SUBMISSION

NATIONAL IDENTITY PROOFING GUIDELINES 2025

May 2025

The Australian Retailers Association (ARA) and National Retail Association (NRA) welcome the opportunity to provide feedback on the National Identity Proofing Guidelines 2025.

The ARA and the NRA, which propose to amalgamate into the Australian Retail Council (ARC), represent a $430 billion sector that employs 1.4 million Australians—one in ten workers—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 ARA and NRA welcome the modernisation of the National Identity Proofing Guidelines. As Australia transitions toward a more digitally enabled identity ecosystem, alongside the introduction of the Digital ID Act 2024, updated Privacy Act reforms, and increased use of biometric technologies, our sector sees a need for practical, consistent, and scalable identity proofing guidance that works in real-world commercial settings.

Retailers are not unfamiliar with identity verification. Whether it's fulfilling age-restricted online orders, deterring in-store theft, onboarding credit customers, or operating across digital platforms, retailers interact with identity systems daily. However, many lack the compliance capacity, technology infrastructure, or legal resources of government and regulated financial institutions. This makes operationalising a complex assurance framework such as Levels of Assurance (LoA) tiers and document categories challenging without clear, use-case-driven support.

The ARA and NRA support the risk-based approach of the guidelines and their alignment with privacy and Digital ID reforms. However, we urge the Government to improve clarity and usability by:

- Providing retail-specific examples of how Levels of Assurance should be applied;
- Clarifying the role of biometrics in relation to the Privacy Act 1988, especially for small-to-medium businesses;
- Explaining how Digital ID services map to the guidelines' assurance levels; and
- Offering practical tools such as risk assessment templates, trusted referee forms, and scalable options for lower-risk environments.

The ARA and NRA have responded to the relevant questions from the consultation below, focusing on the area's most applicable to the retail sector. Our responses reflect both current industry practice and anticipated future challenges as identity verification becomes more integrated across digital, physical, and biometric platforms.

CONSULTATION QUESTIONS

2. Are there any issues you would like to raise around the guidelines?

Clarity and Complexity

- The guidelines are generally clear and well-structured but may be overly complex for organisations without dedicated compliance or legal teams. For example, the detailed distinction between Categories 1–4 credentials and the six Levels of Assurance may be difficult for some private sector organisations to operationalise without clearer examples tailored to non-government contexts.
- It may be helpful to include use-case guidance specifically for commercial entities, such as retailers offering credit services, loyalty programs, or home delivery of restricted goods.

Alignment with Other Obligations

- There is strong alignment with key privacy and verification obligations under the Privacy Act 1988, Identity Verification Services Act 2023, and the Digital ID Act 2024.
- However, there is a need to clarify how compliance with these voluntary guidelines would interact with mandatory obligations under AML/CTF for retailers offering high-value goods (e.g. jewellers, luxury retailers).
- Further clarity on how biometric data collection under these guidelines aligns with privacy requirements (including APPs and the data minimisation principle) would be welcomed.

Integration with the Digital ID framework

- The guidelines are intended to support consistency across both physical and digital identity ecosystems. However, they do not clearly explain how identity verification conducted through accredited Digital ID providers (e.g. under the Digital ID Act 2024 or the Trusted Digital Identity Framework) maps to the LoAs set out in this document.
- Greater clarity on this alignment would support retailers seeking to rely on Digital ID services, particularly in digital onboarding, credit applications, and age-restricted product delivery. It would also help avoid duplication for businesses already engaging with trusted third-party identity providers.

Suggestions for Inclusion

- Practical examples and case studies specific to retail or small-to-medium enterprises would enhance usability.
- Suggested templates for risk assessments, trusted referee statements, or identity verification policies would help retailers implement the guidelines more easily.
- Further guidance on how retailers can rely on third-party providers such as payment platforms, delivery services, and accredited Digital ID providers would support scalable and secure implementation of identity proofing practices.

3. Do the categories of credentials, Levels of Assurance and the associated minimum identity proofing requirements provide sufficient clarity to choose the appropriate processes for your organisation? 4. Are there any other issues we should consider?

The ARA & NRA supports the tiered approach to identity credentials and LoA as a sound framework for managing identity-related risk. However, we believe further refinement is needed to ensure the guidelines are practical and usable across the retail sector.

