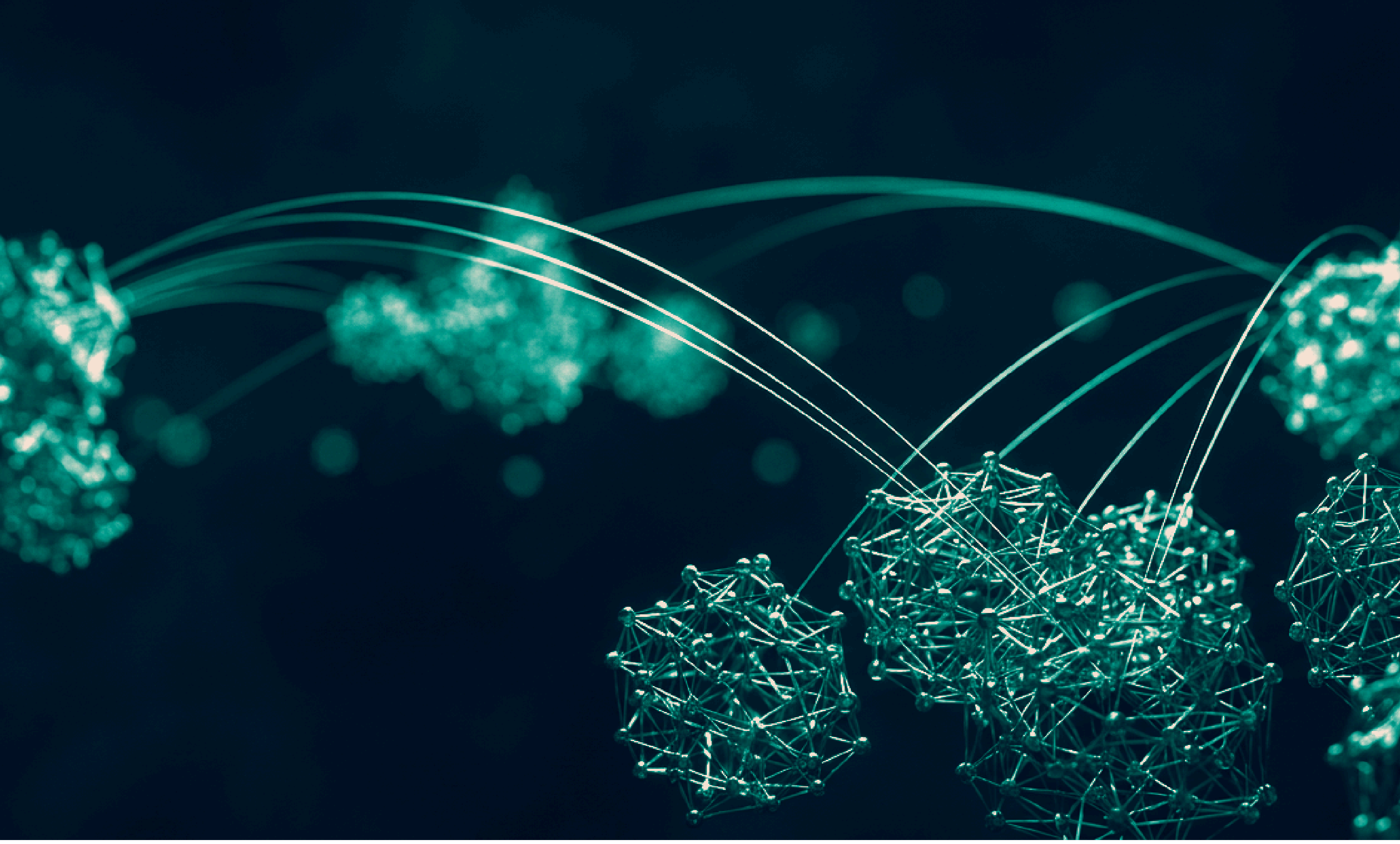


What Coordination Is Worth: How Shared Defence Reduced Fraud Loss in Two Markets

Introduction

Retailers occupy an unusual position in the architecture that has grown up around fraud and scams. They are assessed on outcomes while holding no formal place in the arrangements through which those outcomes are coordinated. They absorb losses without corresponding access to the intelligence, the standards, or the collective representation available to the financial and telecommunications sectors.

The scale of what sits on the wrong side of that line is not trivial. Our earlier analysis in The Hidden Inflation Driver put the fraud burden carried by Australian retailers at around four billion dollars a year, close to one per cent of retail turnover, and traced roughly 0.08 percentage points of headline inflation to it. Losses at that scale stop being an operational matter and become a pricing one.

