Senate Standing Committees on Economics Inquiry

Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

19 January 2024

EQUIFAX

Equifax is a data, analytics and technology company providing risk and due diligence solutions with particular strengths in credit risk, consumer identity and fraud, and employment screening solutions. These assist Australian businesses to not only meet legal obligations (such as responsible lending, or Know Your Customer) but also to mitigate risk, such as credit and fraud.

Equifax supports the Digital ID Bill 2023, in principle, but suggests amendments are needed.

- Encourage faster private sector participation in Digital ID.
- More explicitly support fraud prevention purposes.
- Recognise the role of entities who, as implementation service providers, will enable widespread business participation in Digital ID.
- Reduce the complexity of provisions, including by use of already-legislated provisions.

EQUIFAX AND THE DIGITAL ID BILL

Equifax perspective on the Bill is based on our experience as a leading provider of ***identity verification, fraud prevention*** and ***employment screening solutions***.

Identity verification and fraud prevention solutions

- More than 600 Australian businesses use Equifax to enable them to verify people's identity, including but not limited to meeting Anti Money Laundering/Counter Terrorism Financing (AML/CTF) KYC requirements.
- Supporting this, Equifax is one of the two largest accredited private users of the Attorney General's Identity Matching Services.
- In addition to identity verification services , Equifax has the broadest range of fraud prevention and detection solutions, including but not limited to device intelligence, email risk, knowledge based authentication, death check and visa check.
- As part of our suite of fraud prevention searches, Equifax has been the custodian of Australia's largest known fraud exchange for over 20 years, helping the fraud fighting community to better detect and prevent application fraud.

Employment screening services

- Australian organisations, including hospitals, use our employment screening services to ensure the people they are about to hire, or already employ, have the right credentials to work.
- These credentials (or attributes as described in the Bill) may include a valid visa; a clear working with children check; and valid registration as a medical practitioner
- As an approved vendor to the Australian Health Practitioner Regulation Agency (AHPRA) we are able to confirm that medical practitioners (nurses, dentists, general practitioners and surgeons) have a valid registration to practise.
- Equifax is accredited by the Australian Criminal Intelligence Commission (ACIC) to enable consented access to a Nationally Coordinated Criminal History Check. In addition we have agreements with state registers to confirm clear Working With Children checks.

Adoption of Digital ID - implementation phasing

Multiple submissions to the exposure draft Bill have commented on the proposal for a four staged rollout, with concerns about the lack of timeline for each phase and the resultant delay of private sector participation in the ecosystem.

Equifax supports digital identity and seeks to leverage the leading role we have played for over 20 years in Australia's identity and fraud landscape to support the efficient and effective rollout amongst Australian businesses and community.

For Equifax, an overarching question for the Digital ID Bill is how to drive mass adoption amongst Australian businesses and the community.

Success for the adoption of accredited Digital ID will be reflected by the depth of its penetration into the economy, measured by the number and diversity of businesses utilising it.

There is a strong appetite across the private sector for more robust digital identity solutions; this not only protects consumers against cyber incidents but also helps deter fraud. Wide participation by the private sector will in turn support faster consumer adoption of trusted identity systems.

Delaying the entry of accredited private identity providers will reduce the incentive for additional participants. Lacking any clear timetable for the phases, and in the face of increasingly sophisticated identity fraud, large businesses will develop alternate mechanisms, which in turn perpetuates a mixture of different identity regimes undermining consumer confidence when dealing with business and government.

Deletion provisions in the Bill [50 (5)] will inhibit fraud prevention and investigation

Closely linked to identity verification solutions are fraud prevention measures. Provisions in the Bill relating to the deletion of biometric information [Section 50 (5)] will impede fraud prevention

The Bill recognises the role biometric information plays in deterring fraud by allowing accredited entities to retain biometric information for the purposes of preventing or investigating a Digital ID fraud incident[1].

However, this is then restricted by Section 50 (5), requiring destruction immediately after the completion of investigations or 14 days after collection - whichever is sooner.

[1] Chapter 3 Part 2 Division 2 Section 49 (8) (b)

The timeframe provided is highly problematic; essentially fraudsters will know to wait 14 days after collection to then perpetuate a fraud, when any revealing biometric information will have been destroyed.

Fraud prevention should not be prohibited from using data profiling (53)

Under Section 53 (prohibitions on data profiling to track online behaviour) the Bill permit use of data profiling to improve IT systems and user experience; this should also permit use for fraud deterrence.

Additionally, we note section 53 prohibits data profiling of an individual by tracking online behaviour. However, this prohibition has exemptions [53 (3)] if it's for:

> *(a) is for purposes relating to the provision the entity's accredited services (including improving the performance or useability of the entity's information technology systems through which those services are provided); or*
> *(b) is for the purposes of the entity complying with this Act; or*
> *(c) is required or authorised by or under a law of the 21 Commonwealth, a State or a Territory.*

Equifax **recommends this provision be amended** to include an additional purpose, that of preventing, detecting or investigating potential fraud.

