



**Feedback on the proposed Digital ID legislation **

Date: 10 October 2023


To whom it may concern,

Firstly, we appreciate the opportunity to provide our feedback on the proposed Digital ID legislation. As the leading identity verification provider in Australia, [REDACTED] is passionate about ensuring we provide our expert feedback to help shape a better tomorrow for all Australians that aligns with our vision of “making the world fully accessible to real customers; and to no one else”.

We believe that the advancements in digital identity and the underlying standards are crucial to help solve major risks we face today around identity crime and more broadly organised crime. We commend the developments to date around the Trusted Digital Identity Framework and getting the Digital Identity Bill progressed further after being stalled. We agree that implementing a secure, trusted digital identity can drive economic development and productivity. A robust economy-wide digital identity has the potential to simplify individuals’ interactions with government and private sector businesses, and streamline authentication and verification processes for businesses and other service providers, whilst preserving the privacy of every Australian.

Whilst we positively support the Government putting forward the new Digital ID system as one of the ways to respond to the increase in data breaches, this only provides a voluntary alternative rather than addressing the current issues we face today in relation to identity crime.

Identity crime continues to generate large profits for offenders while causing major financial losses to the Australian Government, private industry and individuals. Driven by the need for Australians needing to provide ID documents for identification verification purposes when applying for services, whether those are federal or state/territory government services or services provided by the private (business or not-for-profit) sector.



█ has the technology today to mitigate identity crime, however, we do not have the required regulation and standards to consistently leverage the technology across public and private sectors. The technological advancements in AI driven biometric technologies means technology can outperform previous “trusted” approaches in correctly identifying an individual to ensure they have a valid Government issued photo identity document, they are a real person and they are the right person. This is why we have continued to provide our expert feedback on the Trusted Digital Identity Framework as part of our accreditation and also agitating private industry regulators. So whilst this is an important step to rebuilding public trust by having appropriate legislation, the trust will come in ensuring the underlying standards and requirements meet the highest standards and align with internationally accepted best practice.

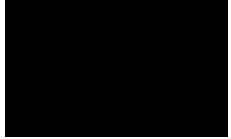
In light of our internal review of the Digital Identity Bill Legislation, the Digital ID Accreditation Rules and the Digital ID Accreditation Rules, please find below a summary of our feedback (in no particular order):

Independent regulators

- ∨ There are new regulators, e.g., ACCC, who are not familiar with digital identity, identity proofing technologies and governance of them. So do they have the “muscle memory” and/or expertise to appropriately provide trust around the privacy and security of digital IDs?

Digital ID Standards

- ∨ Trust is predicated on the strength of the underlying standards that ensure solutions are reliable, safe and secure. The current standards don’t address the current issues we discuss with our clients in relation to identity crime and/or fraud.
- ∨ These standards/rules are crucial to the effectiveness of the entire Digital ID System and a major problem in identity verification today using physical IDs. We need improved regulation and guidelines from not only the Digital ID System regulators, but also have these aligned with industry regulators (AUSTRAC, ARNECC, ACMA for instance) around what good identity verification looks like for consistency. This is going to be paramount in how Digital ID’s are interoperable in the private sector given TDIF IP levels don’t easily correlate with industry regulations.
- ∨ For instance, the National Identity Proofing Standards have not been updated for some time or in relation to advancements in technology and are below that considered internationally accepted best practice, e.g., under NIST Digital Identity Guidelines. The TDIF also has significant limitations in preventing fraud unless binding with the FVS (also not available in the private sector). For example, TDIF only allows for ID evidence validation using the data checking against an authoritative source (DVS) and does not cater/allow/provide



requirements for the "evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified (as per NIST)".


- \\ The Department of Finance interpretation of "biometric information" is misaligned with the globally accepted definition, which is also cause for concern in building trust and assurances in the regulators and the standards that they are trying to govern. See below for further feedback around the interpretation of "biometric information".

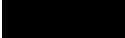
Weaknesses in Australia's privacy laws

- \\ Australia's privacy and data protection laws are not comparable to that of global data protection regimes, e.g., GDPR and EU does not deem the Australian's law to be adequate (see EU Adequacy decisions - noting New Zealand's are).
- \\ Without further improvements to Australia's underlying privacy laws they are not adequate for a launch of a nationwide identity system. The large number of privacy breaches compared to other Western countries is directly linked to the inadequate privacy laws in Australia. This needs addressing before the digital identity ecosystem is launched, otherwise there will be a large breach of a provider and that will undermine faith in the whole system.

