Identity Verification Services Bill 2023

Senate Legal and Constitutional Affairs Legislation Committee

27 October 2023

As one of the two largest Gateway Service Providers (GSPs) to, and as business user of, Identity Matching Services (IMS) we support, in principle, a legislated framework for private sector access to identity matching services.

Equifax notes commentary on the Bill has almost exclusively focussed on privacy considerations. Our perspective is that for the legislation to be successful, it must enable people and businesses to interact in a way that is an easy experience and reduces risk for both parties.

Since the start of the DVS in 2014, concepts around identity have broadened and deepened. Today Equifax combines identity, fraud and financial crime solutions to give businesses a single view of customer risk. Changes to capabilities - including availability of the Face Verification Service (FVS) - will stimulate further innovation.

The IMS reflects a decade-long partnership between the Government and intermediaries (GSPs) such as Equifax. Our views draw from a customer base that includes big banks, small credit unions, equipment hirers, betting agencies and telecommunications companies. The role of a GSP is not as a passive access channel pipe to the IMS, but a proactive manager of significant change, such as a three year process to introduce a new requirement for input of the card number on a driver's licence in addition to drivers licence number.

Equifax supports the FVS within the context of a competitive market for biometric solutions. Already, in relation to the draft Digital ID bills before parliament, there is a debate about the role of non-government identity services and Government credentials (myGovID).

Private sector biometric services are already in the market: Equifax conducted around 1 million facial biometric checks via private biometric services. Looking ahead, Equifax will compare the Government biometric service (FVS) with private sector services along the following dimension:

- Capability: private providers currently offer capabilities of a “liveness” test, document tampering assessment and optical character resolution as well as the capability to match a person’s biometric to non Australian issued documents.
- Complexity for accessing biometrics: the Bill details key obligations, but further details will be contained in proposed Participation Agreements still to be finalised.
- Price: which is yet to be revealed by the Attorney General’s Department (AGD).

A choice is being presented and a comparison will be made between private sector services and the FVS and they will be compared along these parameters.

This creates uncertainty surrounding the investment required to establish and maintain enhanced gateway service provider capabilities.

A successful FVS will be one that creates greater consumer confidence in biometrics; reduces fraud; fosters innovation and competition from private biometric services and attracts participation by Australian businesses.

We draw the Committee’s attention to a few provisions in the Bill that could be reviewed to support enhanced adoption.

Provision 41(b), requires an annual report to Parliament that includes, for the FVS, detailing the total number of requests; the names of the non-government entities that made those requests; and a breakdown of successful and unsuccessful requests by the requesting entity.

While the rolled up number of non-Government FVS requests is of public interest, as is which sectors are using the FVS, Equifax questions the relevance or necessity of revealing individual business volumes, correlated as they would be to business activity, such as applications for credit.

We recommend this provision be amended so that the volume of requests (successful or otherwise) made by an individual business not be published.

We note the Bill formalises a range of requirements for existing users of the DVS. Section 9 details obligations encompassing complaints, corrections, consents and data breach. These will be captured and detailed under proposed Participation Agreements for existing DVS Business Users required to be in place for access to DVS services (Section 15)

There are two ramifications of these provisions. Essentially the impact of compliance remains unclear, yet the deadline to be compliant is fixed.

Firstly, without a draft of Participation Agreements making clear the operational expectations of Section 9, it is difficult to determine what new costs may be incurred by Business Users and what capital expenditure is therefore required.

This similarly applies to Equifax as a Gateway Service Provider, a role that has a very significant commitment of expenditure and resources; we are unable to determine what new costs may be incurred and what capital expenditure would be required in 2024.

These additional costs and complexities are in addition to the yet to be released new fee structure proposed for transactions on both the FVS and the existing DVS.

To address this, we recommend the Committee call for the AGD to immediately release draft Participation Agreements (Business Users and Gateway Service Providers) for consultation; in addition, the Government should release the proposed FVS and DVS fee structure.

Secondly, under Section 15, all of this will be operational 12 months after Royal Assent - a DVS user without a Participation Agreement would then no longer be able to access the DVS.

This hard deadline could have consequences for the finance sector, which is reliant on the DVS to meet their AML CTF obligations.

We recommend the Committee supports a longer transition period. The DVS has been part of business processes for a decade[1] and while it may be desirable to embed it within a legislative framework, a compliance date of 12 months is insufficient time for compliance.

[1] Confidence in the operation of the DVS can be drawn from a 2019 OAIC report which audited 20 DVS users and found the most common recommendation was to improve the readability of their privacy policies.

Finally, in the broader context of identity capabilities available to business, including the Document Verification Service, there is an opportunity to harmonise identity resources for identity verification and reduce complexity for business.

The Commonwealth Electoral Roll has a 2006 prohibition on use for any verification purpose other than AML/CTF requirements. This does not apply to passports, visas or drivers licences which can be used for any reasonable identity need. Outside of the DVS, a similar restriction applies to the use of credit reporting information for identity verification.

While not within the Bill's provisions, **we ask the Committee highlight the need for the Government to take steps to consider allowing their use.** Such a move would be complementary to this Bill and the draft Digital ID bills out for consultation.

APPENDIX - additional background

Equifax and identity

First established in 1967 to provide consumer credit reporting information, Equifax is a data, analytics and technology company and a leading provider of risk solutions, including identity.

Since the start of AML/CTF laws, our role as a provider of solutions to enable the finance sector to meet various compliance obligations has been recognised and supported by Government:

- In 2007 an Electoral and Referendum Act regulation enabled Equifax to be given a copy of the Commonwealth electoral roll to enable entities with AML obligations to verify identity.
- In 2011 legislation enabled the use of certain credit reporting information for the purposes of enabling entities with an AML requirement to verify identity.
- In 2013 Equifax was one of the original private sector entities to sign up as a *Gateway Service Provider* (GSP) to the DVS when it was enabled for access to non-Government entities.

As Gateway Service Provider, Equifax has promoted and assisted the DVS

Successful participation by businesses in the FVS can draw from the experience of the DVS.

At its start, the number of DVS transactions was lower than expected, and as a consequence AGD were in regular discussion with Equifax on feedback from our various customers. This led, in part to the decision to widen access beyond entities with Commonwealth obligations (e.g. AML-CTF Act 2006). As of 2015, DVS use was enabled for any entity where it was "reasonably necessary to verify the identity of the individual for the purposes of the Organisation's functions or activities".

Similarly, GSPs have managed the impact on businesses reliant on the DVS of changes made by the IMS, most notably significant changes to two key verification sources:

- A multi-year change process where verification of drivers licence required the additional input of a drivers licence card number, as well as the drivers licence number.
- The Commonwealth electoral roll was moved behind the DVS (previously it was managed by recognised entities) and with that the loss of fuzzy matching.

Annual Reporting to Parliament- provision 41 (b)

(b) statistics relating to all requests in the financial year from non-government entities for 1:1 matching services, including:
  (i) the total number of those requests; and
  (ii) the names of the non-government entities that made those requests; and
  (iii) the number of those requests the response to which was that the requested comparison resulted in a match for an individual; and
  (iv) the number of those requests the response to which was that the requested comparison did not result in a match for an individual;

Consistent availability of identity resources

Both the DVS and the FVS rely heavily on people holding a drivers licence (~75% of the population) or Australian citizens with passports (~58%).

However the databases with the more significant reach are the Commonwealth electoral roll (~17.6 million citizens) and credit reports (~18.5 million accounts). Both of these can only be used to meet AML/CTF, a legacy restriction originally applying to the DVS that was eased in 2015.