***

The problems with Section 53 and 50 raise the broader question of the role Digital ID can play in fraud and how best it can be extended to support fraud deterrence:

- We recognise there can be a tension between privacy concerns and the risks of retaining biometric information on the one hand and enhancing the ability to combat fraud.
- The Identity Matching Services Bill 2018 generated significant debate about the use of one-to-many biometric matching but on a more practical level, ensuring a biometric held on a document (e.g. face on a drivers licence) is not replicated elsewhere under a different names is critical to confidence in the integrity of the entire identity document system.
- Data breaches continue to happen at scale, deep fakes and AI generated images and sounds continue to evolve and the sheer numbers of identities compromised has created consumer fatigue. All this points to a need for a broader approach, one where transacting businesses are not solely reliant on verifying an identity via document or biometrics.

These are significant issues, but a coherent response is needed, particularly as passage of the Bill gives way to the creation of data standards and rules. As a way forward, **Equifax recommends the Government forms a consultative working group** with industry specifically to advise on how Digital ID can better support fraud prevention.

Role of implementation services when assisting collection of restricted attributes

The construct of governance around disclosing and collecting of restricted attributes needs to provide clarity on the role of implementation services, whereby a third party enables an entity (the Relying Party) to receive a restricted attribute (e.g. criminal history check).

The Digital ID Bill creates a legal framework for the disclosure and collection of attributes. These attributes include restricted attributes such as a criminal history check.

Restricted attributes are particularly important for employment screening purposes, not just at the point of employment, but also ongoing engagement.

As a provider of employment screening services, Equifax obtains, on behalf of a business, a criminal history check; this is then passed on by Equifax to the business, who then makes a decision on how it wishes to proceed.

Once employed, there are important reasons why restricted attributes remain relevant. Many hospitals in Australia use Equifax to continuously monitor that their medical practitioners - including surgeons - continue to hold valid registration.

Section 18 of the Bill sets out a series of conditions relating to the disclosure of restricted attributes to a Relying Party. These include security, fraud controls, privacy impact assessments and protections from further disclosure.

Under Section 9, a Relying Party is defined as:

> *...an entity that would rely on an attribute of an individual provided by an identity service provider or attribute service provider to:*
>
> *(a) provide a service to an individual or*
>
> *(b) enable the individual to access a service such as using their digital ID to verify themselves then be redirected to a particular service.*

Equifax is neither providing a service to the individual nor by virtue of using an Equifax solution are we enabling the individual to access a service. Effectively we are an enabler, an implementation capability, needed by thousands of Australian businesses to access a range of information to help manage risk.

A similar failure to recognise implementation enablers occurred with introduction of the Consumer Data Right and Accredited Data Recipients. While this was addressed by

subsequently creating carve outs under the CDR Rules, to provide certainty in the Digital ID Bill **Equifax recommends it be amended** to recognise entities participating in an implementation or enabling capacity.

Restricted Attributes - membership of a professional association

We note that Section 11 *Meaning of restricted attribute of an individual* includes information or an opinion about the individual's membership of a professional or trade association.

It is not clear why there is a need for this attribute to be cited in the same manner as a criminal record.

Membership of a professional association - or disqualification from membership - is critical information to an employer. We believe the broad remit given to Accreditation Rules can provide any necessary protection, but are concerned there could be unintended consequences from its inclusion as a specific item under Section 11 (1)(d) and **recommend it be deleted**.

Complexity of system design

An additional risk to the success of the ID system lies in the complexity, cost and compliance requirements necessary to participate.. While very large institutions may have the resources necessary, smaller and medium enterprises with less capacity may struggle, leaving the advantages of Digital ID beyond reach. In both situations, the cost of governance and compliance with Digital ID provisions may erode the business benefit from using it.

Equifax suggests the following measures can assist reducing complexity and improve governance:

Align security requirements with existing provisions legislated elsewhere

Industry will benefit from having consistency and alignment in provisions regarding common topics. Multiple legislation are likely to reference Digital ID, including the review of AML/CTF laws and the Privacy Act review.

One example of alignment regards security standards and cyber incidents.Equifax notes the recently released Australian Cyber Security Strategy 2023-2030 and the call to design and align common security standards.

The Security of Critical Infrastructure Act contains an existing provision regarding cyber security incidents and **Equifax recommends this should be adopted in the Digital ID Bill**. The proposed provision in the Digital ID Bill is too broad and will lead to unnecessary reporting burden.

Create repeatable principles

The structure of the Bill varies between highly specific requirements and in other instances deferring detail to Rules or by declaration of the Minister.

Equifax suggests the addition of repeatable core principles be created, in addition to the Bill's objects, in order to provide an overall framework. This may provide sufficient in lieu of detailed provisions and at the very least, can guide the development of rules and technical standards.

Measuring success - governance after implementation

What will a successful Digital ID scheme look like?

There are lessons to be learnt from the lacklustre embrace of the Consumer Data Right by consumers and business.

For Equifax we believe success should be reflected by the depth of its penetration into the economy, measured by the number and diversity of participating businesses. **The establishment of an advisory body with participation from industry is recommended**, **along with the publication annually of a variety of metrics, including numbers of users, and the sectors they come from.**