National Australia Bank
395 Bourke Street
Melbourne VIC 3000

10 October 2023

John Shepherd PSM
First Assistant Secretary, Digital ID Taskforce
Department of Finance
1 Canberra Avenue
Forrest ACT 2603

Dear Mr Shepherd,

National Australia Bank feedback on draft Digital ID Bill and Digital ID Rules

National Australia Bank (NAB) appreciates the opportunity to provide feedback on the exposure draft of the Digital ID Bill and Digital ID Rules. In addition to sharing our views through the provided template, NAB also takes this opportunity to highlight specific opportunities where the proposed Digital ID Bill and Rules can help realise the development of a flexible and empowering digital identity ecosystem for Australians.

As a member of both the Australian Banking Association and Australian Payments Plus, NAB has also contributed to and supports their respective submissions.

As one of Australia's largest financial institutions, the protection of customers and their data has never been more important. NAB sees the development of a forward-thinking and fit for purpose Digital ID ecosystem as a critical pillar to progressing Australia's digital economy, and a necessary measure to reduce the over-sharing of personal data that can expose individuals to scams and identity theft. This can only be done collaboratively between Government and the private sector. NAB welcomes the steps that Government is taking to progress Digital ID in Australia, and we are committed to playing our part.

NAB appreciates that the exposure draft Digital ID Bill and Digital ID Rules recognise the role that private sector Digital ID solutions have in the ecosystem and provides for future interoperability. NAB strongly believes that the success of the overall Digital ID system is contingent on Australians having a choice of identity providers. The availability of choice among multiple providers, from both the private and public sectors, will be crucial in mitigating potential community concerns about privacy or the potential for misuse. Choice will help enable more Australians to become comfortable with ID solutions that will ultimately make their identity more secure.

NAB recognises the role that it can play for Australia as an identity service provider. NAB has worked with other financial institutions and Australian Payments Plus, to launch the initial pilot of the 'Connect ID' service earlier this month. NAB sees the development and entry of private sector Digital ID providers as essential to driving increased consumer awareness of Digital ID and to accelerate the acceptance of Digital ID offerings amongst organisations and entities who need to verify identity or particular attributes.

While NAB supports and is encouraged by the Government's initiative on this topic, we concurrently highlight particular aspects that we believe can be improved.

Proposed phased roll-out of the Digital ID ecosystem

As noted above, NAB considers that a Digital ID ecosystem that provides Australians with choice, is essential for the sustainable development and growth of Digital ID and associated use cases. With this consideration, NAB is concerned regarding the proposed phased approach to Digital ID, and instead highlights the need to progress all components of a unified, interoperable public-private Digital ID ecosystem for Australians.

NAB disagrees with the statement in the *Digital ID Guidebook,* that a phased approach will 'develop the Digital ID market, and increase community awareness of Digital ID.' On the contrary, NAB considers the phased approach risks creating fragmentation in the market and confusion for users, and the sequencing of 'public sector first' creates uncertainty that may discourage private sector investment. The Australian ecosystem will benefit from having multiple providers offering different choices to citizens, which will foster an investment environment that is more conducive for more firms to enter the market.

With multiple private sector Digital ID offerings either in-market or preparing to enter in 2024, a phased approach will inhibit the development of the Digital ID ecosystem and restrict community awareness of Digital ID to only a small number of use cases and government providers. The planned approach involves a scenario where Commonwealth, State-based and private-sector digital IDs will all exist in the market at the same time, but each subject to different constraints on what services they can offer or access, and at what point in time they can offer or access these services.

If Digital ID is to achieve widespread adoption in the community, Australians need to have (i) a choice of secure, accredited providers, and (ii) the ability for that provider to reach and support all of their interactions, whether making a purchase, entering a contract in the private sector, or accessing a public service.

The lack of clarity around the timing of each phase is also of concern. Without detail on how long each phase will run and when Phase 4 will finally be reached, this significantly impedes the ability of private sector providers to plan appropriately for the future development of their product, the development of new use-cases, and the features they can bring to their customers. If phasing is to be adopted, NAB encourages Government to consult with industry on appropriate timing and inclusions in each phase, and for complete roll-out to occur as quickly as possible, to limit the impact on private sector investment, in product development.

While NAB appreciates the Government's intentions in ensuring that the rollout of the Digital ID ecosystem is orderly, this can still be achieved while providing greater customer and citizen choice from Day 1. To ensure strong uptake and awareness of Digital ID and provide the opportunity for states, territories and the private sector to collaborate and bring new services to market sooner, NAB considers that private sector providers (where accredited and meeting security standards) should have access to the same opportunities as government-issued identity sources, sooner.

