

PayIntelli's Newsletter

Exploring the intelligence powering the next generation of payments

PAYMENT FRAUD BRIEFING

The Fraud Defense Reckoning

AI, False Declines, and the New Economics of Payment Fraud

EXPOSURE

72% of organizations struck by payment fraud

SCALE

\$48B lost to ecommerce fraud in 2025 alone

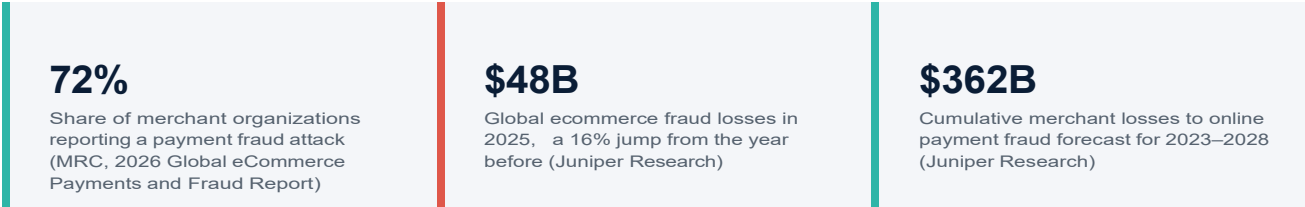
DETECTION

87–94% accuracy for AI-powered systems

01 · THE LANDSCAPE

Fraud Is Winning. For Now.

As of 2026, payment fraud had struck 72% of organizations. That is what the data is telling us here, and why it matters more than ever: fraud is not only increasing, it is changing more rapidly than most organizations can adapt to.



The MRC's report, surveying 1,278 merchant professionals across 37 countries, quantifies a shift many practitioners already sense: first party fraud — customers disputing their own legitimate purchases, now accounts for roughly 36% of all fraud cases globally, more than doubling within a single year. This is not a story about better detection catching more of the same fraud. It is a story about the composition of fraud itself changing faster than most fraud programs were built to track. Separately, Juniper Research's ecommerce specific fraud forecast shows losses climbing from \$44.3 billion in 2024 to a projected \$107 billion by 2029 a 141% increase over five years, driven substantially by AI-powered attacks and the rise of friendly fraud.

Any business making payments at meaningful scale is not looking at theoretical industry figures; it is looking at its own chargeback rates, its own overhead, and its own bottom line.

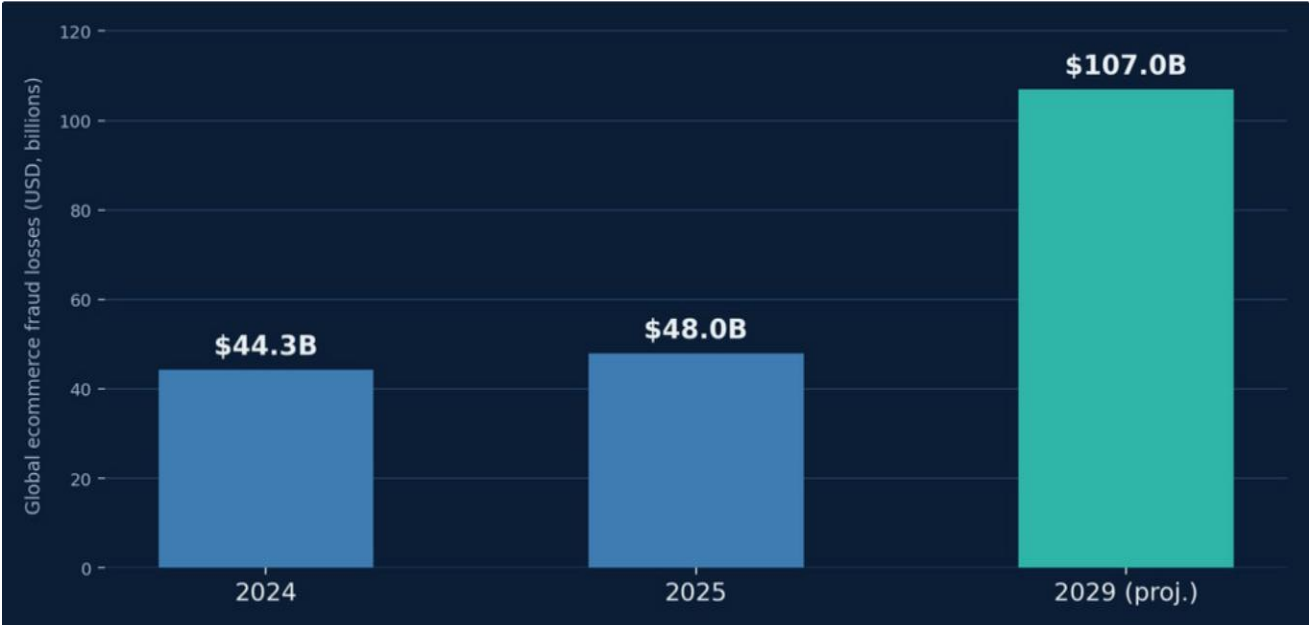
Why this is a structural shift, not a cycle: for more than three decades, fraud detection operated the same way — a new fraud type would emerge, analysts would study it, a rule would get written, and fraudsters would find the gap. AI is beginning to close that gap, and the evidence is starting to stack up in ways that are hard to ignore, as the following pages show.