Two sets of figures published over the past year indicate what coordination is worth against a problem of that size.

Neither dataset measures merchant-borne retail loss directly. What follows is evidence that coordinated defence reduces loss in adjacent categories driven by the same offenders and the same methods. It is not proof that retail losses will fall by a comparable margin, and should not be read as such.

The Australian Comparison

Australia already runs the relevant experiment within its own borders, through arrangements the industry built for itself.

Card fraud operates inside a coordinated framework: common scheme rules, shared data, and an industry body that publishes consolidated figures. In the twelve months to June 2025, fraud on Australian payment cards fell to $854 million from $868 million, and the rate declined from 77.6 cents per $1,000 spent to 71.8 cents. Domestic card-not-present fraud fell 11.1 per cent to $312 million. The improvement came against a larger exposure base rather than a shrinking one: total spending on Australian-issued cards rose from $1.1 trillion to $1.2 trillion over the same period. Online retail expenditure grew faster still, up 14 per cent to a record $82.6 billion.

Scam losses across the Australian economy, which sit within no equivalent coordinated framework, moved in the opposite direction over the same period, rising 7.8 per cent to $2.18 billion across 274,577 reports involving financial loss. Recorded retail crime offences in Victoria also reached their highest level in a decade, rising from 82,748 to 99,114 in the year to June 2025, though physical retail crime and payment fraud involve sufficiently different offenders and opportunity structures that the two should not be read as a single trend.

Both are payment-mediated, both are pursued by overlapping offenders, and both are measured nationally. One sits inside a coordinated framework and improved against rising exposure. The other does not and deteriorated. Two categories are never identical and no single comparison settles a cause, but the direction is consistent.

What Singapore Adds

Singapore recorded 37,308 scam cases and S$913.1 million in reported losses during 2025, reductions of 27.6 per cent and approximately 19 per cent respectively against 51,501 cases and S$1.124 billion the previous year. This was the first annual decline since Singapore began reporting scam figures separately, and it occurred against a regional trend moving firmly the other way. The GSMA's ASEAN Consumer Scam Report 2025, produced by the advisory firm Armidale from a survey of more than 3,000 consumers across six markets, found the proportion of consumers scammed at some point rose from 31 per cent to 45 per cent in a single wave.

Over the preceding two years Singapore had steadily widened the set of parties working to a common standard against scams. Message senders had to register, so unregistered traffic could be flagged to the recipient. Online services came into scope and were expected to act on malicious activity rather than host it. Financial institutions and telecommunications operators moved to an agreed division of duties covering who checks what, and at which point in a transaction. Police and banks established direct operational links so that funds could be stopped while a case was live.

Singapore's participants were directed into that arrangement; Australia's payments industry arrived at its own by agreement. Each step in both cases added participants to the same defence and gave them a shared understanding of their part in it. In both, the losses fell as the coverage widened.

One qualification should temper any conclusion drawn from the Singapore figures. Over the same period the proportion of Singaporean consumers describing themselves as very worried about scams rose from 23 per cent to 50 per cent. Reported losses fell while consumer anxiety approximately doubled. The measures addressed the financial outcome more effectively than they addressed confidence, and diminished confidence in a channel carries its own commercial consequence for the businesses trading through it.

Where Retail Sits

The coordinated arrangements in both markets share a feature. Singapore's brought together financial institutions and telecommunications operators. Australia's do the same, with AusPayNet coordinating the payments industry and the National Anti-Scam Centre working across government, financial institutions and telecommunications operators. Retailers are not among the parties in either.

Consumers, meanwhile, do assess merchants on results. Asked in the GSMA study which parties are demonstrably succeeding at protecting people from scams, respondents rated merchants at approximately 50 per cent, behind banks and fintechs at around 62 per cent and hardware and software providers at approximately 57 per cent, and ahead of telecommunications operators at around 48 per cent and government at approximately 40 per cent. Merchants sit squarely in the middle of the field on which the public keeps score.

When the same study asked who should hold primary responsibility, the parties it put to respondents were government and regulators, banks and e-wallet providers, law enforcement, platforms and telecommunications companies. Retail is measured on the outcome and largely absent from the conversation about who owns it.

Retail is therefore judged on performance without being assigned the mandate, the seat, or the information flow that would support it. A retailer learns when its own chargeback ratio breaches a threshold, because that is what the existing arrangements were built to monitor. It does not learn that the syndicate working through its returns process last month has started on a competitor, because no arrangement exists to carry that. The asymmetry is structural rather than anyone's decision: the flows that exist were designed for payments, and nothing was designed to move fraud signal between merchants.