Whilst NAB is cognisant of potential complexities associated with technical and operational implementation between public and private sector use cases, these challenges are not insurmountable. There will be benefits and learnings for both the public and private sectors where private sector Digital ID solutions are able to be utilised for public sector use cases from the outset, and vice versa. This will ultimately strengthen the trustworthiness and usability of ecosystem as a whole.

Verifiable credentials

Another important clarification is to stress the understanding of 'Identity' and what constitutes sufficient Identification (or verification) for a particular transaction or purpose. Minimising the amount of data

transferred is imperative to helping to combat fraud and scams. NAB considers that there are many such instances where a particular attribute may warrant verification, for instance that a person is at least 18 years old, and that this can be verified by an identity service provider without needing to share or reveal their full identity.[1]

The Digital ID Bill and Digital ID Rules focus on scenarios involving a full identity, however NAB considers it is important to develop a national ecosystem for all such scenarios. If Australia implements separate parallel systems for (i) sharing a full Digital ID, and (ii) providing verification on selected attribute(s), this would be an unnecessary fragmentation that may ultimately hinder adoption.

This also necessitates a broader consideration of how identity data sets are established by a provider, where in many cases a credential or an identifiable attribute will be established in the ongoing course of business, and not necessarily as a specific identity that can be deactivated.[2]

NAB believes that a greater understanding of the way in which identification and attribute services will be provided by private sector solutions is necessary, to ensure the application of the legislation is 'fit-for-purpose.' NAB has provided further detail and commentary on this in the feedback table in relation to the question 'Are the additional privacy safeguards sufficiently robust, clear and practical?' NAB recommends that Government explores this further with private sector providers, so various components can be brought together to create a truly interoperable ecosystem.

Improvements from the Consumer Data Right experience

As Government considers feedback received on the Digital ID Bill and Digital ID Rules, we strongly encourage Government to consider this alongside the Consumer Data Right (CDR) regime and the impacts that its rollout approach has had on its uptake and the usage of CDR functionality.

The gradual, staggered CDR rollout (where designation processes are required for expansion of the CDR into new sectors of the economy) has, with other factors, contributed to a much lower level of uptake than what was envisioned by both Government and the banking sector. While NAB continues to explore innovative CDR use cases for our customers, the small number of active users and limited public awareness of CDR, limits the investment appetite for CDR in the long-term. A robust, highly used and economy-wide Digital ID system is an essential part of Australia's digital infrastructure moving forward, and Australia should seek to avoid a similarly low adoption and active user base in the initial years.

At times, the governance framework around the CDR Rules has also made the regime difficult for participants to interact with. While NAB appreciates that the CDR Rules are an evolving legal framework that is continually reviewed in response to input from policymakers and stakeholders, the lack of a regular cadence for updates to the Rules has limited the ability for participants to effectively plan and prioritise their CDR investments and resourcing.

NAB strongly encourage the Government to consider how the Digital ID Rules may accommodate a regular rhythm of review and feedback with impacted and interested parties. This would allow participants to ensure time and resources are allocated to provide considered and timely feedback as the system grows, and make any adjustments to scheduled product improvements and functionality that may be necessary, and ensure the system is operating smoothly for both customers and participants.

NAB has appreciated the progress Government has made in considering the next steps for the Australian Digital ID system. We commend Government's initiative, but concurrently believe that both the public and private sector need to develop the ecosystem faster, to provide safety and security for Australians. NAB looks

[1] This fact is reflected in certain of the provisions within the exposure draft Bill. See for instance Section 3(1) wherein the objects of the Bill currently only refer to verification of 'identity.'

[2] See in particular Section 28 of the Exposure draft Bill.

forward to continuing to work with Government to ensure Australians can benefit from an innovative, safe and successful Digital ID ecosystem.

[redacted]

Yours sincerely,

Brad Carr
Executive, Digital Governance
National Australia Bank

Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

Your name	Lachlan Stewart
Your organisation	National Australia Bank
[redacted]	[redacted]

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	NAB welcomes the technology neutral approach to accreditation of service providers within Australia's Digital ID scheme and supports the inclusion of services including verified credentials and digital wallets being captured, from the outset. We note that currently the objects of the Act only refer to verification of 'identity.' In NAB's view the objects of the Act should also reflect the fact that individuals may verify not just their identity but also an 'attribute.' As such we recommend that Item 3(1)(a) of the exposure draft Bill be amended to include a reference to 'attribute.' As the technology evolves and additional Digital ID services are provided, NAB supports that all parties in the Digital ID ecosystem and which integrate with the system, should be subject to appropriately rigorous security and privacy standards.