Sources: Merchant Risk Council, 2026 Global eCommerce Payments and Fraud Report; Juniper Research, Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023–2028; Juniper Research, ecommerce fraud loss forecasts.

02 · THE SCALE OF THE PROBLEM

The \$362 Billion Problem Payments Still Hasn't Solved

Online payment fraud is on track to cost merchants \$362 billion between 2023 and 2028. The trajectory for ecommerce fraud specifically shows why the industry's response is only now starting to catch up.



Global ecommerce fraud losses, actual and projected. Source: Juniper Research.

Where the Losses Concentrate

Loss category	Scale	What's driving it
Chargeback volume	337M transactions by 2026	Up 41% from 238 million in 2023; roughly 61% are first-party ("friendly fraud") disputes, not criminal fraud
US chargeback value	\$15.3B	Concentrated in card-not-present ecommerce transactions
Cost per dollar of fraud	\$4.61 per \$1	Total cost to US merchants including fees and operations, up 32% since 2022 (LexisNexis)
Account takeover losses	\$17B in 2025	Credential-stuffing and session-hijacking attacks against existing customer accounts

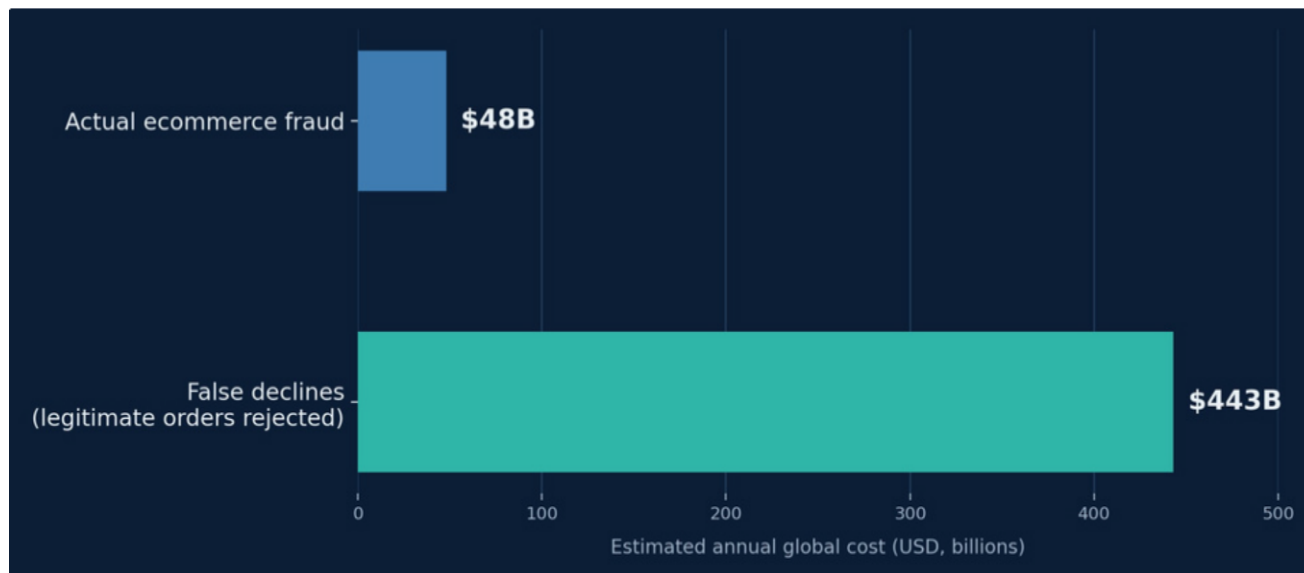
Chargebacks are where most organizations are quietly bleeding. The volume of chargebacks is expected to reach 337 million transactions by 2026, a 41% increase from 238 million in 2023. What surprises most people is that roughly 61% of these disputes are the friendly-fraud kind: real customers contesting actual purchases. That is not primarily a technology problem, it is a problem of relationship, visibility, and evidence, and it explains why fraud losses and chargeback losses need to be tracked as related but distinct problems.

