10 October 2023

[redacted]

Consultation on the Digital ID Bill exposure draft and draft Digital ID Rules

IDCARE supports the government's vision for a Digital ID that provides individuals with a simple and inclusive method for verifying their identity in online transactions, while protecting their privacy and the security of their personal information.

IDCARE's primary concern is that the challenges present in the current analogue systems are further amplified in a 'twin-track' digital-analogue ID system, rather than addressed by the new Digital ID scheme. Gaps in the current legislation include:

- Ownership of the information, biometrics and Digital ID and a right to erasure;
- Minimum response standards where there has been misuse or exposure;
- Capacity to flag identity fraud (beyond simply erasure/deletion);
- Deceased people's information and Digital ID and the rights of their representative;
- Sufficiency of detail in relation to how vulnerable and 'low proofing' community members can benefit from participation.

We also provide suggestions to strengthen the deactivation provision.

Our submission focuses on those areas in which IDCARE has direct experience from working with victims of cyber incidents and fraud; it does not respond to all questions in the consultation.

## About IDCARE

IDCARE is Australia's national identity and cyber support community service. Each year IDCARE is asked by regulators or entities who experience privacy breaches to support impacted persons to respond to the compromise and misuse of their personal information. Since the commencement of 2023, IDCARE's national case management centre has received more than 200,000 phone calls from individuals concerned about the breach of their personal information. This includes breaches that originated from within Government or government agencies or may touch upon Government in terms of effective response and remediation.

Community members receive independent and expert advice from our Case Managers, to help them understand the risks and take steps to address their information exposure or misuse. No other organisation provides the specialist allied health and technical care directed towards crimes of deception. We do not seek to replace or act as a surrogate for notifying organisations, IDCARE services should be seen as escalatory and preserved for those community members who believe their information has been misused.

[redacted]

## Observations and recommendations

### *Learning from analogue system challenges*

*Recommendation 1:* Digital ID legislation should set minimum response standards in the event of an exposure or misuse.

The Bill Objects (cl 3) suggest by inference, that the current ID system is fractious, accommodates little user choice, and advances practices in the production, consumption and usage of personal information that are limited in their protection of privacy and the security of personal information. This inference is correct. But there are considerable gaps in the exposure draft legislation that if unaddressed, will likely mean that the present analogue challenges are further amplified in a 'twin-track' digital-analogue ID system.

This reform is an opportunity to highlight the deficiency in the current Trusted Digital Identity Framework in not setting out robust minimum response standards for users of digital ID (i.e. the consumer). Without further work in the space, the consumer friction experienced in the analogue world will repeat itself in the digital world.

Around three quarters of community engagements to IDCARE's case management services come from people who are the first to detect that their identity information has been compromised, and in many cases, used to commit crimes. From researching this environment it is apparent that this inability to detect ahead of individuals is a continued by-product of a system that places little emphasis or acceptance that community members play a critical detection role. "The system" repeatedly fails to embrace this reality and actually support the community in this role through providing efficient channels of remediation and response. A digital identity system provides a great opportunity to right this wrong and embrace the fact that the individual is critical in the protection and resilience of the overall system.

### *Additional processes*

*Recommendation 2:* Digital ID legislation should acknowledge what, if any, additional identity and/or verification processes are to be imposed on consumers and their likely impacts.

The draft legislation is silent on whether relying parties can impose additional identity and/or verification processes on their users, which may undermine the intent of the Digital ID protections. If the legislation does not explicitly prohibit relying parties from imposing their own additional verification and data collection requirements on users, it is assumed this will happen.

Prior work from IDCARE reveals that this is likely to be strongly influenced by the "riskiness" of a transaction. Put simply, the greater the assessed risk a transaction has in terms of likelihood and consequence of the wrong identity being consumed (relative to the value of the product or service or account to be accessed), the higher the proofing standard will be imposed. This by its very nature is a strong policy caveat to the public discussion on the benefits of a digital identity system. Put simply, there are efficiencies to be gained in not having to re-verify identity credentials as long as the consuming organisation does not impose other additional proofing or verification requirements on the consumer.

