Submission on the Preliminary Report on the Financial System Inquiry

Technology - Cyber security and digital identity

The following paper a submission on the Preliminary Report on the Financial System Inquiry, with respect to Digital Identities.

Summary

There is an increasing reliance in the Financial Services Industry of Digital Identities, both for initial AML/CTF requirements and ongoing interactions between the providers and the end users. This emerging trend has evolved due to isolated changes in legislation, technology and appetite, without necessarily having a cohesive framework within which all parties have a clear and shared view of the expectations. This lack of a framework could lead to less than optimal protection of end users and their Digital Identities in an area of increasing fraud and cybercrime.

This submission seeks to propose a Framework, Roles & Responsibilities and Structure for the verifying, creating and holding Digital Identities or Digital Identity Information in the Financial Services Industry.

Roles & Responsibilities

The Government Role in Digital Identities should encompass the following

- Setting the standards to be adhered to in verifying, creating and holding Digital Identities or Digital Identity Information
- Regulating the verifying, creating and holding Digital Identities or Digital Identity Information
- Authorising Users of Digital Identities and ensuring that the Users follow the aforementioned standards
- Authorising the Providers of Digital Identities information and ensuring that the Providers follow the aforementioned standards
- Authorising the Gateways to the Providers of Digital Identities and ensuring that the Gateways follow the aforementioned standards
- Holding and enabling access to Government Digital Identity Information

The Private sector would include any non-government organisation that verifies, creates, holds or facilitates access to Digital Identities or Digital Identity Information. This would include Financial Service Providers, Utilities (Telephone, Electricity, Water, Gas, etc.), Gateway Providers, Other Digital Identity Information holders (Credit Bureau, etc.).

The role of each Private sector organisation will depend on whether they verify, create, hold or facilitates access to Digital Identities or Digital Identity Information or a combination of all of these.

The Financial Service Providers have the requirement or ability to verify, create, hold or facilitates access to Digital Identities or Digital Identity Information. The Financial Service Providers role would be the following.

- Has an obligation to verify Digital Identities Information in terms of the standards that have been set
- If sufficient Digital Identities Information is verified, then create a Digital Identity in accordance with the standards that have been set
- To hold the Digital Identity Information in accordance with the standards that have been set
- If it chooses to, the Financial Service Providers can provide Digital Identity Information to other Public or Private sector organisations that are accredited Digital Identity Providers, either directly or via Gateway, in accordance with the standards that have been set.
- Provide input into the formulation and ongoing review of the national standards as a part of a joint Public and Private sector body concerned with Digital Identities within Australia (Digital Identities Industry Body)

Future State and Road Maps

Digital Identities is an emerging industry that continues to have new and improving technological solutions to an evolving problem of maintaining security of the individual's Digital Identities. The use of the Digital Identities Industry Body to provide guidance on emerging technologies and appropriate standards, will ensure that appropriate controls exist to help safeguard Digital Identities within Australia.

Biometrics (fingerprint, facial recognition, voice prints, etc.) is one such emerging area, that doesn't yet have comprehensive usage in Digital Identities. Until these technologies mature and expand in usage, a set of minimum standards should be set by the Government, via the Digital Identities Industry Body. These standards would be continuously reviewed and refined as Biometrics continues to emerge in the Digital Identity landscape.

The Digital Identities Industry Body should be tasked with determining a roadmap and Future State for the use and standards of Digital Identities within Australia, in light of Technological changes, criminal activities and global trends.

Digital Identity Information

The AML/CTF Act requires that Electronic Verification is from reliable and independent electronic data sources.

In line with the Role & Responsibilities, Digital Identity Information providers should be accredited to provide Digital Identity Information is in terms of the standards that have been set.

The standards in terms of Digital Identity Information should be set so that the Digital Identity Information is linked to real world activities. For example, Digital Identity Information from Utilities companies.is linked to the ongoing provision of Electricity, Gas, Water, Telephone, etc. Banks provide ongoing financial services.

Digital Identities need to be linked back to real world activities that are linked back to real people. A real world "footprint" will generate a growing digital footprint that can be then utilised to verify the Digital Identity of the individual.

Government Sector - Document Verification Service (DVS)

The introduction of the Document Verification Service (DVS) has allowed formal access to data sources that were previously available via other methods.

A key issue with the provision of data within the DVS is that the data provided doesn't seek to meet the data requirements for AML "Safe Harbour" standards.

The data in the DVS seeks to make available, in electronic format, that information that is physically available on the document that is issued by the Government Department. In the example of Medicare, this is the Document ID, the name of the individual, the position on the card and the card expiry date.

The data required for AML "Safe Harbour" is Name and Address or Name and Date of Birth. So as the Medicare data in DVS only contains Name and doesn't contain either the Address or Date of Birth details, the Medicare data in DVS doesn't meet AML "Safe Harbour" standards and can't be used for Electronic Verification of Digital Identity.

There needs to be a change in the focus of DVS, from providing an electronic copy of the data held on the physical Government issued documents, to providing access to data that meets the AML "Safe Harbour" Standards. In the Medicare example, the DVS needs to hold Name and Date of Birth, at a minimum.

To facilitate the Government's role in the verification of Digital Identities, the DVS needs to be expanded to provide AML "Safe Harbour" standard data (Name and either/or Date of Birth and Address) from additional Government sources, not just limited to those that currently provide physical identification documentation. Additional sources such as Births, Deaths and Marriages (Name and Date of Birth), Australian Taxation Office (Name and Date of Birth &/or Address), Department of Education (Name and Date of Birth &/or Address), Department of Human Services (Name & Date of Birth &/or Address), etc.

Private Sector

There needs to be greater access &/or provision of Digital Identity Information from the Private Sector. A set of standards around the quality, access & privacy of Digital Identity Information is required to facilitate key Private Sector Organisations to make available Digital Identity Information that is held by them.

Accreditation and access to conduct Electronic Verification of Digital Identities, may in turn, require the Private Sector Organisation to provide access to the Digital Identity Information that they hold.

Federated vs Syndicated System

It appears that we are well down the path towards a Federated system. The AML/CTF Act requirement of "independent and reliable" sources has meant that organisations seeking the verify Digital Identities have had the ability to source Digital Identity Information from a variety of sources, both Public and Private sector.

The limitations to date, in accessing the "safe harbour" standard information, from either Public or Private sector sources, has meant that the verifying organisation has needed to go to a wide variety of data sources to meet the "safe harbour" standard.

While greater access to additional Public sources (e.g. ATO, Dept. of Ed, etc.) and the increased provision of "safe harbour" standard Information (e.g. Medicare – DOB Information, etc.), would enable greater Electronic Verification via Public sector sources, there is additional benefit in increasing the availability and quality of Private sector sources.

Key Private Sector sources (Utilities, Banks, etc.) can provide a broader view of the Digital Identity Information. There is also a higher likelihood of key "safe harbour" information, predominately address details, being more up to date from these sources, as the individuals update their records to enable to provision of services.

Going forward, an assessment of the overall quality of the individual's digital footprint (Public and Private Sectors), will be beneficial in Electronic Verification of the Digital Identity.

This would point to a definite benefit in using a Federated system for Digital Identities.

The use of a Federated system for Digital Identities in Australia and a Syndicated system in New Zealand, would mean that it won't feasible to have mutual recognition of Digital Identities between the two Governments.