Digital ID Taskforce
Department of Finance

10 October 2023

Dear Sir/Madam

AUSTRALIAN RETAIL CREDIT ASSOCIATION (ARCA) SUBMISSION – 2023 DIGITAL ID BILL

Thank you for the opportunity to provide a submission in response to the 2023 Digital ID Bill.

The Australian Retail Credit Association (ARCA) is the peak industry association for businesses using consumer information for risk and credit management. Our members include banks, mutual ADIs, finance companies and fintech credit providers, as well as all of the major credit reporting bodies (CRBs) and, through our associate members, many other types of related businesses providing services to the industry. ARCA's members collectively account for well over 95% of all consumer lending in Australia.

ARCA, upon request of the Office of the Australian Information Commissioner (OAIC), has acted as Code Developer for the Privacy (Credit Reporting) Code 2014 (the CR Code) which gives effect to Part IIIA of the Privacy Act (which, in turn, sets out the legislative framework for credit reporting in Australia). ARCA is also the author and administrator (through its subsidiary entity) of the Principles of Reciprocity and Data Exchange (PRDE) which sets out industry agreed rules and standards for participation in comprehensive credit reporting (CCR). ARCA has both a deep understanding of the operation of the Privacy Act (particularly Part IIIA), as well as an understanding and experience of industry self-regulation as concerns the contribution of data.

ARCA's background and experience, as well as the breadth and experience of our Membership, means we are well-placed to comment on issues raised in this exposure draft legislation.

Importance of Digital ID for consumer lending

Consumer lending in Australia relies on credit providers and credit reporting bodies having reliable identity information for consumers. With the increase in frequency and scale of mass data breaches and identity theft there is a growing risk that cyber criminals will use stolen identify information to open transaction accounts and apply for credit in a legitimate consumer's name.

Australian consumers are increasingly aware of and concerned about data breaches and identity theft. The Office of the Australian Information Commissioner's Australian Community Attitudes to Privacy Survey 2023 found that 62% of respondents see the protection of their own personal information as a major concern in their life. The survey also found that 47% of respondents were told by an organisation that their personal information was involved in a data breach in the previous year, and 76% said they experienced harm because of a data breach.[1]

Identity crime has risen significantly in recent years. The Australian Institute of Criminology reported in 2023 that 31 percent of respondents experienced identity crime in their lifetime and 20 percent in the past 12 months.[2] This number has risen sharply in the past two years, where the same survey found 19 per cent of respondents said they had been victims of identity crime at some point in their life.[3]

Trust in identity information is critical for the Australian economy. It is particularly critical when it comes to consumer lending. When an individual establishes a new transaction or credit product, they need to provide identity information to verify their identity (e.g. name, date of birth, and identification document numbers). Just because an individual has access to and provides this information, it doesn't mean that in every instance they are actually the individual in question. The rapid increase in identity theft risks undermining the confidence credit providers have in the system.

For these reasons, ARCA members are supporting of the Government's efforts to provide greater confidence to Australians to create and use a digital ID. We see that Government's initiatives to strengthen the digital ID voluntary accreditation scheme for providers of digital ID services and providing strong privacy safeguards for people creating and using digital IDs from accredited providers will increase the uptake of digital ID.

As digital ID uptake increases, we hope to see a decrease in the number of companies collecting and holding customers' passports, driver's licences and other identity documents that could be lost in a data breach. This means less likelihood of cyber criminals using stolen identity information to apply for consumer credit illegally.

[1] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey, 2023
[2] Australian Institute of Criminology, Identity crime and misuse in Australia, 2023.
[3] Australian Institute of Criminology, Identity crime and misuse in Australia, 2021.

We would encourage government to undertake a campaign to explain digital ID and their benefits to consumers to encourage greater consumer uptake of these products.

