



\Orchestrating a brighter world

A high-angle, wide shot of a modern retail store interior. The store has a curved, multi-level design with a white metal railing on the upper level. The ground floor is filled with clothing racks and display cases. A blue semi-transparent overlay covers the middle section of the image, containing the title and subtitle text. The floor is a mix of light wood and dark grey tiles.

Facial Recognition in Retail: A Practical Guide to Safer Stores

Protecting staff and customers by identifying repeat offenders before incidents occur.

INDUSTRY GUIDE

At a Glance



Staff and Customer Safety

- Retail workers increasingly face aggression and violence
- Employee and customer safety is becoming a critical operational concern



Repeat Offenders and Retail Crime

- Repeat offenders frequently target multiple stores
- Organised retail crime is increasing



Limits of Traditional Security

- CCTV often records incidents after they occur
- Identifying repeat offenders across locations is difficult



Where Facial Recognition Helps

- Identifies repeat offenders
- Alerts store teams in real time
- Supports earlier intervention

The Retail Crime Landscape in Australia

Staff and Customer Safety

- \$7.79 billion estimated annual cost of retail crime in Australia
- Retail crime represents approximately 2% of retail turnover nationally

Source: Griffith University ANZ Retail Crime Study 2024

Theft Incidents Are Increasing

- 595,000+ theft victims recorded nationally in 2024
- 70% of retailers report increased theft in the past year
- Retail locations account for nearly half of theft incidents nationwide

Source: Australian Bureau of Statistics - Crime Victimisation, Australia.
Australian Retailers Association (ARA)

Violence Toward Retail Workers

- Retail employees increasingly face hostile behaviour from customers
- 87% report verbal abuse
- 25% report experiencing physical violence

Source: Shop, Distributive and Allied Employees Association (SDA)

Repeat Offending is Common

- Retail crime frequently involves repeat offenders and organised theft groups targeting multiple stores
- Common targets include: cosmetics, electronics, alcohol, health products
- Top 10% of offenders are responsible for around 60% of retail crime

Source: Australian Retailers Association

Inside This Guide

Retailers are increasingly exploring new ways to protect staff and reduce crime while maintaining a positive customer experience. This guide explores the role facial recognition technology can play in helping retailers strengthen store security:



1. Executive Overview
2. The Problem Retailers Face
3. Why Traditional Security Approaches Are Struggling
4. Where Facial Recognition Fits
5. How Facial Recognition Works
6. Governance, Privacy and Responsible Use
7. Responsible Deployment Framework
8. Operational Implementation
9. Practical Retail Scenarios
10. Risks and Mitigations
11. What Success Looks Like
12. Conclusion

1. Executive Overview

Retail environments across Australia are facing increasing pressures from rising incidents of aggression toward frontline staff, organised retail crime, and repeat offending.

For many retailers, the challenge is no longer limited to loss prevention. Increasingly, the priority is protecting staff and customers while maintaining a safe and welcoming store environment.

Traditional security tools such as CCTV and security personnel remain important, but they often operate reactively, identifying incidents only after they occur. Retailers are therefore exploring technologies that enable earlier identification of risks and improved situational awareness.

One such capability is live facial recognition (LFR). LFR systems compare facial images captured by cameras in real time against a watchlist of individuals previously involved in theft, violence, or other disruptive behaviour. Importantly, LFR is currently the only technology capable of identifying known repeat offenders before an incident occurs, allowing trained staff to verify alerts and manage potential risks proactively.

When implemented responsibly, LFR can help retailers improve staff safety, reduce repeat incidents, and strengthen overall store security.

2. The Problem Retailers Face

Retail crime is now one of the most significant operational challenges facing Australian retailers.

However, beyond financial loss, many retailers are increasingly concerned about the safety of frontline employees and customers. Incidents involving verbal abuse, threats, and physical aggression are placing new pressures on retail environments.

Losses from theft, fraud, and related incidents are estimated at \$7.79 billion annually.

Key Insight

For many retailers, the primary concern is no longer just theft. Preventing violence and protecting staff and customers has become the priority.

Surveys show that nearly nine in ten retail workers experience verbal abuse, while one in four report physical violence.

These incidents affect:

- Staff wellbeing
- Employee retention
- Customer experience
- Operational continuity

Retail crime is therefore both a financial challenge and a workplace safety issue.

