Senate Economics Legislation Committee
Inquiry into Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

Response to Question on Notice
Hearing of 9 February 2024

Topic: Bill impact on fraud prevention

Senator Dean Smith:
"On notice, can you elaborate on those two points: ***how the bill impedes fraud prevention*** *and the efficient checking of health practitioners' registration? If you can provide some additional information on notice in regard to that, that would be helpful"*

Equifax Response
Equifax is host to Australia's largest collection of fraud intelligence data, pooled from members of the Fraud Focus Group. This network aims to assist in the alerting of common trends in fraud activity, fraud patterns and market insights. Our customer's fraud prevention defences rely on these insights and customers reported they helped prevent $2.5 billion of attempted fraud in 2023.

Equifax's experience is that identity and fraud are inextricably linked and any legislation that contemplates how an identity is verified must also address the associated risk of fraud. Digital identity is not intended to be, and should not be used as, an indicator of potential fraud.

Defending against fraud is much broader than certainty about the credentials presented in identity verification. Fraud prevention seeks to manage risk. Identifying the risk of fraud is not a binary process, as fraud manifests in different ways as bad actors adapt their behaviour to exploit vulnerabilities. Managing fraud is ongoing and requires continual data collection and analysis to enable the detection of new patterns of potentially fraudulent behaviour.

Consequently, our view is the bill needs to acknowledge the risk of fraud possible in any digital identity system and make explicit provision for the use of data to enable the continuous process of fraud identification and prevention.

Today, Equifax helps businesses identify fraud by observing historical transactions for patterns known to have been associated with fraud outcomes, detecting attempted fraud in real-time.

One example of fraud prevention activity that would not be supported under the bill is velocity rules/identity takeover alerts.

Equifax searches for repeated use of a combination of attributes within one institution or across industry. If repeated uses within a period of time exceeds thresholds indicative of potential fraud, the next use of those attributes returns an alert. This is used to help industry catch:

- fraudsters shopping around, or
- money mules attempting to open multiple accounts within one institution or across multiple institutions

However, under the Digital ID ecosystem, the fraud prevention method described is not possible.

We believe Digital ID must continue or enhance existing fraud detection capabilities in order to continue to protect the Australian economy from the broad range of impacts of fraud.

As such, where the Bill has a prohibition on online tracking behaviours, and deletion of data after a certain number of days or months, there should be an exemption for fraud.

Biometric destruction

Efforts to understand systemic fraud are further hampered by deletion requirements relating to biometrics. We recognise the length of time a biometric should be held, even for fraud mitigation, must be reasonable and finite, but 14 days is insufficient and further consideration given to a longer time period.

Additionally, the Bill proposes that a biometric must be deleted even where an active fraud investigation is underway. This needs to be amended. Where a fraud investigation is underway - and these can take months, not weeks - the biometric must be retained regardless of when it was collected.