An asset protection lead at a multi-brand retail group described the imbalance this way:

> *"We are required to account for our chargeback rates and to set out what we have done to bring them down. The flagging itself works well. What does not exist is anything travelling in the other direction, to help us share what we are actually seeing with each other."*

Financial services and telecommunications each comprise a small number of large institutions with long-established forums, common infrastructure and existing interlocutors. Retail spans a far larger number of businesses across more channels and more operating models, and the coordinating machinery those conditions require has never been built.

Why the Exposure Is Widening

The coordinated frameworks now in place were designed to address payment fraud, and the Australian figures indicate they perform that function competently.

The categories now growing are those in which the payment itself is entirely legitimate. Returns abuse, first-party chargebacks, loyalty and gift card depletion, account takeover on retail accounts holding stored value, and promotion and refund abuse at scale pass every control in the payments stack, because there is no defect in the payment to detect. They also fall outside every established measurement regime, which is the difficulty we ran into estimating the inflation effect in the first place. Card fraud is collated and published twice yearly. Retail-borne abuse is absorbed into shrinkage, written off, and never aggregated across businesses, so no national figure exists because no mechanism collects one.

Where transactions originate is compounding this. Approximately one in five consumers across ASEAN purchase regularly through social platforms, and those same platforms carry the highest perceived association with scam activity in the GSMA data, with Facebook cited by 61 per cent of respondents. Consumers are transacting in the environments they trust least, and the merchant frequently stands at the end of a transaction that was compromised well before it arrived.

Falling card fraud should not therefore be read as falling retail loss. The two are distinct, and only one of them is under observation.

Limitations

Four qualifications apply to the Singapore result.

The national figures record consumer scam losses rather than merchant-borne retail fraud. These are adjacent rather than equivalent, and a reduction in one does not establish a reduction in the other.

Displacement has not been excluded. Singapore's own experience demonstrates the pattern: registration requirements substantially closed the SMS channel, and activity migrated to applications and social platforms. A national decline may partly reflect movement into channels that are not measured, or into markets with less developed controls.

The composition of losses altered rather than improving uniformly. Government official impersonation scams rose sharply in the same period the aggregate figures fell.

A single year does not establish a trend. The first recorded decline is a significant development, but presenting it as a resolved problem would overstate what the data supports.

What Follows

Both markets point the same way: losses fall where the response is coordinated and rise where it is not. Singapore widened coordination across an ecosystem. Australia built it inside one layer of its payments industry, by agreement between the participants.

For retail the useful implication is that the benefit is not contingent on the route. Three elements account for most of it, and none requires external intervention.

Shared definitions come first, because retail cannot presently compare its own performance. The same event is classified differently across businesses, and a measure that is not consistently defined cannot be benchmarked. Establishing a common taxonomy for fraud, policy abuse and disputes is a matter of agreement rather than authority.

Benchmarking follows from it. A retailer unable to determine whether its losses are typical cannot determine whether its investment is proportionate, and cannot construct an evidenced internal case for the resources required. Aggregate, anonymised, category-level comparison resolves that while exposing no individual business.

Early warning is the third and probably the most immediately valuable, because a pattern identified at one retailer is currently rediscovered independently by the next, at full cost. Intelligence moving between retailers faster than the offender does converts a repeatable method into a single-use one.

A head of risk at a fashion brand at a recent meeting put the gap simply:

> *"The customer I have already blocked is very likely the customer you are about to serve, and neither of us has any way of knowing it."*

The same logic governs whether anything can be done about it afterwards. As a loss prevention lead at a department store group in a recent meeting observed:

> *"An offender who costs me a thousand dollars is not a case anyone will take. Put sixteen retailers together and the same offender is worth fifty thousand, and then it is a case."*

None of that happens spontaneously. Left to itself, an industry tends toward free-riding, since a business can benefit from what others contribute without contributing itself, and toward caution, since no individual firm wants to be first to hand anything over. Both are solved by design rather than goodwill.

The design requirements are reasonably well established. Contribution is aggregate and category-level rather than transactional, so nothing identifying a customer moves. A neutral party holds the data rather than retailers exchanging it directly, which removes the bilateral relationships that make legal teams uneasy. Nothing publishes until a minimum number of contributors sits behind each category, so no participant's figures can be inferred. Reciprocity is structural: benchmarks return only to those who contribute, which is what makes free-riding self-limiting without anyone policing it.