Sources: Chargebacks911, chargeback volume projections; LexisNexis Risk Solutions, True Cost of Fraud study; industry account-takeover loss estimates for 2025.

03 • THE HIDDEN COST

False Declines: The Cost Nobody Budgets For

One of the least-discussed numbers in this whole discussion is not fraud at all. It is the legitimate transactions that overly aggressive fraud filters reject, and by most industry estimates, this costs global retailers far more than fraud itself.



Estimated annual global cost of false declines versus actual ecommerce fraud. Figures trace to a long-standing Aite-Novarica/Javelin estimate widely re-cited across the industry; treat as directional rather than precise. Sources: Riskified; Juniper Research.

False declines are estimated to cost global retailers roughly \$443 billion annually, about nine times the value of actual ecommerce fraud losses. Of the orders that get rejected each year, an estimated \$118 billion represent valid orders from legitimate customers, and by some estimates as many as 39% of those rejected customers never return to complete a purchase with that merchant again.

Why this number is easy to miss internally: a blocked fraud attempt is a visible save that shows up in a dashboard. A wrongly declined good customer is invisible lost revenue and a silently damaged relationship — which is exactly why false-decline costs are so often under-tracked relative to fraud-loss costs, even though the industry estimates put them substantially higher.

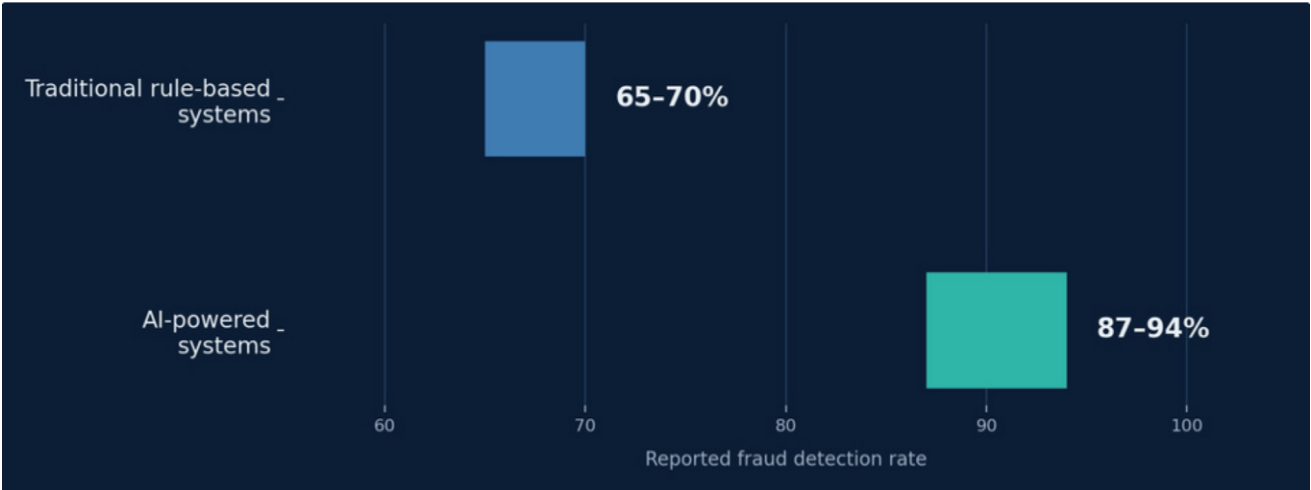
The companies that are able to manage this well are not doing it with more aggressive rules or more manual reviews. They are doing it with better signal: more context about what a legitimate transaction actually looks like across the full customer lifecycle, not just at the moment of checkout, so they can maintain a smooth ride for good customers while still catching fraud. That distinction between blocking more and blocking better — is precisely where AI-driven approaches are pulling ahead, as the next page shows.

