on participants.

Further, the proposed reporting timeframes are not consistent with existing obligations contained within legislation covering cyber and data breach reporting, such as the Privacy Act (Cth) and the Security of Critical Infrastructure Act (Cth).

Additionally, CBA recommends that where an accredited entity has a similar existing obligation with a Commonwealth regulator, the Digital ID regulator should rely on the compliance assessment already undertaken. For example, under the Critical Infrastructure legislation, the regulator can waive the requirement to comply with the Risk Management obligation where the entity is compliant with APRA's CPS 234. We recommend a similar approach could be taken here for entities that can demonstrate existing compliance, as it would minimise overlapping obligations and compliance costs for participants, and as well as unnecessary regulator resource expenditure to accredit participants.

CBA recommends that the Government run a separate consultation on cyber security reporting requirements and aligns reporting timeframes with other frameworks.

In addition, the Digital ID regulator should rely on compliance assessments made by comparable regulatory regimes for accreditation, rather than asking participants to undergo redundant assessments.

Fit and Proper Person assessments

CBA is supportive of a 'fit and proper person assessment' for digital identity, however the current assessment criteria are broad and onerous without a commensurate reduction in risk of consumer harm. For example, the current scope captures bodies corporate and people within organisations that have no connection to its digital identity product. CBA considers that the 'fit and proper person assessment' should be more appropriately tailored to the people who lead and manage an organisation's digital identity product, and specifically in regards to ensuring that AGDIS requirements are met.

CBA also recommends TDIF accreditation requirements be amended to adopt alternative approaches which would achieve a similar degree of reduction in risk of consumer harm. For example:

- Model the Fit and Proper Person assessment on the APRA CPS520 standard or Australian Financial Services License (AFSL) requirements, with targeted adjustments for digital identity services; or
- If an organisation meets the 'fit and proper person' assessment under the abovementioned regimes, reliance on that assessment could be placed in lieu of an additional assessment, thereby reducing the compliance burden for organisations already subject to similar regulations.

CBA recommends alignment of the Digital ID 'fit and proper person' assessment to existing industry regulatory requirements.

'Fit and proper person' assessments should only apply to those who directly have accountability for the digital identity services delivered within the AGDIS.

Additional privacy safeguards

CBA recommends further consultation on additional Digital ID privacy safeguards, in particular so that interaction with the Privacy Act can be appropriately considered.

There are a number of outstanding questions in relation to the privacy safeguards, such as:

- Whether the additional safeguards will be subject to existing exemptions where there is a 'permitted general situation' under the Privacy Act; and
- How the 'disclosure of restricted attributes' will operate alongside existing restrictions on the use and disclosure of government related identifiers in Australian Privacy Principle (APP) 9 of the Privacy Act.

The proposed 14-day retention period for biometric information collected for fraud prevention and detection purposes[15] conflicts with existing obligations under the Privacy Act. In particular, APP 11.2 states that an APP entity may retain personal information so long as it is needed for a legitimate purpose under the APPs (e.g. in this case, for fraud prevention purposes). CBA notes that the proposed 14-day retention period would mean an

[15] Exposure Draft, s48

organisation's fraud detection and prevention methodology is dictated by a statutory timeframe, which goes against the policy intention of APP 11.2.

> CBA recommends the Government conduct additional consultation to clarify the interaction between proposed Digital ID privacy safeguards and the Privacy Act.

Interoperability

The current provisions regarding the circumstances in which the Minister can grant an exemption from interoperability are too broad and lack the necessary clarity or criteria required to provide some certainty for industry to plan and invest with confidence[16]. The legislation should be amended to provide clear criteria upon which the Minister must base their decision to grant an exemption to the interoperability obligation.

> CBA recommends the legislation sets out clear criteria for the Minister to provide an exemption to participants from interoperability obligations.

Charging model

CBA notes that the future charging framework should be defined to drive participation in digital identity networks for both relying parties and service providers. Given that the Government has cited citizen choice as a key design principle for the AGDIS, the charging framework will therefore need to create appropriate incentives for service providers to invest and innovate in the future identity system.

The legislation does not provide guidance on the future charging model, but does provide that the Rules will set out future fees, along with other arrangements in relation to "exemptions, refunds, remissions or waivers"[17]. CBA is concerned by providing such broad powers in the Rules, given the potential to undermine competitive neutrality principles. CBA recommends that the Government provide more detail on the proposed charging framework and consult with industry in parallel to progression of Digital ID legislation.

> CBA recommends that the Government consult as matter of priority on the draft charge framework that will underpin the operation of the AGDIS to provide industry with the require clarity prior to the AGDIS coming into effect

In summary, CBA strongly supports the Government's intent in developing a national digital identity framework. The expansion of the AGDIS will be central to securing the privacy of Australian citizens and to ensuring they benefit from a modern, fit-for-purpose digital infrastructure when transacting online with the Government and private sector businesses.

[16] Exposure Draft, s75
[17] Exposure Draft, s142

CBA is confident that a framework underpinned by the principles outlined in this submission will ensure that Australian citizens will get the full economic benefit from the existing investments made by both Government and private sector entities in digital identity services.

CBA welcomes the opportunity to discuss our submission in more detail. Should you wish to do so, please contact CBA by email at GovernmentIndustry-InternationalAffairs@cba.com.au.