AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

# Consultation on Verifiable Credentials Policy

July 2026

The Australian Retail Council (ARC) welcomes the opportunity to provide feedback on the Australian Government's consultation on proposed policy settings for the adoption and use of verifiable credentials.

ARC represents the Australian retail sector. Valued at $444 billion, retail supports more than 1.5 million jobs, including employing more young Australians than any other industry. Retail is embedded throughout the economy and plays a critical role in the supply chain of Australian businesses. ARC advocates for policies and reforms that drive growth, resilience and long-term prosperity for Australian retail and the millions who rely on it.

This submission focuses on the practical implications of verifiable credentials for retailers, particularly where retailers may be asked to verify credentials across customer, workforce, supply chain and regulated transaction settings.

## General comments

ARC supports clear, nationally consistent and practical regulatory frameworks that provide certainty for businesses and consumers. In relation to verifiable credentials, ARC supports the objective of developing a trusted and interoperable framework that can reduce fraud, improve privacy and streamline verification processes, provided it is practical for businesses to implement.

ARC notes that the case for verifiable credentials will vary by use case. While there are potential benefits in some retail settings, including age verification, identity checks, workforce onboarding, concessions, parcel collection, short-term vehicle hire and regulated transactions, adoption should not be treated as inevitable or uniform across the economy. Government should prioritise use cases where there is demonstrated demand, clear public benefit, strong privacy or fraud-prevention benefits, and a practical path to implementation for businesses.

Feedback received from members indicates that verifiable credentials may provide practical benefits in retail settings where businesses are required to verify credentials presented by customers, workers, contractors, delivery partners, suppliers or other businesses. These interactions may occur across point-of-sale systems, online channels, workforce systems, parcel collection processes, regulated product sales, concession checks and supply chain assurance.

The framework will only succeed if it can be incorporated into business-as-usual retail operations. Verification often occurs in high-volume, time-sensitive settings and may be handled by frontline staff, franchisees, small business owners or digital systems. The policy settings should therefore be practical, low-cost and clear enough to support consistent implementation across large and small retailers.

Consumer confidence will also be critical. Customers must be confident that using a digital credential does not expose more personal information than necessary and that physical or assisted options remain available where they cannot or do not want to use a digital credential.

ARC considers that the Commonwealth Verifiable Credentials Trust Framework should be guided by legal equivalence, good-faith reliance protections, open verifier access, interoperability, low-cost trust services, selective disclosure, protections against issuer tracking, clear implementation guidance, consumer education and continued support for physical and assisted channels.

AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

## Detailed comments

### 1. Legal equivalence and good-faith reliance

ARC notes the proposed policy position that verified digital credentials should be treated as equivalent to the relevant physical credential. ARC supports this principle, provided the system is sufficiently rigorous, reliable and supported by clear guidance for businesses.

Retailers require confidence that a digital credential can be accepted wherever the equivalent physical credential would be accepted. This may include age verification, concession eligibility, parcel collection, regulated transactions and workforce checks. Without this certainty, retailers may be cautious about accepting digital credentials or investing in the systems needed to verify them.

Equivalence should also be supported by a clear safe harbour for businesses that rely in good faith on a successfully verified credential. This is particularly important where a retailer has followed the approved verification process but the credential is later found to have been compromised, revoked or improperly issued.

Retailers should retain the ability to apply proportionate risk-based controls. Additional checks may be appropriate for unfamiliar credential types, sensitive goods, high-value transactions, regulated deliveries, failed verification attempts or other circumstances where there is a reasonable operational or legal concern. The framework should provide guidance on how this risk-based discretion operates alongside the principle that genuine digital credentials should not be refused simply because they are digital.

### 2. Open verifier access

ARC supports an open-by-default model for verifiers and does not support mandatory accreditation, registration or approval requirements for retailers undertaking routine credential verification.

Mandatory accreditation would add cost and complexity, particularly for small and medium businesses, and could slow adoption. Retailers already operate under a range of privacy, consumer, workplace, cyber security and sector-specific obligations. The framework should avoid duplicating those obligations or creating new barriers to routine verification.

Additional verifier assurance may be justified for some highly sensitive credentials, but those cases should be narrow, well-defined exceptions rather than the default position.

ARC would support an optional trusted verifier listing for businesses that want to demonstrate a higher level of assurance. However, this should remain voluntary and should not become a practical requirement for retailers to verify credentials.

ARC also cautions against classifying routine driver's licence verification for short-term vehicle hire as a high-risk verifier activity requiring accreditation. Vehicle hire operators already undertake licence verification as part of a regulated commercial activity, and additional accreditation requirements could create unnecessary disruption across hire networks without a clear corresponding benefit.

### 3. Interoperability and low-cost trust services

Interoperability is critical. Retailers should not need to support different technical approaches for different jurisdictions, agencies, wallets or credential types. Fragmented implementation would increase integration costs, create operational confusion and reduce the incentive to invest in verification capability.