### *Currency and accuracy of identity information*

*Recommendation 3:* Delegated legislation or rules should provide an unambiguous requirement to validate against current sources of identity information in a timely way.

A further consideration is the focus on the currency and accuracy of the information consumed. When IDCARE supported community members impacted by Optus, Medibank and Latitude, there were parallel statements being made publicly by Ministers across States, Territories and the Commonwealth about the benefits of replacing a licence card version number and the apparent protections in doing so. In practice,

IDCARE's ongoing testing of the identity response system revealed that despite community members having replaced their licence in accordance with these public statements, the consumption and acceptance of the historical details was still apparent in many cases. This was particularly evident where service providers relied upon identity agents or brokers to verify a customer's details which clearly did not utilise current national verification systems.

In other words, the reality is that many hundreds of thousands of Australians are likely to remain exposed where identity information brokers and consuming entities choose not to verify against a current source of identity information (such as the document verification service). It is not likely that an arbitrary timeframe of 5 years to re-validate a digital identity is sufficient, particularly given in the last 18 months more than two-thirds of the Australian population have had their identity compromised.

*Most likely vectors of abuse and exploitation*

IDCARE has historically supported governments in their awareness of the likely threats and abuse scenarios that result in the exploitation of a digital identity system. Existing case examples as well as those drawn from overseas countries such as India and New Zealand, point to three most likely abuse and exploitation scenarios:

(1) End-user device exploitation – the exploitation of smart phones has emerged as one of the most common means by which people have their analogue identity information compromised and exploited. This could be as simple as the end-user not updating their operating system; it was recently reported in a recent iOS update that if not acted upon could result in a remote exploit by a threat actor. Although IDCARE advises people to be wary of links and attachments on communications, in this recent example, the consumer need not have done anything to be exposed, except to not update in a timely manner.

(2) Scam compliance – several examples of scam compliance have been reported to IDCARE whereby criminals have convinced people to enrol in a digital identity service, only for the relying party products and services to be exploited by the scammers. Scam compliance is a behavioural term that means that an individual is believing a scammer and is responding to the demands of a scammer. IDCARE has observed continued trends in relation to scammers and identity thieves capturing liveness test information and other data attributes known to be used in a digital identity enrolment setting. The controls and systems in place to verify and authenticate the end-user will not reveal that the community member is part of a scam. The prevention and treatment here is in relation to raising awareness of the risks relating to someone encouraging digital identity usage and an ability for the digital identity system to alert the relevant consumer of the abuse of related products and services. In other countries IDCARE has previously observed the targeted abuse of vulnerable persons with such scams, particularly in accessing Government benefits and tax refund schemes.

(3) Alternative Enrolment Channel Exploitation – there is a clear need to address the potential barriers for vulnerable or under-credentialed individuals to participate in the digital identity system, in order to maximise participation and social equities. As digital identity uptake grows, there may well be a temptation to deny access or renewal of identity credentials or other services without a person having to do so via a digital identity channel.

    While mandatory enrolment is not proposed in this reform, if other countries and Australian States are an indicator of the inevitability of policy choices, it is quite conceivable that a future decision may be made on this footing. To pre-empt both the need to support vulnerable and under-credentialed community members, and a shift in policy in terms of exclusive use of a digital identity to access certain products, services or credential renewal, the Government's work on examining alternative enrolment (and participation) channels is critical. This will, inevitably, lead to the exploitation of such

channels and finding the right balance between supporting participation across the community with the right level of control and response presents as a complex and necessary challenge to address.

In IDCARE's work across remote communities, there are a number of common customary practices that would benefit from Government's understanding of norms and how these may influence future decisions in relation to access. In recent work performed for the Department of Home Affairs, IDCARE identified certain customary practices across communities that present as good opportunities for Government to support community members and community touch-points in their facilitated engagement with community members who seek to engage in the digital identity system. It was commonplace for IDCARE to witness in some remote communities "identity custodians". These are trusted persons in the community that support identity enrolment and storage of identity information on behalf of community members. On the face of it, some of these practices may indeed by contrary to government and industry terms and conditions for the enrolment, protection and access of such credentials. But these practices are nevertheless critical for the ongoing functioning of such communities and their participation in the identity system.