3. Why Traditional Security Approaches Are Struggling

Retailers rely on several established security tools:

- CCTV surveillance
- Electronic Article Surveillance (EAS)
- Security guards
- Incident reporting systems

CCTV is reactive

Records incidents after they occur rather than preventing them

Security staff have limited coverage

High precision

Repeat offenders are difficult to track

Costly and infrequent

Organised retail crime is increasing	Limited visibility across stores	Manual identification is unreliable
Groups increasingly target high-value goods across locations	Retailers may struggle to share information about repeat offenders across multiple locations	Staff must rely on memory or manual records to recognise banned individuals

Key Insight

Security staff cannot realistically remember every repeat offender's face, particularly across multiple stores. Live facial recognition enables retailers to consistently identify known repeat offenders in real time, helping staff intervene earlier and prevent incidents before they escalate.

4. Where Facial Recognition Fits

Facial recognition technology works best as one layer within a broader retail security strategy.

It complements CCTV and security personnel by helping retailers identify known offenders entering the store. In retail environments, facial recognition can support:

- Identifying repeat offenders
- Alerting staff when watchlisted individuals enter
- Enabling earlier intervention

Retail deployments typically use LFR to compare facial images captured at store entry points against a controlled watchlist of individuals previously involved in theft, violence or abusive behaviour.

If a potential match is detected, authorised staff receive an alert and determine the appropriate response.

5. How Facial Recognition Works

Facial recognition systems perform three core functions.

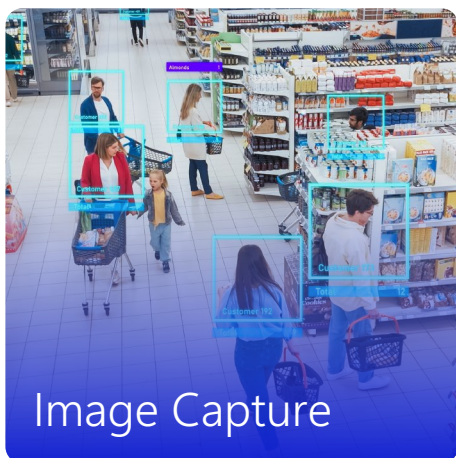
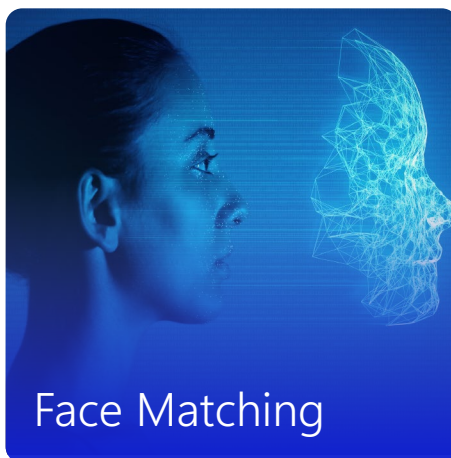


Image Capture

Cameras capture facial images at store entry points.



Face Matching

The system compares facial features against biometric templates stored in a secure watchlist.



Real-Time Alerts

Authorised staff receive an alert and verify the potential match. This human-in-the-loop workflow ensures the system supports decision-making but never replaces human judgement.

Key Insight

Responsible deployments include safeguards such as human verification of alerts, limited watchlists, and secure data storage

6. Governance, Privacy and Responsible Use

Facial recognition deployments must align with Australian privacy legislation. The Privacy Act 1988 and the Australian Privacy Principles (APPs) establish requirements for organisations managing personal information.

Several regulatory reviews of LFR deployments in retail have reinforced the importance of strong governance frameworks, transparency with customers, and human verification of system alerts.

Key governance considerations include:

Lawful purpose – Technology should be deployed for legitimate purposes such as protecting staff and preventing crime

Transparency – Customers should be informed through signage and privacy policies

Data security – Biometric data must be protected through encryption and restricted access

Data minimisation – Information should only be retained as long as necessary

Many organisations also conduct a Privacy Impact Assessment (PIA) before deployment to evaluate privacy risks and ensure compliance with regulatory obligations.



7. Responsible Deployment Framework



8. Operational Implementation

Successful deployment requires clear procedures and staff training. Operational elements typically include:

Alert Handling

Staff review alerts and verify potential matches

Incident Documentation

Actions are recorded to support accountability

Watchlist Governance

Only authorised personnel can enrol individuals, using controlled approval processes

Non-Confrontational Engagement

Employees respond calmly and professionally

Staff Training

Employees receive training on procedures and technology use

Program Review

Systems are reviewed regularly to ensure effectiveness and compliance

9. Practical Retail Scenarios

These examples illustrate how facial recognition can support different retail environments; actual deployments may vary depending on store type and operational needs.

