Beyond the Tipping Point: Tracking the High-Speed Growth of Digital Retail Fraud in Australia

Introduction

Digital fraud in Australian retail has entered a phase of accelerated expansion, driven by structural shifts in consumer behaviour, the rapid migration to online channels, and increasingly sophisticated fraud ecosystems. No longer limited to stolen cards or isolated chargebacks, digital fraud now spans a wide spectrum of abuse that impacts retailers through every online touchpoint. This includes card-not-present fraud, refund and returns abuse, account takeover, scam-driven authorised transactions, BNPL misuse, voucher and promotion abuse, synthetic identities, and the growing pool of digitally enabled deception that results in direct merchant loss.

When viewed holistically, digital fraud has now pushed beyond a tipping point. Multiple data sources indicate that total losses across Australian retail have surged into the multi-billion-dollar range in 2024 and 2025. Growth rates are consistently in the double digits, with some categories expanding faster than overall e-commerce itself. The magnitude and velocity now warrant coordinated industry action, as individual retailers cannot absorb the rising operational and financial burden alone.

The Size of the Digital Fraud Problem

Official domestic card data provides only the starting point. The Australian Payments Network reports that card-not-present fraud reached about A$785 million in FY2024, representing 92 percent of all card fraud. This figure, however, captures only card-based online fraud and does not include the broader universe of digital retail losses. When refund abuse, returns manipulation, account takeover, BNPL fraud, scam-driven consumer misrepresentation, and digital marketplace risks are incorporated, the true cost to retailers becomes far larger.

By aggregating Australian datasets, merchant surveys, chargeback analytics, returns-fraud studies, and international benchmarks adjusted for Australia's retail turnover, the total digital retail fraud burden is estimated to fall in the following ranges:

- Card-not-present fraud: ~A$785 million
- Refund and returns abuse: A$1.0 to A$1.5 billion
- Scam-driven authorised transactions resulting in chargebacks or unrecoverable goods: A$500 million to A$1 billion
- Account takeover and credential misuse targeting retail accounts: A$200 to A$300 million
- BNPL and stored-credential retail fraud: A$200 to A$300 million
- Promo, coupon, and marketplace abuse: A$150 to A$250 million

Taken together, digital fraud losses for Australian retailers are now likely within A$3 billion to A$4 billion per year. This aligns with international patterns, where digital retail fraud has grown faster than online retail revenue for multiple years.

High-Growth Fraud Categories

Not all digital fraud types are expanding at the same rate. Several areas show particularly sharp growth.

Refund and returns abuse

Returns fraud is rising faster than any other form of retailer loss in many markets. Wardrobing, empty-box returns, false defect claims, and serial returners are now recognised as major sources of margin erosion. Retail surveys indicate that the proportion of returns containing some form of fraud or abuse has increased year on year, with apparel, footwear, consumer electronics, and cosmetics among the hardest hit categories. Generous return policies, designed for customer experience, have become structural vulnerabilities.

Scam-driven authorised transactions

A growing share of retailer chargebacks originate from customers who were deceived by external scams. Consumers are manipulated into placing high-value orders from a legitimate retailer site, often for digital goods or resellable electronics, only to later find the product diverted or used by the scammer and they then claim the transaction was unauthorised. Although technically a consumer scam, the financial burden falls on retailers who must absorb the losses. This category has grown significantly due to the rising professionalism of scam operations and the use of social engineering to trigger merchant liability.

Account takeover

Retailer accounts are increasingly targeted for credential theft. Once inside an account, fraudsters exploit saved cards, stored addresses, loyalty balances, and fast checkout flows to place rapid sequences of fraudulent orders. Account takeover losses across Australian retail are estimated in the hundreds of millions annually and are rising with the expansion of mobile shopping and one-click payment experiences.

BNPL and stored credential fraud

The growth of BNPL (Buy Now Pay Later) has created new fraud vectors for digital retail. Fraudsters exploit soft credit checks, limited identity verification, and rapid approval flows to obtain goods before detection. These losses often fall back on the merchant. BNPL fraud is growing in line with BNPL adoption and affects fashion, electronics, gaming, and lifestyle categories in particular.

Retail Categories Hit Hardest

Digital fraud affects every retail vertical, but certain sectors are disproportionately impacted due to product characteristics, return policies, and transaction patterns.

Apparel and fashion

This segment suffers some of the highest levels of refund abuse, wardrobe-as-a-service behaviour, and false defect claims. High return rates make it easier for fraudulent returns to blend in, and the growth of fast fashion and influencer cycles magnifies risk.

Consumer electronics

Laptops, phones, gaming consoles, and accessories attract non-delivery claims, account takeover, and scam-induced purchases. High resale value makes electronics one of the most common targets for digital fraud and chargeback abuse.

Online marketplaces

Marketplaces experience combined pressure from buyer fraud, seller fraud, synthetic identities, and refund claims routed through platform policies. Dispute rates are significantly higher on marketplace channels compared to direct retail websites.

Sporting goods, tools, and home improvement

These categories face return manipulation such as using items for short-term projects or swapping new products for older ones before returning them. The high unit value of items makes this behaviour costly.

Health and beauty

This sector experiences high volumes of false quality complaints and empty-box returns due to the ease of arguing subjective dissatisfaction.

Key Indicators Highlighting Acceleration

Several quantitative indicators demonstrate how rapidly digital fraud is scaling across Australian retail.