What moves through such an arrangement is fraud signal: the fact that a delivery address, a device or a pattern of returns behaviour has been seen before, and how often. Prices, margins, supplier terms, marketing plans and customer lists are not fraud signal and have no place in it. Identifying an offender faster is not a competitive act, and nothing about a shared defence requires any participant to know anything about another's commercial position.

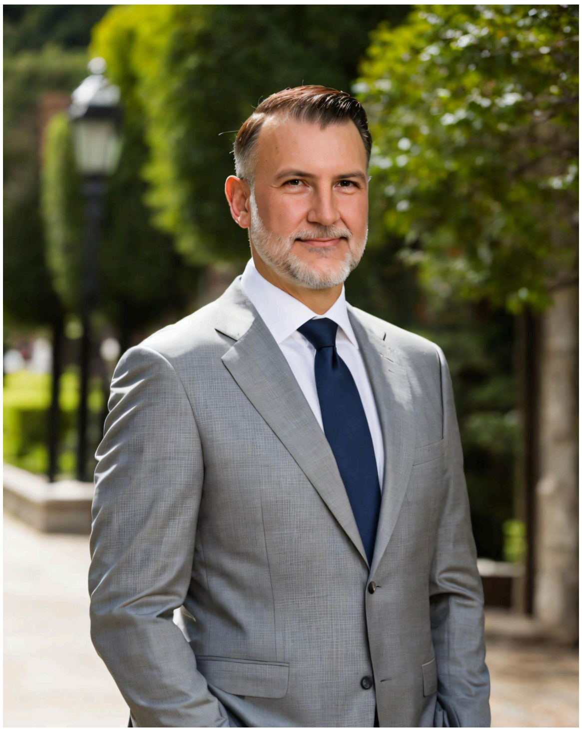
Customer acceptance is often assumed to be the barrier. The GSMA research found 72 per cent of ASEAN consumers comfortable with providers using limited, purpose-bound signals at the point of transaction to prevent fraud, rising to 78 per cent where those checks apply only to suspicious transactions. Consent is conditional rather than absent. Where the data is minimal, the purpose explicit and the trigger exceptional, consumers are already supportive. The constraint operates between institutions rather than between institutions and their customers.

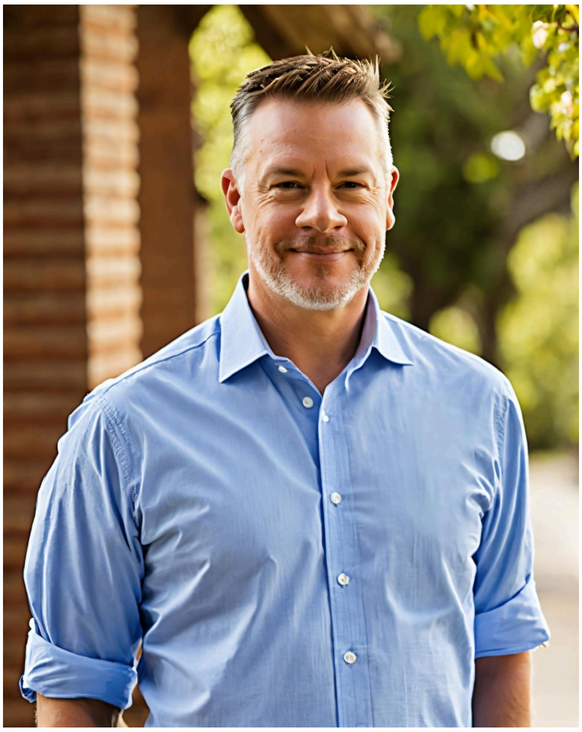
Two markets, two quite different starting points, and the same result wherever the defence was organised rather than individual. That is the finding retail should take from it. An industry that builds this deliberately should expect a benefit of the same kind, on a timetable and a design of its own choosing.

Sources & Data Notes

Singapore Police Force, Annual Scam and Cybercrime Brief 2025 and Mid-Year Scam and Cybercrime Brief 2025. Monetary Authority of Singapore, Guidelines on the Shared Responsibility Framework. Australian Payments Network, Fraud Statistics July 2024 to June 2025. Australia Post, eCommerce Report 2026. Australian Competition and Consumer Commission, Targeting Scams: report of the National Anti-Scam Centre, 2025. Crime Statistics Agency Victoria, recorded offences year ending June 2025. GSMA, ASEAN Consumer Scam Report 2025: Victims Rising, Defences Under Strain, produced by Armidale, surveying more than 3,000 consumers across Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. CROSEC, The Hidden Inflation Driver, November 2025. Quoted remarks are from senior retail practitioners speaking under Chatham House rules and are reproduced without attribution.

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.

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

Published August 2026