14 August 2026

Department of Finance
Attn: Digital ID Act Review
One Canberra Avenue
FORREST ACT 2603

Response to Statutory Review of the *Digital ID Act 2024*

To whom it may concern,

The FSC welcomes the opportunity to provide comment on the Statutory Review of the *Digital ID Act 2024* (the Act).

Overall, the FSC supports the objectives of Act and recognises the role the framework can play in providing secure, privacy-enhancing and trusted identity verification.

This Review is being conducted at a time where the Act has been operating for less than two years and implementation remains underway to support private sector participation in the Australian Government Digital ID System (AGDIS) from December 2026. As the Issues Paper acknowledges, further time will therefore be required to assess the success of private sector participation and the extent to which the Act is achieving its objectives.

Notwithstanding this, the FSC considers that broader industry adoption of Digital ID and the realisation of the intended economic benefits will ultimately depend on whether participation in the Digital ID framework presents a sufficiently compelling value proposition for businesses and customers. This can be supported by the development of a broader range of practical use cases, greater interoperability across jurisdictions, demonstrating the scam and fraud prevention outcomes associated with digital ID adoption and greater alignment with existing AUSTRAC customer identification requirements.

Finally, the FSC also supports the continuation of key existing features of the framework, including support for attribute-based verification and the voluntary nature of Digital ID use, which help promote data minimisation, privacy and accessibility.

These matters are explored in further detail below.

About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 130 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, and financial advice licensees. Our Supporting Members represent the professional services firms such as ICT, consulting, accounting, legal, recruitment, actuarial and research houses.

The financial services industry is responsible for investing more than $4 trillion on behalf of over 16.9 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.

Summary of Recommendations

1. The Department should prioritise expanding practical use cases in the private sector to increase the value proposition of Digital ID adoption for all stakeholders.
2. The Department should consider opportunities to streamline requirements and open risk-based pathways to becoming an accredited Digital ID service provider.
3. The Department should work with state and territory governments to develop greater

interoperability and mutual recognition between comparable digital identity frameworks, including mechanisms for recognising equivalent accreditation, assurance and compliance requirements.
4. The Department should develop and report measures of the fraud and scam prevention outcomes associated with the use of Digital ID, including its impact on reducing identity theft, impersonation fraud and account compromise.
5. The Department should work with AUSTRAC to better align the Digital ID framework with existing customer identification and verification requirements, including by providing clear guidance on the circumstances in which regulated entities can rely on Digital ID to satisfy AML/CTF identification requirements without duplicative verification.
6. The Department should ensure the Digital ID framework continues to support attribute-based verification and remains sufficiently flexible to accommodate emerging credential models.
7. The Department should retain the principle of voluntary Digital ID use and ensure appropriate alternative identity verification channels remain available for customers who cannot or choose not to use Digital ID.
8. The Department should provide additional guidance on the practical operation of existing accountability and redress arrangements, particularly where incidents involve multiple participants in the Digital ID ecosystem.

Broader use cases are needed to strengthen the value proposition for Digital ID usage

The FSC supports the objective of increasing the use of Digital ID across the Australian economy. However, broader private sector adoption will ultimately depend on the Digital ID framework offering a sufficiently compelling value proposition for both businesses and their customers.

At present, many businesses have established secure and effective identity verification and customer onboarding processes. Transitioning to the use of Digital ID would require businesses to incur implementation and ongoing compliance costs in circumstances where the incremental commercial or operational benefit is unclear, especially where there is limited customer demand for alternative identity solutions. Further, as the framework expands to support private sector participation in AGDIS from December 2026, it will be important that participation requirements for relying parties remain proportionate to risk and do not impose unnecessary costs or barriers that undermine the business case for adoption.

Greater adoption of Digital ID in the private sector would be encouraged by high-volume use cases across banking, telecommunications, utilities, insurance and other sectors, creating stronger network effects for both consumers and businesses. Without this greater adoption, there is a risk that the benefits envisioned by the Act will not be realised to their full potential.

Recommendation #1: The Department should prioritise expanding practical use cases in the private sector to increase the value proposition of Digital ID adoption for all stakeholders.

The process of accreditation for Digital ID service providers is complex and creates participation barriers

The FSC recognises that accreditation delivers important security, privacy and trust outcomes. However, the current framework can be resource-intensive and complex for entities seeking accreditation. Indeed, the Issues Paper acknowledges that since commencement there have been no new applications for accreditation.[1]

The compliance, assurance, governance and technical requirements associated with accreditation can require significant investment before a clear commercial return is established. As a result, for

[1] Department of Finance, Statutory Review of the Digital ID Act 2024 – Issues Paper, 14 July 2026, p.19.

potential participants, the cost and effort involved may outweigh the immediate benefits of joining the ecosystem.

A more proportionate and streamlined accreditation model with more risk-based pathways to accreditation would help increase participation while maintaining appropriate privacy, security and consumer protection safeguards.

Recommendation #2: The Department should consider opportunities to streamline requirements and open risk-based pathways to becoming an accredited Digital ID service provider.

Greater interoperability and mutual recognition would reduce fragmentation

The FSC considers that the long-term success of Digital ID will depend not only on the operation of the Commonwealth framework, but on the extent to which Australia's broader digital identity ecosystem operates cohesively.