Page # of guide	Question	Your response
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	
16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	While the intent of this is clear, it would be important to ensure that the conditions are not contradicting other legal or regulatory obligations, such as documentation requirements under the AML/CTF legislation.
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	**Application for Accreditation** Section 14(1) of the draft Bill specifies that an entity may apply for accreditation as *one* of the following kinds of accredited entities. This appears to limit an entity from participating as both an ISP and an ASP and as such, NAB recommends that clarification is made here.
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	NAB welcomes strong privacy safeguards, as this is vital to ensuring trust and adoption of Digital ID solutions. A properly resourced regulator will be important to ensure trust in system, including with the ability to respond quickly and efficiently to ecosystem feedback and incidents.

Page # of guide	Question	Your response
		NAB makes the following comments and recommendations in relation to the current drafting of the privacy safeguards in the exposure draft Bill and Rules. **<u>31 Chapter applies to accredited entities only to the extent the entity is providing accredited services etc</u>** The Privacy Safeguards are stated to apply to an accredited entity only to the extent the entity is providing its accredited services *or doing things that are incidental or ancillary to the provision of those services*. (*Exposure Draft, Chapter 3 – Part 1, section 31*). In NAB's view the phrase 'or doing things that are incidental or ancillary to the provision of those services' in section 31(b) has the potential to cause unintended negative consequences unless there is sufficient clarity in the legislation to ensure that an accredited entity's normal business activities are not captured by the legislation. For example, NAB may act as an Identity Service Provider or Attribute Service Provider in a private sector digital Identity solution and will offer NAB customers the ability to verify their identity or an attribute utilising the information that NAB has already collected and validated as part of its onboarding process. If NAB were to become accredited under the scheme, arguably a plain reading of the phrase 'or doing things that are incidental or ancillary to the provision of those services' may capture NAB's collection, use and disclosure of personal information to provide banking services to its customers (as these would be incidental or ancillary to its provision of the accredited services). It will be extremely important to ensure that accredited entities 'BAU' processes are not impacted by becoming accredited within the Government's digital identity scheme, as (1) NAB does not believe this is the intent of the legislators; (2) if this is not made sufficiently clear (that 'BAU' activities are not impacted, including for instance where an accredited ISP receives updated

Page # of guide	Question	Your response
		personal information from an individual user as part of providing its accredited services and feeds this updated information back into its own systems of record to ensure a customer's profile is up-to-date), NAB considers that this will strongly disincentivise accreditation and ultimately lead to less choice for consumers and citizens. Having regard to the above we also note the definition of 'system information' in the Digital ID rules (section 10) and note the breadth of this definition may inadvertently capture information that an accredited entity generates, collects, holds or stores as part of its BAU activities and therefore an overarching data localisation requirement in respect of such data is likely to be prohibitive to participation. NAB recommends that this definition be reconsidered in the context of private sector accredited entities and further clarified so as to not capture information that is otherwise used and handled as part of an accredited entity's core business. A Digital ID is defined under the exposure draft Bill as follows: 'Digital ID of an individual means a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services.' We also note the requirement for Digital IDs to be 'deactivated on request' under section 28 of the exposure draft Bill. For private sector operators, which otherwise provide services to their customers (i.e., financial services) the concept of 'deactivation' of a Digital ID may not be fit for purpose as private sector operators will not separately create a 'Digital ID' for an individual customer. For example, NAB customers who wish to utilise a NAB Digital ID solution would opt in to do so and NAB would utilise the information already provided by the customer to verify these details to a Relying Party. Additionally, the customer's profile information would still be needed and relevant to their ongoing relationship with NAB as a banking customer.

Page # of guide	Question	Your response
		Therefore, whilst a customer may choose not to use the NAB Digital ID offering and would not be required to do so, NAB could not 'deactivate' their customer profile. **<u>41 Collection of certain attributes prohibited</u>** Section 41 of the Bill prohibits outright the collection, use or disclosure of certain attributes of an individual, including information or opinion about an individual's racial or ethnic origin. In NAB's view this may have unintended negative consequences of diminishing inclusion as part of Australia's Digital ID ecosystem where for instance, certain individuals (including First Nations Australians) may need to prove racial or ethnic origin in order to obtain access to entitlements or services and this would prohibit such Digital ID services being provided within the ecosystem. Rather than an outright prohibition, NAB suggests amending this section to require express consent. **<u>43 Disclosure of Restricted Attributes</u>** Section 43 prohibits an accredited entity from disclosing a restricted attribute of an individual to a Relying Party that is not a participating Relying Party if the Accredited entity's conditions on accreditation do not include an authorisation to disclose the restricted attribute to the Relying Party. We note that the definition of a restricted attribute includes information or an opinion about an individual's membership of a professional or trade association (section 11(1)(d)). Professional memberships are an important attribute for individuals to be able to share within a digital ID ecosystem to gain access to employment opportunities. It is unclear to us on the current wording of section 43(2) whether an accredited entity would need to seek authorisation for each individual relying party to which it may provide professional membership information or whether a 'blanket' authorisation may be sought. In NAB's view if authorisation were required to be sought prior to each individual relying party