The Importance of Competition and Choice for Consumers

ARCA welcome the legislation's aim to facilitate the reciprocal or shared use of Digital IDs between public and private sector organisations. Ensuring interoperability between the public and private sectors will improve the customer experience and uptake of digital IDs. ARCA is also supportive of the Government's commitment to allow private sector digital ID providers access to Government services. This is an important step in promoting a whole-of-economy scope to digital ID.

We also appreciate that Government sees that value in private sector providers of digital ID products, operating alongside the Government's digital ID product - myGovID. Some consumers may be uncomfortable with using a government identity document in all situations (such as purchasing alcohol) so having a choice of provider will maximise the update of digital IDs, especially amongst that cohort of consumers.

We foresee that the timing of Phases 3 and 4 will be critical to driving uptake of the digital ID in the economy and Australia's ability to reap the economic and productivity benefits of consumers being able to transact and verify themselves using a secure and trusted digital ID.

However, we are concerned that there is a lack of clarity around the timing of Phase 3 and Phase 4; and we are also concerned with the phased approach being proposed, i.e. Phase 3 (which allows the use of government Digital ID and attribute providers in private sector services) and Phase 4 (which allows the use of private sector Digital ID and attribute providers in some government services). We do not support the phasing of 3 and 4 and would prefer to see both myGovID and private sector accredited digital ID providers both access government services concurrently.

There are a number of reasons why we hold this view. The first is that there is no detail around the time between Phase 3 and Phase 4. This lack of detail creates risk for continuing investment of private sector providers in digital ID products. There has been a significant investment made by the private sector to date in the development of these products and the private sector will have to continue to invest more to meet the new standards and achieve the trustmark required by this legislation. Additionally, there are ongoing costs for private sector providers in maintaining their systems and meeting accreditation standards. A lack of certainty around timing of phasing raises risks and questions over the value of ongoing investment in digital ID products.

We are also concerned that a phased approach will result in more consumers choosing to uptake the myGovID over private sector digital ID products. Again, this could discourage ongoing investment from the private sector, leading to less choice for consumers and potentially less innovation. In turn, this could slow the uptake of

digital ID, particularly with the cohort of consumers that are not comfortable with selecting a government-issued digital ID.

Our preference is to have no phasing between public and private sector access services for commercial or government accredited digital ID providers. Additionally, we would also appreciate clarity around the timing of the different phases. This will provide the private sector with more certainty to base investment decisions, and drive increased innovation in the sector and quicken the speed of economy-wide adoption of digital ID, and the benefits that will accrue from this.

Definition of digital ID to be broadened

Section 9 of the draft bill defines digital ID as: *a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services.* ARCA's concern with this definition is that is doesn't explicitly provide for occasions where an individual will use their digital ID to access face-to-face services. E.g. verifying proof of age in a liquor store. We note that this is the same definition used in the National Strategy for Identity Resilience. We recommend amending this definition to be broad enough to encompass a scenario where an individual uses digital ID in a face-to-face interaction.

Coordination between the Privacy review, review of AML/CTF, National Strategy for Identity Resilience (NISR) and Digital ID legislation

The Australian Government's 2023 response to the review of the Privacy Act (and proposed reforms), the 2023 consultation on proposed reforms of Australia's anti-money laundering and counter-terrorism financing (AML/CTF), the National Strategy of Identity Resilience and digital ID bills, must be considered in a coordinated way because they have an individual and cumulative impact on ARCA members.

Most ARCA members are reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and have obligations around retention of records of identification procedures. They also have obligations to check a customer's identity and the validity of that identity (i.e. passports not more than two years expired). Proposed reforms of the AML/CTF regime should make clear whether AML/CTF reporting entities can accept digital ID to satisfy their obligations and also confirm which entity has the obligation to check the validity of the source documents (i.e. Digital ID provider or AML/CTF reporting entity).

We see an opportunity to revisit the AML/CTF obligations as the uptake of digital ID increases in Australia. This would further reduce the number of identity documents required to be held by private sector entities that fall under this regime. We would also encourage the Government to take a whole-of-government approach to understanding how each reform interacts and the impacts on the private sector.