*Recommendation 4:* Digital ID legislation should address the potential barriers for vulnerable or under-credentialed individuals to participate in the digital identity system, and ensure that people without a Digital ID will not be excluded.

(4) Third-party Identity Service Provider Exploitation – ongoing monitoring by IDCARE of hacking and ransomware groups continues to identify a strong preference in targeting "identity credential honeypots" including Managed Service Providers, accountants, and law firms. These stakeholders are effectively intersection points where data obtained from businesses, government and community organisations are vast and provides a strong criminal return on investment for the acquiring of identity credential information. We would see identity service providers as being an example of these honeypots and a likely target of hacking groups in the tapping into strong identity credential veins of information.

Existing legislative obligations are in place and IDCARE notes the ongoing consideration by Government of privacy reforms. The design of our digital identity system must anticipate the targeting of these providers and Government is encouraged to think carefully as to the sufficiency of protection and response given the inevitable and enduring interest by hacking groups in their business purpose.

Observations of recent breaches involving managed service providers highlights the complexities associated with what entity owns the breach response, whether the assessments of serious harm are actually genuine given the conflicted nature of such events for the breach entity (they derive their own assessment), and the appropriateness of protection and response measures taken. A breach of an identity service provider or other stakeholder in the identity system, would benefit from specialist advice and proactive engagement by an independent third party, such as the Digital ID Regulator.

It is apparent from ongoing engagement with privacy regulators, that there is little appetite at present for these entities to be more involved in guiding and advisory of a breach response as the breach is unfolding. However, in not extending a more independent view of the risk of harm and the appropriateness of response as and when events are unfolding, and waiting for a shortfall or resultant inadequacy of response, clearly defeats the overall Parliamentary intent of having such legislation (i.e. to reduce the harm to the community from such breaches).

*Recommendation 5:* IDCARE encourages the legislation to provide for independent and expert assistance to be extended to digital identity stakeholders when breaches occur.

*Digital ID and information ownership*

*Recommendation 6:* The Bill include an explicit statement of ownership.

The draft Bill, rules and reform guide are silent as to the ultimate ownership of the digital ID, personal information and biometrics. Ownership becomes an important issue in the response to the compromise and/or misuse of an identity credential; a digital identity would be no different. For example, a model whereby a person who has to rely on the actions of other parties to determine the extent to which their personal information has been accessed and misused is often confronted with considerable bureaucratic practices that do not lend themselves to the criticality of the issue that person confronts.

It is commonplace for victims of identity compromise and misuse to have to complete *Freedom of Information Act* or equivalent State legislative processes and wait up to 30 days or more for a response when crimes in their name are literally unfolding before their eyes. Victims of these crimes need immediacy in terms of responsiveness. They don't want to report to Government using an online form that at least nine out of ten times leads to no tangible response. They don't want to join a queue of people who are not having crimes committed in their name or be beholden to decisions from stakeholders that are made in ways that do not acknowledge that the actual credential or details is not 'owned' by the individual.

For example, Australian travel documents under the *Australian Passports Act 2005* are owned by the Commonwealth and not the person who has paid for their passport. Ownership becomes an issue when actions are either taken unilaterally by Government in response to a perceived risk to the travel document holder or when the person with the travel document seeks actions to be taken by others. An ideal scenario in the digital context is that consumers have technology solutions that assist them to determine when their identity credential has been consumed and enables a much more citizen-centric means of responding and protecting against threats that are thwarted over concerns about identity credential ownership.

*Erasure right*

*Recommendation 7:* The Bill include a right to have any information destroyed (in addition to the right to request deactivation) should an individual wish to withdraw their information entirely from any entity or shared provider to which they have previously given consent.

