



The Industrialisation of Return Fraud: How generative AI turned an opportunistic nuisance into a shadow economy

Introduction

Generative AI has changed what retail fraud costs to commit, and that single fact is reorganising the whole problem. Retail fraud used to sort neatly into two boxes. Organised retail crime syndicates ran high-volume theft as a business. Friendly fraud was the otherwise ordinary customer who claimed the parcel never arrived. Those boxes have collapsed into one, because the skill that used to separate the

professional from the opportunist is now available to anyone with a browser.

Fabricating evidence, manufacturing an identity and running a convincing social engineering script each used to require real capability. None of them do now. What was a manageable line item has become a threat to margin, and it arrives at the worst possible moment: margins are already thin, and the generous returns policy that used to win customers has become one of the main ways retailers lose money. Retailers



are no longer dealing with individual bad actors. They are up against a shadow economy running automated agents, synthetic evidence and Refund-Fraud-as-a-Service. In many cases that economy is now more operationally efficient at committing fraud than the retailer is at preventing it.

The Quantitative Landscape and Financial Impact

The numbers are worse than most boards think. According to comprehensive research by Appriss Retail and Deloitte, consumers returned approximately \$685 billion worth of items in 2024, representing 13.21% of total retail sales. Within this volume, return and claims fraud accounted for \$103 billion of losses. Roughly 15% of all retail returns are now fraudulent or abusive, and that share climbs as the tools spread.

The pressure is still building. Total retail loss due to shrink, fraud, return abuse, and operational leakage is projected to reach \$796 billion in 2025. Return losses hit net profit one for one, which makes them considerably more damaging than an inventory discrepancy of the same size.

The Industrialisation of Deception: Mechanisms of GenAI Fraud

The shift comes down to one thing: the technical barrier is gone. Producing a convincing fake receipt, or a photograph of a cracked screen that was never cracked, used to take real skill in Photoshop. It now takes a prompt and about a minute.

Synthetic Evidence and RFaaS GenAI tools are now widely used to create "Synthetic Evidence" for refund claims, typically involving the fabrication of product damage or the doctoring of transaction documentation. Fraudsters use non-diffusion GenAI technology to add realistic defects, such as tears to apparel or cracked screens to electronics, to photos of pristine items.

"We are starting to see a lot more fraudulent faulty returns. The garment is completely fine, but they do not want to pay to return it, so they position it as faulty. And I have seen images come through our returns portal that I am pretty sure are AI generated."

Head of e-commerce, fashion retailer,
speaking at a CROSEC Advisory
Board session

Refund-Fraud-as-a-Service is where this turns professional. These organisations, often operating via Telegram channels like "Noir's Luxury Refunds," offer to handle the entire refund process for a consumer in exchange for a percentage of the refunded value, typically 15% to 40%. These rings use jailbroken Large Language Models (LLMs) like "WormGPT" and "FraudGPT" to automate phishing campaigns and generate brand-approved marketing copy for "lure" emails that are nearly indistinguishable from legitimate corporate communications.

Synthetic Identity and Mule Accounts
GenAI is also being used to compromise the identity layer through "Synthetic Identity Fraud." This involves creating fake personas by combining real personal information, such as a stolen Social Security number, with fabricated data.



These identities are used to open retail accounts, build positive purchase histories, and eventually execute large-scale "bust-out" schemes. The emergence of "Synthetic Money Mules" allows fraudsters to maintain control over the movement of stolen funds without the risk associated with recruiting real-person mules.

The Policy Paradox and Consumer Behaviour

The trap is that the things driving revenue are the same things being exploited. Frictionless checkout and a generous returns policy win customers and hold the door open. Approximately 82% of consumers cite free returns as a major consideration when shopping online, and 76% are more likely to choose a retailer providing an "instant refund". This demand for immediacy creates a "security gap" where automated refund systems issue credits before goods are physically inspected.

The tools have shifted what shoppers think is acceptable, too. Around 45% now say bending the truth on a return is fair game. Practices like "bracketing" and "wardrobing" are now gateway behaviours to outright fraud, with 60% of retail executives identifying wardrobing as a significant type of fraud they encounter.

However, over-correction carries high costs. False positives, erroneously flagging legitimate customers, cost merchants up to 75 times more than actual fraud attacks. Approximately 25% of buyers who experience a false decline will immediately turn to a competitor, and false positives can reduce Customer Lifetime Value (CLTV) by up to 68%.

The Board's Strategic Response: Defensive Evolution and Governance

Traditional rules-based detection is no longer sufficient. Modern defences are shifting toward Behavioural AI and Computer Vision (CV). Behavioural biometrics analyse patterns such as keystroke dynamics and navigation flow to identify bot-like consistency, improving detection rates by 23% while reducing false positives by 37%. Computer Vision is now used in processing hubs to authenticate physical damage claims, with some retailers reporting reductions in fraudulent returns by as much as 35% and a full return on investment within nine months.

Board-Level Responsibility In Australia, the regulatory environment is holding directors increasingly accountable for digital risk. ASIC has emphasised that director duties are "technology neutral," and a "wait-and-see" approach to AI regulation is no longer acceptable. The Scams Prevention Framework Act 2025 imposes legal obligations on Australian companies to protect against scams, with potential fines of up to \$50 million for non-compliance. The Australian Institute of Company Directors (AICD) has outlined eight elements of effective AI governance, including identifying accountable executives and ensuring AI use aligns with broader organisational strategy rather than just cost-cutting.

Conclusion: The Barrier Is Not Coming Back



The skill barrier is not coming back. Every month that passes makes a fabricated receipt, a fabricated defect and a fabricated identity cheaper and more convincing, and no single retailer can outspend that curve alone.

What changes the economics is not better detection inside one merchant. It is that a pattern caught at one retailer stops working at the next. Fraud scales because information does not. That is a coordination problem, and it is the one part of this the industry has never seriously tried to solve together.



Sources & Data Notes

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

Appriss Retail & Deloitte:

2024-2026 Total Retail Loss Benchmark Reports and consumer returns studies.

Australian Retailers Association (ARA):
Retail crime cost estimates.

National Retail Federation (NRF):

2025 Retail Returns Landscape report and historical return fraud data.

AICD & ASIC:

Guidelines on AI governance and regulatory signals regarding director duties.

Adyen & Experian:

2025 Retail Reports and surveys on AI-driven fraud surges.

Forter & Ravelin:

Research on GenAI image manipulation and the state of refund abuse.

AUSTRAC & NASC:

Reporting on financial crime, scams, and synthetic identity trends.



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 a retailer-led association that closes the gaps fraudsters exploit between retailers. We bring retailers together to share intelligence, agree common definitions and build honest benchmarks, so that a pattern caught by one retailer is not a surprise to the next. Retailer membership is free, permanently.

All rights reserved. No part of this publication may be reproduced without written permission. This report is provided for informational purposes only and does not constitute legal, financial, or security advice.

Social Media

Connect with CROSEC on LinkedIn or X for more on retail fraud, scams and economic crime.

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

Email: info@crosec.org

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

X: [@crosecassoc](https://twitter.com/crosecassoc)

© 2026 CROSEC. The Commercial Retail
Online Security & Economic Crime
Association.

Published March 2026