- Chargeback volumes in e-commerce have grown more than 20 percent year on year.
- The average value of disputed transactions is rising, especially during peak shopping periods.
- A significant proportion of retailers report that refund abuse and returns manipulation have increased by double digits in the last year.
- Digital account takeover attempts have climbed alongside the growth of mobile commerce and password reuse.
- BNPL-related fraud shows strong correlation with overall BNPL adoption.

Every dataset points toward the same conclusion, the digital retail fraud environment is expanding faster than internal fraud teams can manage using existing tools and processes.

Why the Industry Has Crossed a Tipping Point

Three structural forces explain why digital fraud has broken through historical limits.

1. The shift to digital retail - More than half of all retail growth is now online. As transactions migrate to digital channels, fraud follows.
2. Lower friction in payments - One-click checkouts, saved cards, BNPL, and instant refunds improve customer experience but reduce friction that traditionally deterred fraud.
3. Professionalisation of fraud - Scam networks, Telegram refund communities, and dark web fraud-as-a-service models have made digital fraud scalable, repeatable, and easy for low-skill actors to execute.

Conclusion

Digital retail fraud in Australia has moved from a controllable operational cost to a material financial risk for the entire sector. Losses now sit in the multi-billion-dollar range, spreading across chargebacks, returns abuse, account takeover, BNPL exploitation, and scam-driven authorised transactions. Growth rates show no sign of slowing, and the cumulative burden is eroding retailer margins at the same time that customer expectations for fast, frictionless service continue to rise.

The industry is now beyond the tipping point. Without coordinated intelligence sharing, standardised fraud indicators, and cross-retailer collaboration, digital fraud will continue to scale faster than individual merchants can respond.

The next phase of Australia’s retail sector will be defined not only by innovation in commerce, but by the strength of its collective response to the high-speed expansion of digital fraud.

Sources & Data Notes

This report draws on multiple data sources across the Australian retail, payments, and fraud ecosystem. Key inputs include:

Australian Payments Network (AusPayNet):
FY2024 card fraud statistics including card-not-present (CNP) fraud volumes, domestic versus international online fraud trends, and category-level fraud ratios.

National Anti-Scam Centre (NASC) and ACCC Scamwatch:
2024 scam loss reporting, authorised push-payment scam trends, consumer manipulation patterns, and cross-channel scam pressure impacting retailers.

Retail industry surveys and chargeback analytics:
Merchant-reported dispute volumes, refund and returns abuse rates, serial abuser patterns, and retailer cost data from leading payment service providers, chargeback platforms, and eCommerce risk solutions.

Returns and refund fraud benchmarks:
International datasets from the National Retail Federation (NRF), Appriss Retail, and returns-fraud studies used to estimate the Australian impact of wardrobing, defective-claim abuse, empty-box returns, and policy exploitation.

Account takeover and credential-misuse data:
Industry reporting from major identity, authentication, and fraud-risk vendors covering credential stuffing, loyalty account compromise, and eCommerce account takeover trends.

BNPL and stored-credential fraud reporting:
Loss data, approval-flow risk factors, and merchant impact assessments from BNPL providers and industry research aligned to the Australian digital commerce environment.

Marketplace, coupon, and promotion-abuse insights:
Data from marketplace platforms, retail analysts, and fraud-as-a-service monitoring groups, including synthetic identities, voucher abuse, and promotional exploitation.

Where Australian figures were unavailable, reputable international benchmarks were ratio-adjusted using Australia's retail turnover, digital penetration, and historical fraud proportions.

All loss ranges presented in this report are indicative estimates derived from aggregated datasets, industry surveys, and modelled extrapolations across the retail sector.

About the Authors

Leslie Falvey is a senior executive with deep experience across retail, payments, and digital commerce. He has worked with boards of both high-growth and large multinational organisations, focusing on governance, risk, and operational performance. Leslie has spent his career at the intersection of technology and retail, helping companies navigate eCommerce expansion, online payments, and emerging fraud threats. He brings a connected, execution-driven approach and regularly shares insights on digital fraud trends, customer abuse patterns, and practical strategies to reduce losses across the retail sector.

Tyson Hackwood is a senior executive with extensive experience across retail, payments, and digital platforms. He has led commercial, partnership, and go-to-market activities for global technology companies, working with retailers, banks, and fintechs to strengthen digital performance and reduce risk. Tyson has deep expertise in online payments, identity, and the evolving fraud landscape, with a strong track record of improving organisational resilience. He brings a practical, partnership-driven approach and regularly advises on fraud trends, ecosystem collaboration, and strategies that help retailers operate more securely and efficiently.

About CROSEC

CROSEC is an industry-led initiative dedicated to reducing digital fraud across the retail sector through collective intelligence, practical tools, and coordinated action. We bring retailers, payment providers, platforms, and technology partners together to share insights, standardise fraud indicators, and strengthen defences across the entire ecosystem. Our mission is to help retailers stay ahead of rapidly evolving fraud threats and minimise losses through collaboration rather than isolated effort.

Social Media

Connect with CROSEC on LinkedIn or X for more insights on leadership, M&A and private equity.

Website: https://www.crosec.org/

Email: info@crosec.org

LinkedIn:
https://www.linkedin.com/company/crosec/

X: @crosecassoc

Published October 2025