Businesses operating nationally should, as far as practicable, not be required to navigate duplicative accreditation, assurance or compliance requirements to participate in comparable digital identity solutions across different jurisdictions.

The FSC therefore supports the Review examining opportunities for greater interoperability and mutual recognition between the Commonwealth framework and comparable state and territory arrangements. Where schemes provide substantively equivalent assurance, privacy and security outcomes, there should be scope to recognise existing assessments or compliance processes rather than requiring organisations to demonstrate compliance afresh.

Greater alignment would reduce unnecessary compliance costs and improve customer experiences. Over time, a nationally interoperable ecosystem should also strengthen the value proposition for investment by allowing businesses to integrate Digital ID solutions that can be used across a wider range of transactions and jurisdictions.

Recommendation #3: The Department should work with state and territory governments to develop greater interoperability and mutual recognition between comparable digital identity frameworks, including mechanisms for recognising equivalent accreditation, assurance and compliance requirements.

Fraud and scam prevention outcomes should form part of the framework's measures of success

The FSC considers that the effectiveness of the Digital ID framework should be assessed, in part, by the extent to which its adoption contributes to improved fraud and scam prevention outcomes.

Digital ID has the potential to reduce risks associated with identity theft, impersonation fraud and account compromise by providing businesses with a trusted means of verifying an individual's identity while reducing reliance on the repeated collection and sharing of identity documents.

Demonstrating these fraud and scam prevention outcomes would assist in assessing whether the framework is achieving its objectives and could also strengthen the business case for adoption by allowing businesses to better assess the potential fraud and risk-reduction benefits of integrating Digital ID.

Recommendation #4: The Department should develop and report measures of the fraud and scam prevention outcomes associated with the use of Digital ID, including its impact on reducing identity theft, impersonation fraud and account compromise.

Greater alignment with existing customer identification requirements would support adoption

Financial services businesses are already subject to extensive customer identification and due diligence requirements, including under the AML/CTF framework. Many of these businesses have made significant investments in systems and processes to support compliance with these obligations.

The FSC considers that the value proposition of digital ID adoption depends in part on the extent to which verification undertaken through the Digital ID framework can be relied upon to satisfy existing customer identification and verification requirements.

Greater alignment between the Digital ID framework and existing AML/CTF and customer identification requirements could reduce duplication, streamline customer onboarding and support adoption by regulated entities. This would be particularly beneficial where organisations are already subject to extensive customer due diligence obligations. Greater regulatory clarity as to when and how Digital ID can be relied upon for these purposes would also provide regulated entities with greater certainty when considering investment in Digital ID integration.

Recommendation #5: The Department should work with AUSTRAC to better align the Digital ID framework with existing customer identification and verification requirements, including by providing clear guidance on the circumstances in which regulated entities can rely on Digital ID to satisfy AML/CTF identification requirements without duplicative verification.

Attribute-based verification and emerging credential models should continue to be supported

The FSC supports continued development of attribute-based verification and emerging credential models that allow organisations to verify only the information required for a transaction. This can reduce unnecessary collection and retention of personal information while supporting effective identity verification, consistent with the Act's privacy and data minimisation objectives.

Recommendation #6: The Department should ensure the Digital ID framework continues to support attribute-based verification and remains sufficiently flexible to accommodate emerging credential models.

Alternative identity verification channels should be retained

The FSC also supports the continued availability of alternative identity verification channels as Digital ID adoption increases. Customers who experience digital exclusion, accessibility challenges or other barriers should not be disadvantaged by an increased adoption of Digital ID. The principle that use of Digital ID remains voluntary is therefore an important safeguard.

This is consistent with s74(1) of the *Digital ID Act 2024*, which requires participating AGDIS relying parties to provide an alternative and reasonably accessible means of accessing a service without Digital ID.

Recommendation #7: The Department should retain the principle of voluntary Digital ID use and ensure appropriate alternative identity verification channels remain available for customers who cannot or choose not to use Digital ID.

Additional Guidance Regarding the Practical Operation of Existing Accountability and Redress Arrangements would be Helpful

The existing Digital ID framework contains accountability and redress mechanisms, including incident reporting and redress requirements. However, as participation in the Digital ID ecosystem expands, clear guidance and transparency regarding the practical application of existing accountability, remediation and redress arrangements would be helpful for both participants and customers.

Customers are unlikely to distinguish between Digital ID providers, exchanges, or relying parties. Where fraud, impersonation, identity misuse or service failures involve multiple participants, clear accountability for investigation, remediation, customer communications and customer outcomes will be important to maintaining consumer confidence and trust.

Greater clarity on how existing arrangements operate in practice, particularly where incidents span multiple participants, would support effective implementation and help maintain consumer confidence and trust in the Digital ID ecosystem.

Recommendation #8: The Department should provide additional guidance on the practical operation of existing accountability and redress arrangements, particularly where incidents involve multiple participants in the Digital ID ecosystem.

If you would like to discuss anything contained in this submission, please contact Julia Hukka, at +61 432 482 155 or jhukka@fsc.org.au.

Yours sincerely,

Julia Hukka
Policy Manager – Investment Platforms and Superannuation