

## **SUBMISSION**

### **2025 DIGITAL ID RULES AND ACCREDITATION RULES CONSULTATION OCTOBER 2025**

The Australian Retailers Association (ARA) and National Retail Association (NRA) welcome the opportunity to provide feedback on the 2025 Digital ID Rules and Accreditation Rules Consultation

The ARA and the NRA (the Associations), which propose to amalgamate to form the Australian Retail Council (ARC), represent a \$430 billion sector that employs 1.4 million Australians, making retail the nation's largest private sector employer and a cornerstone of the Australian economy.

Our combined membership spans the full breadth of Australian retail: from family-owned small and independent businesses, which comprise 95% of our membership, to the largest national and international retailers that support thousands of jobs and sustain communities across both metropolitan and regional Australia. Our industry operates more than 155,000 retail outlets nationwide, with the majority of those also represented by an online or e-commerce presence.

A strong retail sector delivers widespread benefits to all Australians, with a significant portion of every dollar spent in retail flowing back into employees, suppliers, superannuation funds, and local communities. We are united in advocating for the policy settings, reforms and collaboration that will drive growth, resilience, and long-term prosperity for Australian retail and the millions who rely on it.

## **EXECUTIVE SUMMARY**

The Associations welcome the opportunity to provide feedback on the 2025 Digital ID Rules and Accreditation Rules. As Australia's largest private sector employer, retailers rely on secure, practical, and efficient identity systems to support business operations and consumer trust.

We focus on two key areas:

1. **Protective Security Policy Framework (PSPF):** Support for allowing private sector participants to use ISO/IEC 27001 or other recognised international standards, avoiding unnecessary duplication and aligning with global best practice.
2. **Express Consent Expiry:** Support for extending business-purpose consent from 12 months to seven years, reducing administrative burden while ensuring individuals can withdraw consent at any time.

These reforms will help deliver a secure, outcomes-based Digital ID system that is workable for business and trusted by consumers.

## **BODY OF SUBMISSION**

The Associations have consistently supported the development of a secure and trusted national Digital ID system. A well-designed framework has the potential to reduce duplication in identity verification, minimise the need for businesses to store sensitive customer information, and improve confidence in digital transactions. Importantly, any regulatory settings must remain risk-proportionate, outcomes-based, and practical for both large and small retailers to implement.

While the consultation covers a broad range of technical and operational issues, our submission focuses on PSPF and Express consent expiry which are of direct relevance to retailers.

These are critical to ensuring the Digital ID system is workable for the private sector, aligns with international best practice, and reduces unnecessary administrative burden while maintaining strong protections for individuals.

## 1. Protective Security Policy Framework (PSPF)

The Associations support the decision to allow private sector participants, including retailers, to meet accreditation requirements through ISO/IEC 27001 or another approved international information security standard, rather than mandating the Commonwealth's Protective Security Policy Framework (PSPF).

### Rationale

- **Proportionate and outcomes-based:** ISO/IEC 27001 is a globally recognised, outcomes-based framework already in use across many retail organisations. Requiring PSPF compliance would impose government-specific obligations with little additional security benefit for the private sector.
- **Harmonisation and efficiency:** Aligning with international standards avoids duplication and supports consistent application of security practices across jurisdictions and global supply chains. This is particularly important for retailers that operate in multiple countries or rely on international vendors.
- **Scalability:** ISO/IEC 27001 provides a flexible framework that can be adapted to businesses of different sizes and risk profiles, including small and medium retailers that may lack the compliance capacity of larger enterprises.
- **Trust and confidence:** Security is central to building consumer and business trust in the Digital ID system. ISO/IEC 27001 offers a recognised benchmark without introducing unnecessary complexity.

### Considerations for Implementation

- **Transition periods:** Adequate lead time should be provided for any updates to international standards, ensuring businesses can adapt without significant disruption.
- **Support for SMEs:** Given the diversity of the retail sector, tailored guidance and practical templates should be made available to smaller retailers to reduce compliance costs and promote consistent adoption.

## 2. Express Consent Expiry

The Associations support the proposed extension of express consent for business purposes from the current 12 months to seven years, while retaining a 12-month consent period for personal use.

### Rationale

- **Reduced administrative burden:** Annual renewals of consent create unnecessary red tape, particularly for long-term functions such as payroll, HR systems, finance, and ABN authorisations. A seven-year period better reflects the operational realities of these processes and reduces compliance overhead for businesses.
- **Proportionality:** The proposal balances efficiency for business transactions with safeguards for individuals, as personal use consents remain limited to 12 months.
- **Alignment with business cycles:** Seven years aligns with standard record-keeping obligations under the Corporations Act and the ATO, and more closely reflects employment cycles and financial reporting periods.

### Considerations for Implementation

- **Right to withdraw:** It is essential that individuals retain the ability to withdraw consent at any time. Clear and simple withdrawal mechanisms will ensure this measure strengthens efficiency without reducing individual control.
- **Scope and clarity:** The concept of "business purposes" should be clarified through additional examples. Beyond payroll and HR, use cases may include supplier verification, franchise management, and other functions where identity checks are long-term and ongoing.
- **Retail applicability:** Retailers often deal with large, distributed workforces and franchise networks. Extended consent periods will significantly reduce administrative duplication in these contexts, provided guidance is clear and consistently applied.

## CONCLUSION

The Associations welcome the opportunity to comment on the 2025 Digital ID Rules and Accreditation Rules. We support the direction of the reforms, particularly the adoption of internationally recognised information security standards and the proposed extension of express consent for business purposes.

These changes will help ensure the Digital ID framework is both secure and workable for the private sector, reducing unnecessary compliance burden while maintaining strong protections for individuals. We encourage government to provide clear guidance, proportionate implementation, and transitional support to ensure smooth adoption across the retail industry.

The retail sector is committed to working constructively with government to build a trusted and effective Digital ID system that enhances consumer confidence, streamlines business processes, and supports Australia's broader digital economy.

---

The Associations appreciate the opportunity to contribute to this important discussion.

We encourage the Federal Government to continue collaborating with business groups and service providers to ensure the Digital ID framework is practical, proportionate, and delivers strong security outcomes without creating unnecessary compliance burdens.

Any queries in relation to this submission can be directed to our policy team at [policy@retail.org.au](mailto:policy@retail.org.au).