1. Usability in commercial settings

The categories of credentials and associated LoAs are comprehensive but require clearer guidance on how they apply to typical retail environments. We strongly recommend the inclusion of worked examples for

- High-value transactions (e.g. jewellery or electronics sales),
- Home delivery or age-restricted product fulfilment,
- Customer onboarding for loyalty or credit programs.

2. Proportionality and risk scaling

There must be clearer direction on how to apply the LoA framework in proportion to risk. Retailers should not be required to adopt unnecessarily high assurance levels for low-risk interactions (e.g. loyalty scheme registration or order pickup), which may add friction without improving security outcomes.

3. Implementation constraints

While larger retailers may be able to align their systems with LoA requirements, many retailers especially SMEs face cost and technology barriers. Additional support, including template policies and simplified assessment tools, would assist in operationalising the guidelines across the sector.

Q5. Do the guidelines provide sufficient information on how biometrics should be linked to a person's identity? If no, how could this be improved?

Biometric identity proofing is not currently in widespread use across the retail sector. However, it is an area of emerging relevance, particularly in high-value, high-risk, or digital service settings (e.g. facial recognition for loss prevention, age estimation at self-checkouts, or identity verification by third-party credit providers).

Given this context, the ARA & NRA considers that while the guidelines appropriately acknowledge the role of biometrics and the importance of privacy, they do not yet provide sufficient practical guidance on how biometrics should be securely and lawfully linked to a person's identity in real-world retail environments. In particular, the guidelines should be improved in the following areas:

- While the guidelines acknowledge the need to comply with the Privacy Act 1988, further clarity and practical guidance are required on how biometric binding can be implemented in a way that meets key APPs; particularly APP 3 (data minimisation), APP 5 (notification), and APP 11 (security), in real-world commercial settings.

- Practical implementation advice: The guidelines should offer clearer technical and operational instructions on how to perform biometric binding particularly where a retailer engages a third-party provider. Examples of accepted methods at each Level of Assurance would support lawful and consistent adoption.

- Scalable and proportionate models: Many retailers particularly small to medium businesses do not have the infrastructure to implement biometric verification directly. The guidelines should provide lower-tech or risk-scaled alternatives that still achieve secure identity proofing outcomes without requiring full biometric systems.

The ARA & NRA supports a future-facing identity framework that enables innovation but requires stronger and clearer guidance to ensure biometric identity proofing can be adopted lawfully and proportionately by the retail sector.

Q9. Does the risk management framework provide sufficient clarity to develop identity proofing processes, while maintaining flexibility for your circumstances?

The ARA & NRA supports the inclusion of a risk-based framework and agrees that identity proofing should be proportionate to the risks associated with different types of transactions. The framework outlined in the guidelines is broadly useful, particularly in distinguishing between varying LoAs.

However, we believe the framework would benefit from greater practical clarity to support adoption across the retail sector. In particular:

1. More guidance on risk calibration

Retailers require clear examples of how to determine whether a transaction is low, medium, or high risk in practice. For example:

- What LoA is appropriate for a loyalty program?
- What risk controls are expected for age-restricted products or high-value electronics?
- How should click-and-collect identity checks differ from in-store credit applications?

Providing industry-specific scenarios would help retailers apply the framework consistently and confidently.

2. Support for small and medium retailers

Smaller retailers often lack in-house risk professionals or legal teams. A simplified version of the framework, accompanied by ready-to-use tools (such as checklists or risk templates), would make the framework more accessible and support broader compliance.

3. Integration with existing obligations

Many retailers are already subject to other risk-based requirements such as AML/CTF for high-value goods, or risk assessments under workplace safety and consumer protection laws. The guidelines should clarify how identity risk assessments can align with or complement these existing obligations to avoid duplication.

In summary, the ARA & NRA supports the flexibility built into the risk framework but recommends additional guidance, practical tools, and sector-specific examples to ensure the framework can be effectively applied in the retail environment.

The ARA and NRA appreciate the opportunity to contribute to this important discussion.

We encourage the Government to continue collaborating with business groups and service providers to ensure the guidelines remain practical, risk-proportionate, and adaptable to the diverse operating environments across the Australian economy, including retail.

Any queries in relation to this submission can be directed to our policy team at policy@retail.org.au.