Protection of biometric information

- \\ The Department of Finance deems an image of a photo ID to be "biometric information" using the definition from the National Identity Proofing Guidelines, e.g., a photo of a driver's licence would be considered biometric information. This interpretation also contravenes the TDIF's own requirements for remote identity proofing! We have provided this feedback to the Department of Finance.
- \\ The definition requires that it is "information" about a "measurable biological characteristic". The word "information" is key because it is not a mere picture that is capable of being measured, but information from that mere picture. This aligns with all other global definitions of biometrics which require some form of technical process or scanning.
- \\ This Department of Finance interpretation will also mean if you want to use a Digital ID in the private sector, it would not meet current record keeping requirements under either AUSTRAC Know Your Customer (finance) or ACMA verification of identity (telco), breaking the intent of interoperability.
- \\ IDPs should be able to use biometrics to both detect and prevent fraud attacks, as we consistently see across our identity verification transactions in Australia fraudsters having multiple accounts with the same face (prohibited



under paragraph 45.(2). As IDPs, like  have new fraud detection and prevention techniques that leverage one-to-many facial recognition algorithms.

Choice

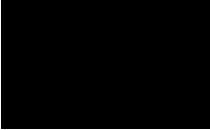
- \\ The Digital ID legislation will enable more choice of who you create a Digital ID with and where you can use it. First mover advantage is well known to be essential in capturing a consumer market.
- \\ The government already has two huge advantages over the private sector in persuading citizens to use its reusable digital identity: (1) myGovID is already prominently available for tax and state use cases; and (2) the government is a brand that is “inherently trusted” - noting however there are publicly known weaknesses with myGovID both from fraud being created using a “trusted identity” and accessibility issues from an independent audit of myGovID, which has diminished trust in the Government..
- \\ The proposed order of the phases has myGovID being unleashed on the private sector, a phase before private sector IDs can be used in the public sector. This will give myGovID another huge boost in consumer adoption before the private sector IDs can get going. Is it right or fair that the government is giving itself such a huge advantage over the private sector in this way? Especially given the independent regulator is the ACCC and they continually are assessing whether a monopoly is being created unfairly around providing all Australians choice.

Using a Government ID in the private sector

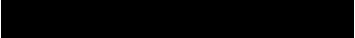
- \\ Whilst the concept is great, there is a misalignment with TDIF and what industry regulators require when it comes to identity verification. They are all following different standards and requirements making it very hard to provide a consistent, reliable and secure digital ID experience for all Australians to trust.
- \\ Not all State’s mDL were built adhering to the internationally accepted standard for mDL making them not interoperable within the private sector. This goes back to ensuring a common set of standards and requirements are adhered to that are focussed on the identity proofing process of both physical and digital identity documents. So there must be state and federal alignment in order for a digital economy to thrive.

Lack of use cases

- \\ As the experience with TDIF has shown, a reusable identity eco-system needs use cases more than anything else that diminishes the value of having accredited services.. For TDIF, there is not a single non-government use case yet that is being used consistently. NSW same day alcohol is due to be first one in June 2024 (noting, Liquor and Gaming NSW have delayed this twice already).

- 
- ∨ The government decided against the advice of the eSafety commissioner and will not require age verification to stop young children accessing pornography. Ignoring the question as to whether this was the correct decision, it is an opportunity missed for a compelling use case for a private and secure digital identity.

High standards for the Accreditation

- ∨ As one of the three TDIF accredited companies, we at  can attest to the high standards that TDIF holds companies to. It is imperative that these high standards are maintained in the accreditation scheme for digital identities. In the UK, by contrast, the assessors for the UK trust framework are private companies and the standards of testing are much lower.

Accessibility

- ∨ Very high standards should be mandated for accessibility. Some suggestions are:
 - At least WCAG 'AA' rating for all biometric and liveness solutions. There are providers in the market that do not meet this, and that means less choice for blind or visually impaired people.
 - The biometric technology works as well on the low end of devices as the high end of devices, so removes any sort of bias to devices, timing, document coverage or demographic.

Australia first

- ∨ The handset and operating system market is dominated by US giants (and Samsung). There is a real risk that Australia's identity ecosystem will be dominated by handset and operating system manufacturers unless the Australian government acts to stop this. Some thought should be given to promoting and protecting Australian identity businesses in Australia's own ecosystem.

Thank you again for the opportunity to provide our feedback.

