Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

Your name	Lisa Schutz
Your organisation	[redacted]
[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?	
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?	

Page # of guide	Question	Your response
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	There needs to be harmonisation with CDR Accreditation. A concept of what being accredited in one regime means for the other.
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?	No. Biometric information is not sufficiently protected. There are many options for strong authentication without biometrics. The sanctity of the citizen's person requires that they not be made to use elements of their physical selves which are by nature not capable of re-issue – to authenticate themselves. To be clear, biometrics, is not actually bullet proof. The risk is simply moving to the citizen in an irrevocable way and leads to a dystopian reality. Not a risk. The large tech platforms do understand this. Compelling sharing of biometrics is not a comfortable position for a Government to adopt. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/biometrics-keep-your-fingers-close/ba-p/1276934
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 restriction on disclosure of biometric information?	See above. No.
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	

Page # of guide	Question	Your response
	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?	
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	Insufficient. Two additional mechanisms are needed: - **Add Citizen Receipts to the process** (which would be provider regardless of which ID provider/method you use): Just like when you purchase goods in a store – you get a copy of your receipt as does the corporate you are dealing with. Currently the Digital ID framework has no such concept of a “receipt to the consumer”. We suggest a new type of provider be added to the Trusted Digital ID Framework – ID

Page # of guide	Question	Your response
		Monitor. We have prepared a separate submission to explain this in more detail. This ID monitor would be agnostic to your chosen ID method for a particular transaction and makes sure that citizens know when the ID is being relied upon in real time. This will cut the cost of ID theft dramatically. See Submission Part 2.0. - **Know Your Provider measures should be a requirement too:** The requirement that corporates relying on Digital ID provide a two-factor mechanism to identify themselves when they reach out to a consumer - this would stop most scams in their tracks. For instance, if a telco calls me, they push a notification to their app on my phone or they email me. If they email me, they SMS at the same time. This protocol would dramatically cut fraud. **Opt-in biometrics only:** Thirdly, as per points in #21, biometrics should <u>not</u> be required for strong authentication. This transfer risk to the citizen unnecessarily. This requires an additional aspect to section 47. Which is that while it's fine to collect biometrics to support ID verification for Government relying parties, that is only OK if the individual freely gives their consent to supply biometrics. It would **not** be freely given consent were the Government to mandate use of biometrics. Hence there needs to be a companion section that makes sure that biometrics are never mandated points of identity verification for any relying party in Australia.
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	The mistake made by this legislation is not tackling the demand side of storage of Identity Documents. In parallel, a requirement should be on all regulators and agencies to <u>not</u> require storage of identity documents in the first place and require cleaning up of databases to occur. Any regulator involved in a sector that stores identity data has a role to play here. Thinking here of APRA, ASIC and AFCA in Financial Services and AUSTRAC in general. The fact of an identity check and the provenance of that check should be sufficient.

Page # of guide	Question	Your response
		It should be a regulator checklist to make sure that proper data governance is being applied. If this is not done, then migration to Digital ID will not happen to minimise risk to the citizen and community.
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 certainty for accredited entities while maintaining currency?	Principles based as much as possible rather than prescription. Ideally, let industry drive the standards with Government as the orchestrator. We would contrast the approach being taken in NZ, with their Consumer Data Right versus the heavy prescription in Australia. In NZ, (see role of NZ Payments Centre here) the Government sets the framework, the rules and laws but the industry sets the standard. That leaves the role of the Data Standards Body as reviewing industry produced standards rather than setting them.
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?	Verifier recommends that the Consumer Data Right Standards Body and the Australian Digital ID Standards Body be run from the same organisation. Both are part of “rewiring the data flows in the economy” and the gap between Digital ID policy and consented data sharing has been going on too long. And, as per #34 above, a lighter touch with industry setting standards wherever possible, and where that is not possible, a principle not prescription approach, is suggested.

SENATOR THE HON KATY GALLAGHER
Minister for Finance
Department of Finance
One Canberra Avenue
FORREST ACT 2603
AUSTRALIA
By Upload

Verifier Australia Pty Ltd

Submission to The Department of Finance on Exposure Draft Digital ID Bill 2023

About Verifier

Verifier is a permission-based private data exchange platform for regulated markets that applies Privacy-by-Design principles, respecting the information security needs of consumers and income data providers. Our clients include banks and non-bank financial institutions.

Verifier is a RegTech firm (and founding member of The RegTech Association) and an Accredited Data Recipient (unrestricted) in Australia's Consumer Data Right.

Purpose of Verifier's submission:

Verifier believes that the TDIF is a strong start **but could be enhanced to create the fraud resilience** we need in the economy right now, especially after the data breaches of 2022 and 2023.

Two things are needed urgently:

- Firstly – add the **role of ID Monitor** to the TDIF and use that to provide alerts to citizens whenever their DVS credentials are accessed.
- Secondly, unleash the value of **Single Touch Payroll** as an attribute.

1. Verifier suggests future proofing the Bill for addition of the ID Monitor role to the TDIF

Verifier welcomes the opportunity to make this submission and to recommend that the current Digital ID Bill include the ability to design and implement "citizen ID receipts" regardless of whether or not the identity check occurs with a TDIF Identity Service Provider.