Data quality and consistency critical

It is common for ARCA members to find inconsistency between identity documents, e.g. different names of drivers licences and passports. This creates friction in the system and issues for customers. As we move to a whole-of-economy digital identity system, we need to make it easy for people to fix source documents and optimise the process for cleaning up source documents. Data quality and consistency is critical, especially in ensuring matching fields are similar to avoid false negative responses.

We understand that the Attorney-General's Department intends to conduct work in this area, as identified in the National Strategy for Identity Resilience. We support this work, and again hope it aligns with other Government reforms, as noted above.

Definition of cyber security incidents

ARCA is concerned with the inconsistency in the definition of a cyber security incident in this Bill compared with other *government legislation.* Specifically, the *Security of Critical Infrastructure Act 2018 (the SOCI Act).* This Bill defines a cyber security incident as meaning one or more acts, events or circumstances that involve:

(a) unauthorised access to, modification of or interference with a system, service or network; or
(b) an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or unauthorised access to, modification of or interference with a system, service or network; or
(c) an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or
(d) unauthorised impairment of the availability, reliability, security or operation of a system, service or network; or
(e) an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network.

In contrast, s12 M of the SOCI Act defines a cyber security incident as one or more acts, events or circumstances involving:

a) unauthorised access to or modification of computer data or computer program, or
b) unauthorised impairment of electronic communications to or from a computer, or
c) unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

Our concerns are twofold. The first is the principle of having consistent definitions across government legislation especially when ensuring the cyber security of the digital ID system is as important to Australia's critical infrastructure.

Secondly, we are concerned that the inclusion of 'attempt to' in the Digital ID Bill is too broad. Cyber security attempts are extremely common and not preventable. Organisations that hold information about customers have frequent attempts on them

each day. The Bill creates risk, uncertainty and undue reporting obligations on accredited entities for a cyber security attempt. For example, the Digital ID regulator:

- may suspend the accreditation of an accredited entity if there is a cyber incident,
- require an entity to undergo a compliance assessment,
- and report on the number the digital ID fraud incidents or cyber security incidents, and the responses to any such incidents in an annual report to the Minister, for presentation to the Parliament.

It is unreasonable to expect accredited entities to report cyber security attempts and responses as these would require vast amounts of data. Similarly, it is not reasonable for the Regulator to have the power to require a compliance assessment or risk of accreditation suspension when they have no power over cyber security attempts.

For these reasons, ARCA would prefer the Bill use the definition of cyber security incident under the SOCI Act.

Digital inclusion

ARCA supports the Government's principle of a voluntary scheme, that provides Australians with the choice of adopting a digital ID or using traditional forms of ID. We think that this an important feature that will ensure digital inclusion.

We are concerned though, that the Bill does not prevent private companies excluding the acceptance of traditional forms of ID. Some businesses might choose to decide only to accept digital ID as a way to minimise their risk of collecting data on individuals, or because it is a more reliable form of identity. However, ARCA would not want to see individuals without a digital ID being excluded from accessing these services.

ARCA members want to ensure that digital IDs are available for all consumers who want to obtain one. For that reason, we encourage the government to consider balancing the identify documents required for consumers to obtain a digital ID with the need to ensure the integrity of the digital ID system. That is, we want to make sure that it is not overly onerous for consumers to obtain a digital ID by providing an unnecessarily high number of identity documents. The more barriers put in place for consumers, the slower the uptake of digital ID.

Similarly, ARCA members are eager to ensure that consumers who may not have access to traditional forms of ID, e.g. some indigenous Australians or newly arrived migrants are supported to obtain a digital ID rather than prevented from doing so. Again, this requirement needs to be balanced with the integrity of the system. However we want to make sure that as many people who want a digital ID are able to easily obtain one.

We would welcome the opportunity to discuss this submission further.

Yours faithfully
Elsa Markula
Chief Executive Officer