19 October 2023

John Shepherd PSM
First Assistant Secretary
Digital Identity Taskforce
Department of Finance
One Canberra Avenue
FORREST ACT 2603
Via online submission portal.

Dear Mr Shepherd,

RE: Digital ID Bill and Digital ID Rules 2023

The FSC welcomes the opportunity to consult on the exposure draft *Digital ID Bill 2023* and the draft *Digital ID Rules*.

FSC members are supportive of implementing a voluntary digital ID verification system in Australia so long as the system remains voluntary for use by individuals and acceptance by relying parties.

The FSC submits that in order to increase uptake of the system by FSC members and other relying parties, the Department should ensure that any identification accepted through the system satisfies all requirements under the law and/or regulatory schemes, including Australian Financial Complaints Authority (**AFCA**) expectations. Further, there should be clarity that any relying party that utilises a Digital ID for identification purposes would not be exposed to any further risk should that Digital ID prove to have been made fraudulently or otherwise erroneously and where the relying party has unknowingly relied on a Digital ID that reasonably appears to be valid.

Finally, the FSC seeks clarity in relation to the governance arrangements for any technical or security standards expected to be created to underpin the legislative framework of the Digital ID, and the Government's expected implementation timeline.

About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services. Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, investment platforms and financial advice licensees.

The financial services industry is responsible for investing more than $3 trillion on behalf of over 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is one of the largest pools of managed funds in the world.

Financial Services Council Ltd
Level 5, 16 Spring Street
Sydney NSW 2000
E. info@fsc.org.au
W. fsc.org.au
ABN 82 080 744 163

Summary of Recommendations

1. Any Digital ID system implemented in Australia should remain voluntary from both a consumer and relying party perspective.
2. The Department provide certainty to relying parties that the Digital ID will be acceptable, without any further validation, for use in contexts such as AML/CTF identification requirements and forthcoming Government scam and fraud mitigation measures.
3. The Department address concerns around the inconsistency of information verified by different DVSs and Digital ID suppliers and uplift the required verifications to ensure a robust and consistent system.
4. The Department provide clarity for relying parties that if a Digital ID is appropriately relied upon for identification that later turns out to be fraudulent or erroneous, there will be no further action on the relying party in relation to losses occurred from relying on the verified Digital ID.
5. The Department provide clarity as to the liability of all parties within the Digital ID system, including if relying parties can, in fact, pursue an accredited entity for any damages as a result of using the Digital ID.
6. The Department provide clarity for relying parties in relation to change of customer details and how these will be communicated through the Digital ID system to relying parties.
7. The Department outline expected governance arrangements for any standards setting bodies that may be charged with creating standards to underpin the rules of the Digital ID system, including the expectation that any changes to said standards be done following a proper and transparent consultation process.
8. The Department provide a clear timeline for the rollout of the National Digital ID system.

A Voluntary System

FSC members are supportive of a digital identity verification system that is robust and interoperable. However, the FSC submits that there should be no plans to make the system compulsory either from an individual user perspective, or from a relying party perspective.

As cybersecurity becomes an ongoing and increased focus across industry cohorts, options to reduce the amount of customer data retained by funds are welcomed. However, choice remains paramount and FSC members are only supportive of a system where they can have the option to determine which forms of identification or identity verification technology best meets their business and regulatory requirements.

Recommendation 1

Any Digital ID system implemented in Australia should remain voluntary from both a consumer and relying party perspective.

Certainty for Relying Parties

In order to increase uptake of the Digital ID among relying parties, the FSC submits that the Department should provide certainty that accepting a verified ID through the Digital ID system would completely satisfy any legislative, regulatory, or prudential identity verification requirements.

FSC members are subject to the Australian Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regime. This means they are required by law to confirm the identity of customers and their beneficial owners using their products and services by collecting at a minimum their full name and date of birth, or their residential address.

In accordance with the risk-based approach applied under the AML/CTF regime, businesses are required to collect and verify additional customer identification information where the assessed financial crime risk is considered high. Businesses also have an obligation to undertake ongoing and enhanced customer identification practices, and this can include completing a 'refresh' of the customer identification processes at appropriate intervals, having regard to the assessed financial crime risks.

Further, the wealth sector, including superannuation funds, have a certain level of exposure to fraud and scam risk meaning that as trustees, they must satisfy themselves that a person requesting to transact on a superannuation account, is the person whom they say they are. In addition to the AML/CTF requirements covering financial crime risks, there are also prudential and regulatory expectations on superannuation funds to ensure that fraud risk is appropriately managed. For example, persons who have experienced fraud or scam activity within their superannuation account can complain to AFCA to seek redress from the fund. AFCA expects a reasonable level of identity confirmation to have occurred in addition to other risk mitigation activities in order to clear the superannuation fund of any wrongdoing.

For this reason, it is important that funds receive clarity in relation to the expectation that any identity verification received through the Digital ID regime meets the appropriate legislative, regulatory, and prudential standards, without any further validation required. The requirement for clarity around whether further validation is required is key as in June 2019, AUSTRAC announced that digital driver licences issued by an Australian state or territory would be considered "independent and reliable documents", however, entities were still required to establish whether the document was valid.[1] If reliance on the Digital ID continues to be subject to the requirement that entities assess the validity of the ID, the value for entities to rely on the system may be limited.