Scenario 1 - Supermarkets

Situation - Supermarkets frequently experience repeat theft incidents involving high-value goods such as alcohol, meat, and cosmetics. In some cases these incidents escalate into aggressive or threatening behaviour toward store staff

Challenge - Store teams must identify individuals linked to prior incidents while managing busy stores and maintaining positive customer interactions

Approach - LFR systems compare faces captured at store entry points against a watchlist of individuals previously involved in theft or aggressive behaviour

Outcome - Earlier identification of repeat offenders helps store teams manage risks proactively and improve safety for staff and customers

Scenario 2 - Electronics Retail

Situation - Electronics retailers are often targeted by organised retail crime groups seeking high-value products such as smartphones, tablets, and gaming devices

Challenge - Retailers must manage coordinated theft attempts while maintaining visibility across multiple store locations

Approach - Facial recognition technology helps identify individuals previously involved in theft incidents when they enter the store, enabling security teams to increase situational awareness

Outcome - Improved security visibility and a more proactive response to organised theft activity



Scenario 3 - Pharmacy & Health Retail

Situation - Pharmacies often operate with smaller store teams and carry high-demand items such as cosmetics, supplements, and over-the-counter medications

Challenge - Staff may be exposed to aggressive behaviour or repeat theft incidents while managing limited personnel resources

Approach - Facial recognition systems alert staff when individuals previously associated with abusive or threatening behaviour enter the store

Outcome - Improved staff awareness and safer working environments for frontline employees



Scenario 4 - Hardware & Lifestyle Retail

Situation - Hardware and lifestyle retailers often experience repeat visits from individuals involved in theft, intimidation, or aggressive behaviour toward staff

Challenge - Large store layouts and multiple entry points make it difficult for teams to recognise repeat offenders quickly

Approach - LFR systems monitor entry points and compare captured images against a watchlist of individuals linked to prior incidents

Outcome - Improved visibility of repeat offenders entering the store allows teams to respond earlier and support safer working environments

10. Risks and Mitigations

Risk	Description	Mitigation
Privacy concerns	Customer concerns about biometric data	Transparent policies, signage, and public information
Data security risks	Unauthorised access to data	Encryption and access controls
Algorithm bias	Accuracy differences across groups	Independent testing and diverse datasets
Over-reliance on technology	Automated decisions	Human verification of alerts
Reputational risk	Public concerns about surveillance	Clear communication and governance
Legal compliance	Regulatory obligations	Privacy impact assessments

11. What Success Looks Like



Retailers implementing facial recognition technology typically measure outcomes across several areas.



Improved staff safety

Earlier identification of repeat offenders can reduce aggressive incidents



Reduced repeat offending

Consistent identification helps deter repeat visits



Better situational awareness

Security teams gain improved visibility across stores



Strong governance

Clear policies and oversight ensure responsible use

12. Conclusion

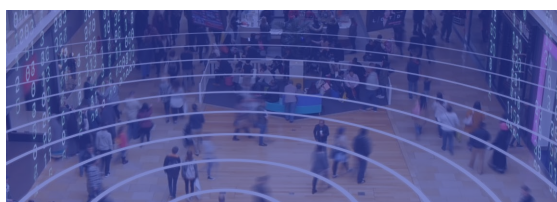
Retail crime and customer aggression are increasing challenges for Australian retailers.

Facial recognition technology offers one potential tool to help address these issues.

When deployed responsibly — with strong governance, transparency, and human oversight — it can help retailers identify repeat offenders, improve situational awareness, and create safer store environments.

The ultimate goal is not simply reducing loss.

It is creating retail environments where employees feel safer, customers feel welcome, and businesses can operate with confidence.





Orchestrating a brighter world

NEC Leadership in Biometrics

NEC is a global leader in biometric technologies, with facial recognition algorithms consistently ranked among the most accurate in independent evaluations conducted by the U.S. National Institute of Standards and Technology (NIST) and the UK National Physical Laboratory (NPL).

NEC has more than 30 years of research and development in biometric technologies, supporting deployments worldwide across border control, public safety, aviation, and retail environments.

This global experience enables NEC to support responsible and effective deployments of live facial recognition in retail environments.

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.

©2026 NEC Australia Pty Ltd. All rights reserved. NEC and NEC logo are trademarks or registered trademarks of NEC Corporation that may be registered in Japan and other jurisdictions. All other trademarks are the property of their respective owners. All rights reserved. Printed in Australia. Note: This disclaimer also applies to all related documents previously published.

nec.com.au 