The draft Bill does not include a right of erasure, which would more clearly follow where it is clear that the individual user owns their identify information and Digital ID. We acknowledge that there is a right to request deactivation and a requirement to destroy information once the entity is not required or authorised to retain the information. Nevertheless, we recommend that there be an explicit right to have any information destroyed (in addition to the right to request deactivation) should an individual wish to withdraw their information entirely from any entity or shared provider to which they have previously given consent.

*Deactivation requirement (draft Bill, cl 28)*

*Recommendation 8:* Deactivation provisions refer to individual's representatives, set a notification obligation, and define 'as soon as practicable'.

We are concerned that the deactivation provision does not set out sufficient obligations on the Digital ID entity and ensure people are fully informed about the response to their request. We propose three additions:

1. The provision currently refers only to 'the individual', we recommend broadening this to *'the individual or their representatives or nominees'*.
2. The provision does not set any notification obligations, we recommend that entities be required to provide notice (or attempt to provide notice to the last known contact details) that the deactivation has been completed.
3. Set an outer limit for the meaning of "as soon as practicable" in responding to the request. For example, "as soon as practicable but no later than 14 days after the request is received.

### *Capacity to freeze Digital ID or flag identity compromise (rather than erasure/deletion)*

*Recommendation 9:* The Digital ID legislation should require providing the capacity to freeze the Digital ID.

IDCARE has heard from thousands of community members about how difficult it can be to regain control of their identity or accounts once there has been takeover, we have referred above to the slow rate of response systems when individuals are experiencing misuse. We suggest a mechanism for clients to be able to flag that their identity or credential or biometric information has been compromised to put an immediate freeze on their Digital ID. We make this recommendation with a strong caveat that it is the consumer that makes this choice, and not the credential issuer or other entity, and that such an avenue is readily accessible, available and confirmed.

### *Age of access*

IDCARE supports the proposal to align Digital ID scheme access with age of access to relevant entities, such as the age that a young person can independently apply for a Tax File Number.

### *Deceased people*

*Recommendation 10:* The Digital ID legislation should refer to deceased individuals and their representatives.

We note that the Bill is silent on deceased people. Our experience is that it is critically important for this to be explicitly contemplated, and we recommend that deceased people's representatives be included in rights to seek erasure and/or deactivation.

### *Threshold for creating and amending Rules without consultation (cl 158)*

*Recommendation 11:* The threshold for creating and amending Rules without consultation should be narrowed.

We are concerned with the threshold of at which the Minister can make amend the rules without consultation is too broad and should be further defined or narrowed. We acknowledge the need to maintain agility in the context of a fast-moving environment. Nevertheless, being *satisfied of an imminent threat or a hazard with a significant impact* can both be interpreted broadly. One option would be to narrow the threshold further with a second limb, such as, a requirement that exceptional circumstances make proceeding without consultation justified in the circumstances.

### *Funding and Sustainability of Support Services*

*Recommendation 12:* IDCARE encourages Government to consider ways in which identity verification and authentication service costs can include an IDCARE component so that the service scales with the identity usage and participation.

Funding arrangements with the Commonwealth require urgent consideration. Around 40% of IDCARE support services for the community is in response to demands by the Commonwealth. It is inevitable that the creation of a twin-track digital-analogue identity system is only going to further increase the demand from the community in redressing compromised and exploited identity credentials for the reasons stated in this submission. As a joint-industry-government and community collaboration and not-for-profit established in 2013 in response to the then Council of Australian Governments identity security strategy, IDCARE has never received Government grants or been able to sufficiently scale our community services adequately in response to the demands from the Commonwealth (community members referred to IDCARE by the Commonwealth or who have experienced a Commonwealth related identity exploitation event).

IDCARE's community support should scale with the participation of the identity system. But it does not. To pay for our specialist services and ensure the community does not pay, IDCARE needs to produce reporting and other incidental services to government and industry in order to reinvest into our frontline identity security community work. IDCARE is confronting a situation before then end of this calendar year where Commonwealth funding to directly address Commonwealth–eligible community members will cease for the financial year. Examining ways in which this critical service is able to be delivered to the community in a way that scales with the threat and impact is a critical consideration of Government and requires urgent attention.

[redacted]

We look forward to the outcomes of this work.

[redacted]