[1] Australian Government: AUSTRAC. (2019). *Digital driver licenses now acceptable as ID.* Link

In addition to the current regime, there is also significant government activity occurring in relation to scam activity, including the creation of industry specific codes and legislated principles of scam mitigation activities. The FSC submits that the digital ID system should be consistent and align with any forthcoming requirements in relation to those matters as well.

Recommendation 2

The Department provide certainty to relying parties that the Digital ID will be acceptable, without any further validation, for use in contexts such as AML/CTF identification requirements and forthcoming Government scam and fraud mitigation measures.

In addition to the need for clarity mentioned above, it should be noted that there has been some hesitation amongst industry to take up digital verification services due to the way the validation is conducted both by the provider and by the document verification service (**DVS**). For example, some state-based DVSs, do not allow for verification against driver's license numbers. Verifying driver's license numbers are pivotal in detecting fraudulent documents which might have been based on stolen and duplicated details.

Further, some verification services do not verify against all fields in a document. For example, they may verify the license number but not the address. In order to provide the most robust verification that can be relied on to satisfy both legislative and best practice requirements, consistency between how verification is achieved and also what information a DVS validates against would be appropriate.

Recommendation 3

The Department address concerns around the inconsistency of information verified by different DVSs and Digital ID suppliers and uplift the required verifications to ensure a robust and consistent system.

Further, clarity is sought in relation to any discovery that a Digital ID has been set up either with incorrect details or fraudulently and in the case of the latter, when this is then used to commit further fraud. In order to encourage the uptake of Digital ID, the FSC submits that the Department should provide certainty that there will be no further action taken against a relying party who appropriately utilised a Digital ID to confirm a person's identity that later turned out to be either fraudulent or otherwise incorrect.

Recommendation 4

The Department provide clarity for relying parties that if a Digital ID is appropriately relied upon for identification that later turns out to be fraudulent or erroneous, there will be no further action on the relying party in relation to losses occurred from relying on the verified Digital ID.

Liability of Parties

In addition to the certainty requested above, FSC members require clarity as to the liability framework of the various participants in the system.

A relying party may suffer direct damages as the result of utilising a digital ID. For example, and as noted above, fraud is a significant risk in the wealth context. Organisations that rely on an ID verification through the Digital ID framework may suffer damages if that ID turns out to be fraudulent. These damages may be monetary and/or reputational and can take the form of AFCA complaints ruled against them, regulatory action, civil litigation, or the requirement for the organisation itself to pay damages.

The published draft considers the question of liability, however, there appears to be some inconsistencies between clauses. For example, Part 3, Division 1, Section 79(3) notes that an accredited entity is not liable to ANY action (civil or criminal) in relation to that accredited service. However, Division 2, Section 80 seems to imply that reliant party liability can only be limited by contract with the provider.

In order to support a trusted environment, a clear understanding of the liability framework is required.

Recommendation 5

The Department provide clarity as to the liability of all parties within the Digital ID system, including if relying parties can, in fact, pursue an accredited entity for any damages as a result of using the Digital ID.

Changes to Customer Details

FSC members require further clarity in relation to the process where a customer's credentials change. For example, when a change of name occurs or their passport/drivers licence number changes. If an organisation is relying on a digital verification for identity purposes, they may not be aware that these details have expired. Clarity is sought regarding how the Digital ID handles updates to customer details and the mechanism for the passing on of those changes of details to relying parties. If updates are passed to relying parties in a way that can be taken as verified and trusted, this would help ensure relying parties' records continue to be accurate, up to date, complete, relevant and not misleading as required under Australian Privacy Principle 13. Additionally, it could assist with relying parties who provide a designated service under AML regulations to comply with ongoing customer due diligence requirements.

Recommendation 6

The Department provide clarity for relying parties in relation to change of customer details and how these will be communicated through the Digital ID system to relying parties.

Financial Services Council Ltd
Level 5, 16 Spring Street
Sydney NSW 2000
E. info@fsc.org.au
W. fsc.org.au
ABN 82 080 744 163

Governance of Standards

The FSC seeks clarity in relation to the governance arrangements for any standards that would be implemented to underpin the official rules of the Digital ID system. The FSC believes that a body with suitable technical knowledge should be charged with creating any technical and security standards prescribed in the rules for accessing the Digital ID service. However, there should be an explicit obligation that that body consult with all stakeholders on any proposed new or revisions to the Standards in a transparent and fair manner.

Recommendation 7

The Department outline expected governance arrangements for any standards setting bodies that may be charged with creating standards to underpin the rules of the Digital ID system, including the expectation that any changes to said standards be done following a proper and transparent consultation process.

Timeline of Rollout

The FSC also seeks further clarity in relation to the implementation timeframes for the rollout of the Digital ID service so that relying parties can plan their own implementation and uptake.

Recommendation 8

The Department provide a clear timeline for the rollout of the National Digital ID system.

If you would like to discuss anything contained in this submission, please do not hesitate to get in contact.

Yours sincerely,

Kirsten Samuels
Policy Manager, Superannuation and Innovation