Peak Season 2025 in Australia: The Rising Ticket Size of Card-Not-Present Fraud

Introduction

Australia's peak online trading window spans Black Friday and Cyber Monday through to Christmas. It is consistently the period where operational load increases, and fraud controls are most likely to be stressed.

Australia Post's 2025 Black Friday and Cyber Monday results illustrate the scale of that pressure:

- Parcel volumes up 6.3% YoY across the four-day period (28 Nov to 1 Dec 2025)
- A busiest delivery day of over 5.8 million parcels
- Approximately A$1.5 billion spent online
- 3.1 million Australian households shopping online, up 9.2% YoY

Against that backdrop, the governance question for boards and senior risk leaders is whether the organisation is managing fraud as a value-at-risk problem, not a case-volume problem. In peak season, a small number of higher-value CNP events

can drive disproportionate margin erosion, increase dispute and operational costs, and force blunt control tightening that damages conversion.

Australia-wide benchmark: average value of CNP fraud transactions

AusPayNet's Fraud Statistics provide an Australia-wide benchmark for card-not-present (CNP) fraud, including both the number of fraud transactions and their total value, which allows an implied average value per CNP fraud transaction to be calculated.

AusPayNet reports the following for Australian-issued scheme cards (credit, debit, charge):

2023 (calendar year)

- CNP fraud transactions: 5,162,087
- CNP fraud value: A$687,897,333
- Implied average value per CNP fraud transaction: ~A$133

2024 (calendar year)

- CNP fraud transactions: 5,632,266
- CNP fraud value: A$816,358,630
- Implied average value per CNP fraud transaction: ~A$145

This implies the average value per CNP fraud transaction rose by roughly 9% from 2023 to 2024.

What changed from 2023 to 2024: value rose faster than volume

AusPayNet's totals show the value of CNP fraud grew materially faster than the number of CNP fraud transactions:

- CNP fraud value increased from A$687.9m (2023) to A$816.4m (2024), about +19%
- CNP fraud transactions increased from 5.16m (2023) to 5.63m (2024), about +9%

That gap is the key indicator that the average fraud ticket size is rising.

The offshore mix is becoming more expensive

AusPayNet also breaks down CNP fraud into activity perpetrated in Australia vs overseas on Australian-issued cards.

In Australia (CNP)

- 2023: 2,458,990 transactions, A$325,423,473, implied average ~A$132
- 2024: 2,660,161 transactions, A$362,242,971, implied average ~A$136

Overseas (CNP)

- 2023: 2,703,097 transactions, A$362,473,860, implied average ~A$134

- 2024: 2,972,105 transactions, A$454,115,658, implied average ~A$153

The most material change is offshore: the implied average value of overseas CNP fraud rose by about 14% year-on-year.

AusPayNet's 2024 commentary also highlights that overseas CNP fraud growth outpaced overseas spending growth.

Why peak season amplifies the "value per failure" problem

Peak periods do not need new fraud techniques to create higher losses. They amplify the cost of control gaps through three predictable mechanisms:

- Higher legitimate spend variance: gifts, one-off purchases, and unfamiliar shipping patterns increase false-negative risk.
- Queue pressure: manual review and exception handling become less selective.
- Shorter interception windows: faster fulfilment and dispatch reduce time to stop suspect orders.

If average CNP fraud ticket size is rising in the base year, peak conditions increase the probability that those higher-value events convert into real losses.

Implications for peak season 2025

AusPayNet's fraud statistics are published as calendar-year totals. They are the best Australia-wide benchmark for CNP fraud outcomes, but they are not reported as a November-December peak-season slice.

AusPayNet reports CNP fraud as calendar-year totals rather than a November-December series. As a result, Australia-wide peak-season CNP fraud averages for 2025 are not yet available in the public dataset. The points below translate the latest confirmed trend (2023 to 2024) into peak-season risk implications.

- Peak season 2025 is showing elevated online activity and delivery throughput, as reflected in Australia Post's BFCM indicators.
- The latest completed national CNP fraud dataset shows the implied average value per CNP fraud transaction increased from 2023 to 2024 and is likely to increase for 2025.

If the average value per CNP fraud transaction increased again in 2025 at a similar rate to the 2023 to 2024 uplift (about 9%), the implied average would be around A$160.

Implications for boards and fraud leaders

For boards and executives (commercial risk):

- Require value-weighted reporting, not only case counts.
- Track tail exposure: share of fraud losses coming from the top decile of order values.
- Set clear peak-season risk appetite for high-value segments (categories, fulfilment methods, customer cohorts).

For fraud and risk leaders (execution):

- Apply step-up controls to high-value baskets and high-risk fulfilment choices (expedited shipping, re-route, address change).
- Harden “account change” moments (new device, password reset, new delivery location) before allowing higher-value checkouts.
- Optimise for time-to-intercept, not only authorisation-stage detection.

Conclusion

Peak season 2025 in Australia is again demonstrating the conditions that allow CNP fraud to do outsized damage: elevated order volumes, accelerated fulfilment cycles, and higher noise in customer and delivery patterns. In this environment, the commercial risk is increasingly driven by value concentration, not just case counts.

AusPayNet shows that CNP fraud value increased strongly from 2023 to 2024, and the implied average value per CNP fraud transaction also rose. This matters because as the average ticket size rises, each control failure becomes more expensive through higher COGS exposure, higher dispute costs, and higher operational overhead, especially during November and December when teams are least able to absorb additional load.

For boards, the priority is governance that treats fraud as a value-at-risk problem with explicit peak-season risk appetite and value-weighted reporting. For fraud and risk leaders, the priority is execution: targeted step-up controls for high-value baskets, stronger account and fulfilment safeguards, and faster interception before dispatch.

Sources & Data Notes

This article draws on publicly available data across the Australian retail, payments, and economic ecosystem. Key inputs include:

Australian Payments Network (AusPayNet):
2023 and 2024 scheme card fraud statistics, including card-not-present (CNP) fraud transaction counts and CNP fraud values, with splits for activity occurring in Australia versus overseas. The implied average value per CNP fraud transaction is calculated by dividing total CNP fraud value by the number of CNP fraud transactions for each year.

Australia Post:
Peak period indicators for Black Friday and Cyber Monday 2025, including parcel throughput, household participation, and online spend estimates, used to evidence peak-season operational intensity entering the November-December trading period.

Where Australian figures were unavailable, reputable international benchmarks were used as context and, where appropriate, adjusted to Australian conditions using relevant scaling factors such as retail turnover, digital commerce penetration, payments mix, and observed fraud proportions from local datasets.

All estimates presented in this report are indicative and are derived from publicly available sources, aggregated industry reporting, and transparent calculations or modelled extrapolations. Estimates should be interpreted as directional, reflecting the limitations of reporting coverage, timing, and definitional differences across data sources.

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 digital retail fraud, payments risk, and practical loss reduction.

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

Email: info@crosec.org

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

X: @crosecassoc

Published December 2025