Page # of guide	Question	Your response
		being onboarded, this may limit adoption for such important applications such as in the employment context. **<u>44 Restricting the disclosure of unique identifiers</u>** In NAB's view this section to be amended to allow for the provision of 'unique identifiers' to service providers or contractors to the extent that such entities need access to the relevant 'unique identifiers' to be able to provide services to the accredited entity. **<u>Definition of cyber security incident</u>** We note that the definition of a cyber security incident currently includes unauthorised "attempts" to gain access… or impair systems…etc (section 9, Digital ID Bill) and we note the corresponding obligation on accredited entities to notify the Digital ID Regulator of cyber security incidents. In NAB's view capturing 'attempts' sets too low a threshold, as entities and government agencies are routinely subject to 'attempts,' which are successfully prevented. As such NAB considers that by including 'attempts' within the meaning of cyber security incidents this will overly burden Regulators and accredited participants as they will be subject to unnecessary notification requirements where there has been no actual breach of their systems.
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the	

Page # of guide	Question	Your response
	restriction on disclosure of biometric information?	
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	In NAB's view, individuals should be able to access both private sector and government Digital ID solutions for both government and private sector use cases, from the outset of the rollout. Whilst NAB appreciates there may be implementation challenges associated with connecting private sector and government solutions, we do not believe these challenges are insurmountable and consider that government and industry addressing these issues together will yield better results for consumers and citizens.
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	Please see NAB's comments above. NAB urges Government to enable interoperability between public and private sector use cases from the outset. Ministerial directions and phasing risk unnecessarily inhibiting Australia's adoption of Digital ID solutions, which will limit access to productivity and privacy enhancing facets of this scheme.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	In NAB's view, phasing the rollout of the ADGIS will have a negative effect on the Digital ID services market in Australia. NAB believes that choice is a critical enabler for adoption of Digital ID solutions. Where individuals do not have choice from the outset to determine which Digital ID provider they wish to use for both government and private sector services, NAB considers this may undermine adoption and the digital ID services market in Australia as a whole.
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any	

Page # of guide	Question	Your response
	additional exceptions appropriate?	
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	NAB supports the principle of interoperability by default. To ensure that there is consumer and citizen choice, NAB's strong view is that there needs to be clear grounds on when interoperability should not be required. Section 75 of the exposure draft Bill lists grounds on which the Minister may grant an exemption from the interoperability requirement, including the following: - that the Minister is satisfied that a service, or access to a service, provided by a participating relying party that is a government entity is of a kind that should be provided only to other government entities; - if the relying party service would promote the use of Digital IDs in the AGDIS In NAB's view it is not sufficiently clear on which grounds a Minister may be satisfied that it is necessary to limit access to some government services to a government-issued Digital ID, and we would strongly urge for these grounds to be made more explicit within the legislation. Further, NAB would also be interested to understand the intention behind limiting interoperability where a Relying Party service would promote the use of Digital IDs in the AGDIS.
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between	NAB strongly encourages collaboration between industry and government to ensure best practice, longevity and the sustainability of Australia's Digital ID scheme. The establishment of a public-private 'task-force' would ensure that Data Standards could be implemented in a way that was cost-efficient for the

Page # of guide	Question	Your response
	certainty for accredited entities while maintaining currency?	economy, flexible and enables the best use of technology for the benefit of Australians.
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	Further to NAB's comments above in relation to the need for industry-government collaboration, certain learnings from not only Australia but also the UK where the Open Banking Implementation Entity (OBIE) has been credited as a success factor in that jurisdiction's roll out of technical standards. In particular: - the benefits of industry expertise in developing standards that are consensus driven, with an outcome-based approach aligned to the policy objectives of a particular legislative framework; - the need for cross-sectoral membership for any implementation entity to drive the best outcomes for citizens and consumers (where a diversity of perspectives such as consumer groups, industry and government, amongst others are taken into account.) NAB notes that any funding model if an implementation entity akin to the OBIE were to be considered for the Digital ID scheme, would need to be sustainable, requiring contributions from a wide pool of industry participants.