Level 29
31 Market Street
Sydney NSW 2000

ARC supports nationally consistent standards, common technical specifications, wallet certification criteria, trusted registers of issuers and wallet providers, and common APIs and software tools. Retailers should be able to accept credentials from any standards-compliant wallet, including commonly used digital wallets, and should not be locked into a single Commonwealth application, closed system or narrow list of approved wallets.

Core Commonwealth trust services should be free or low cost and treated as critical digital infrastructure. Point-of-sale, e-commerce, workforce management and customer service systems may require updates to support credential verification. Standardised APIs, software libraries, test environments and implementation guidance would reduce duplication and make adoption more feasible, particularly for smaller retailers without large internal technology teams.

Interoperability will also be relevant for logistics and parcel services. For high-value, sensitive or regulated deliveries, verifiable credentials may support sender and recipient verification, provided the systems are consistent and can be used across digital and face-to-face channels.

## 4. Privacy and data minimisation

Verifiable credentials may help reduce the amount of personal information retailers need to collect and retain. For example, a retailer may need to confirm that a customer is over 18 without collecting their full date of birth, address or document number. A business may need to confirm that a customer holds a concession entitlement without retaining unnecessary card details.

ARC supports selective disclosure, data minimisation and clear limits on what information a verifier may request and retain. The framework should distinguish between preventing issuer tracking and allowing verifiers to retain records where there is a lawful or genuine business need. For example, businesses may need to retain records for compliance, insurance, audit, dispute resolution, fleet management or other operational purposes. Where retention is required, businesses should retain the minimum data needed and apply existing privacy and security safeguards.

The framework should prevent issuer tracking. Verification should not allow an issuer to see when, where or how a person uses a credential, unless a specific lawful exception applies. This will be important for public trust and to the willingness of customers and workers to use digital credentials in everyday settings.

Practical guidance should be provided for common retail use cases, including proof of age, concession entitlement, parcel collection, regulated product collection or delivery, workforce onboarding, right-to-work checks, licensing and supplier compliance. Examples of appropriate and inappropriate data requests would be particularly useful for small businesses that do not have in-house privacy expertise.

## 5. Implementation, training and inclusion

The implementation of verifiable credentials will require consideration of point-of-sale, e-commerce, workforce and customer service processes. Staff will need to understand what a valid presentation looks like, what information can be requested, what should not be collected, how to manage failed verification and how to support customers who cannot or do not want to use a digital credential.

This is a critical implementation issue. Government-led digital reforms can fail to achieve their intended benefits where the practical impacts on businesses, frontline staff and consumers are not considered early enough. The framework should therefore be designed with implementation in mind from the outset.

AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

ARC recommends nationally consistent training materials, implementation toolkits and pilot programs for both large retailers and small businesses. Guidance should be practical and scenario-based, covering common frontline situations such as age checks, parcel collection, online verification, concession checks, workforce onboarding and regulated product transactions.

Consumer education will also be important. Customers must understand how verifiable credentials work, what information is being shared, what information is not being shared, and how their privacy is protected. Without this confidence, adoption is likely to be slower and retailers may face more questions or resistance at the point of service.

Verifiable credentials should remain an additional option, not a replacement for physical credentials. Customers who do not have a digital wallet, have limited connectivity, live in regional or remote areas, are visiting from overseas, have accessibility needs or prefer physical credentials must continue to be served. Clear fallback processes will be needed where a person cannot present a digital credential, where verification fails or where a physical credential remains the most appropriate option.

## 6. Retail use cases, security and liability

ARC considers that verifiable credentials are most likely to deliver value where they solve high-volume verification problems and provide clear benefits to businesses and consumers. Relevant retail use cases may include proof of age, customer identity checks, parcel collection, short-term vehicle hire, concession and entitlement verification, workforce onboarding, licensing, contractor verification, supplier compliance, product authenticity and supply chain assurance.

These use cases should be prioritised where they reduce fraud, improve privacy, reduce manual paperwork, speed up customer service and create clear public or economic benefit. Some use cases, including supply chain assurance, may require a longer transition because they involve multiple parties, smaller suppliers and sometimes international systems. The framework should recognise these implementation realities and avoid assuming uniform readiness across the sector.

ARC notes that verifiable credentials may reduce fraud and improve assurance, but they will not remove all risk. Credential verification depends on issuer trust, wallet security, revocation processes, device security, staff behaviour and the surrounding business process.

The framework should support strong security standards while avoiding unreasonable liability for verifiers that have relied in good faith on Commonwealth trust services and followed reasonable procedures. This will be important to building confidence across the retail sector and ensuring verifiable credentials reduce compliance friction rather than adding to it.

ARC looks forward to continuing to work with Government on the development of a trusted, interoperable and practical verifiable credentials system. Any queries in relation to this submission can be directed to policy@retail.org.au.