Sources: Riskified, false-decline cost analysis; Aite-Novarica / Javelin false-decline research (widely re-cited estimate); Juniper Research, global ecommerce fraud loss figures.

04 · AI AND FRAUD DEFENSE

Where Machine Learning Actually Changes the Game

For more than three decades, fraud detection operated the same way: a new fraud type would emerge, analysts would study it, a rule would get written, and fraudsters would design around it by the time the rule shipped. The performance difference between rule-based and AI-powered detection is now large enough to show up clearly in independent research.



Reported fraud detection rates by approach. Source: 2024 meta-analysis of 47 peer-reviewed studies on AI-driven fraud detection in banking.

A 2024 meta-analysis covering 47 studies in payment fraud detection found that AI-powered systems achieve detection rates of 87 to 94%, compared to 65 to 70% for traditional rule-based approaches, while also reducing false positives by 40 to 60%. That second figure matters as much as the first: detection rate alone tells only half the story if the system that catches more fraud also rejects more good customers, which is precisely the false-decline problem described on the previous page.

40–60%

Reduction in false positives that AI-powered fraud detection systems achieve relative to traditional rule-based methods, according to the same 47-study meta-analysis — meaning fewer good customers get wrongly declined even as more real fraud gets caught.

The mechanism behind this gap is structural, not incremental. Rule-based systems can only catch patterns someone has already written a rule for; AI models trained on transaction behavior can flag anomalies that don't match any known fraud signature, which is exactly the capability needed against fraud vectors that are evolving faster than any manual rule-writing process can rack. Industry survey data suggests a meaningful share of card issuers and acquirers have already realized measurable savings from AI-based fraud detection over the past two years — getting that reduction in false declines down matters just as much commercially as catching more fraud in the first place.

Source: 2024 systematic meta-analysis of 47 studies, "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity."

05 • WHAT'S NEXT

The Difficulty Ahead Is Worth Naming Now

The gap between AI-driven and traditional fraud detection is widening, but the fraud landscape itself is not standing still. Three shifts are worth planning for before they show up as a crisis in someone's chargeback report.

First-Party Fraud Keeps Growing

With first-party fraud now representing roughly a third of all fraud cases globally, and having more than doubled within a year, fraud teams need dispute-evidence and customer-relationship tooling that looks nothing like traditional criminal-rebuilt for a new class of payment initiator one whose fraud detection because the "fraudster" in these cases is a real, existing customer.

Agentic Commerce Is a New Attack Surface

As AI agents begin transacting on behalf of consumers, fraud models trained on human checkout behaviour will need to be "normal" behaviour patterns don't yet have historical data behind them.

The False-Denial Problem Will Get Harder Before It Gets Easier

As fraud volume and sophistication both increase, the temptation to tighten fraud rules further — and reject more borderline transactions — will increase with it. Left unchecked, that instinct widens the false-denial gap described on page 4 rather than closing it. The data throughout this report points to the same resolution: better signal and continuous learning close that gap; blunt rule-tightening widens it.

The throughline across every section of this report: whether the problem is chargebacks, false declines, or detection accuracy, the organizations pulling ahead are the ones treating fraud defense as a continuously learning system rather than a fixed set of rules updated periodically. That is precisely the shift the detection-rate data on page 5 makes concrete.

Sources: Merchant Risk Council, 2026 Global eCommerce Payments and Fraud Report; industry analysis on agentic commerce and payment fraud exposure.

06 • TAKEAWAYS & NEXT STEP

What This Means for Your Roadmap

- **Measure false declines as rigorously as fraud losses.** If you can't quantify how much legitimate revenue your fraud rules are rejecting, you are likely underestimating your largest fraud-related cost.
- **Separate first-party fraud from criminal fraud operationally.** The two require different tooling, different evidence, and different customer-relationship approaches.
- **Treat AI-based detection as a false-decline reduction tool, not just a catch-more-fraud tool.** The 40–60% false-positive reduction is often the larger commercial win.
- **Start planning for agentic-commerce fraud exposure now.** Checkout behavior models built for humans will not transfer cleanly to AI-initiated transactions.

Want to pressure-test your own fraud defense stack?

Book a working session with Payintelli's enterprise architecture team.

[Book an Enterprise Architecture Discussion](#)

- www.payintelli.com
- linkedin.com/company/payintelli
- info@payintelli.com