We would like to think that **Section 14(1)(d)** allows that this new type of role be created – ID Monitor Provider - however, we would like this considered expressly before the Exposure Draft is finalised.

Why this ID Monitor role matters: *ID receipts to solve the impact of ID theft.*

If I go to a store and transact, the corporate I am dealing with offers me a receipt and they keep one too. A fundamental shortfall of the current Trust ID framework is that it has no concept of citizen "ID receipts". There is no transparency to the citizen of when their ID is being used. If it's a use they know of – great. But how can they know if their ID is being mis-used.

If the role of the ID Monitor is introduced, any ID check that contacts either the DVS or Face Verification Service then pings the ID Monitor and alerts the possessor of those credentials that their ID is being looked at. This would apply to at least all non-Government uses of ID checks.

Verifier recommends that, to de-risk the system, Relying Parties pay for both the service of their ID Service Provider (who access ID for the corporate) AND also pays for the services of an ID Monitor (who provides a separate notification to the citizen via their chosen ID Monitor pathway).

That means that one ID check would trigger activity in an Identity Service Provider AND an Identity Monitor. So if that is ID theft, the Identity Monitor Provider will alert the person. And, if it's a legitimate check of ID, then as we often do these days for accessing cloud providers when we are on the move or do something different to our normal pattern, we are comforted by getting a second factor confirmation of the transaction we are doing.

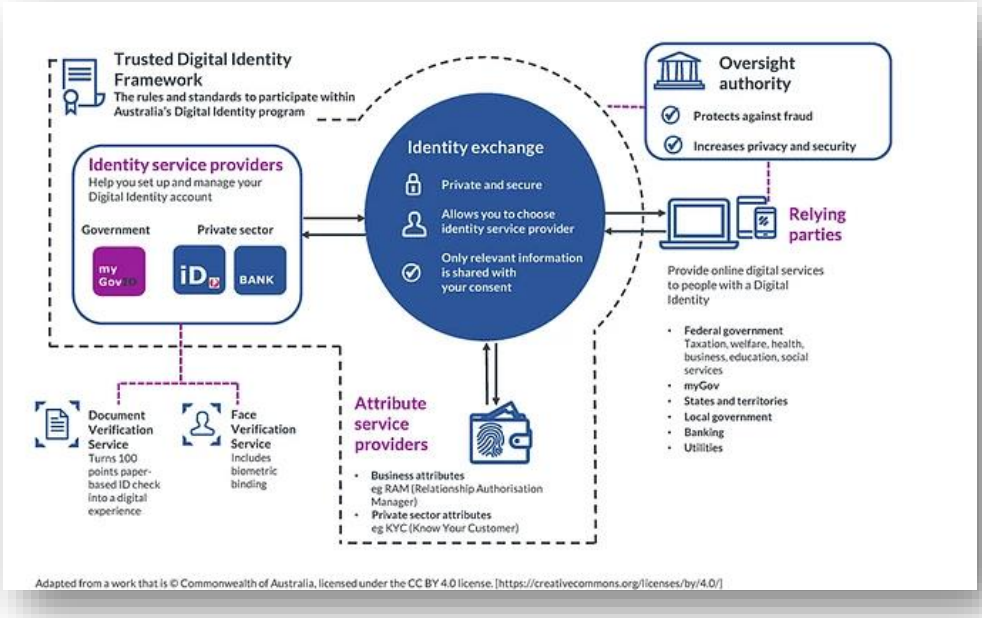
We get two factor notification this for checking our photos online, why not for our most highly prized digital asset?

Global Leadership

If Australia added this ID Monitor role, we would have a global opportunity to create a new standard for digital ID management that is truly Privacy-by-Design. And, in doing so, Australia would reinforce the presumption of the right of consumers to control their digital destiny - which is consistent with the direction of CDR policy.

ID Monitor - fits within the existing Trusted Digital ID Framework

The diagram below helps explain the point – you see the Document Verification Service icon – the simplest way to proceed would be that every time the DVS is contacted an Identity Service Provider can then return the Yes/No response to the Relying Party – but they also have to check with the Identity Monitoring Providers to see if the citizen wants to be told when their credentials are accessed.



Creating the ID Monitor role solves the consequences of data breaches like those of 2022 and 2023

Yes, application-based ID services are great, but they do not solve for the universe of ID transactions going on in the economy. Adding the ID Monitor role puts a lid on ID theft using the TDIF.

Let's use TDIF to solve the cyber threats of right now.

2. Single Touch Payroll and an additional attribute – via Sending Service Providers

Verifier has previously briefed Treasury on the potential for Single Touch Payroll data to support the TDIF. This does not require designation under CDR but our recommended approach harmonises to CDR and would be available to the TDIF.

We are happy to connect the dots should Single Touch Payroll be of interest as an identity attribute. Our view is that Single Touch Payroll data should be used as an identity attribute – since asking someone when they get paid is not a data point that is stored in the person's wallet – and therefore, asking for confirmation of pay date is a mitigant to ID theft. This might mitigate the need for biometrics in many cases and help solve for ID theft.

We would be happy to discuss any aspect of our submission with you or your staff. Please contact me in the first instance.

Sincerely
Lisa Schutz, CEO
Verifier.