SEON

The Retail Fraud Report: Securing eCommerce

A vertical excerpt of the 2025 Digital Fraud Outlook

Table of Contents

Introduction

The eCommerce sector faces an existential paradox in 2025: while digital innovation accelerates transaction speeds and payment options, fraudsters exploit these advancements with unprecedented sophistication. Global fraud losses are projected to reach $48 billion this year, driven by AI-powered scams, synthetic identities and vulnerabilities in emerging payment ecosystems like digital wallets and cryptocurrencies.

Despite 75% of businesses across verticals planning budget increases for fraud prevention, eCommerce remains disproportionately underfunded, with 19% of retailers anticipating budget cuts, a notably divergent trend from the broader industry momentum. Traditional fraud detection methods are no longer sufficient in today’s frictionless economy. For eCommerce leaders, the imperative is clear: fraud prevention must transform from a backend safeguard into a strategic lever that supports growth, preserves brand integrity and secures long-term customer loyalty.

The 2025 Digital Fraud Outlook surveyed 574 global professionals in fraud, risk and compliance — including 109 eCommerce leaders — to uncover how businesses adapt to today’s fraud threats and reshape their prevention and detection programs to meet tomorrow’s challenges.

Key Industry Trends

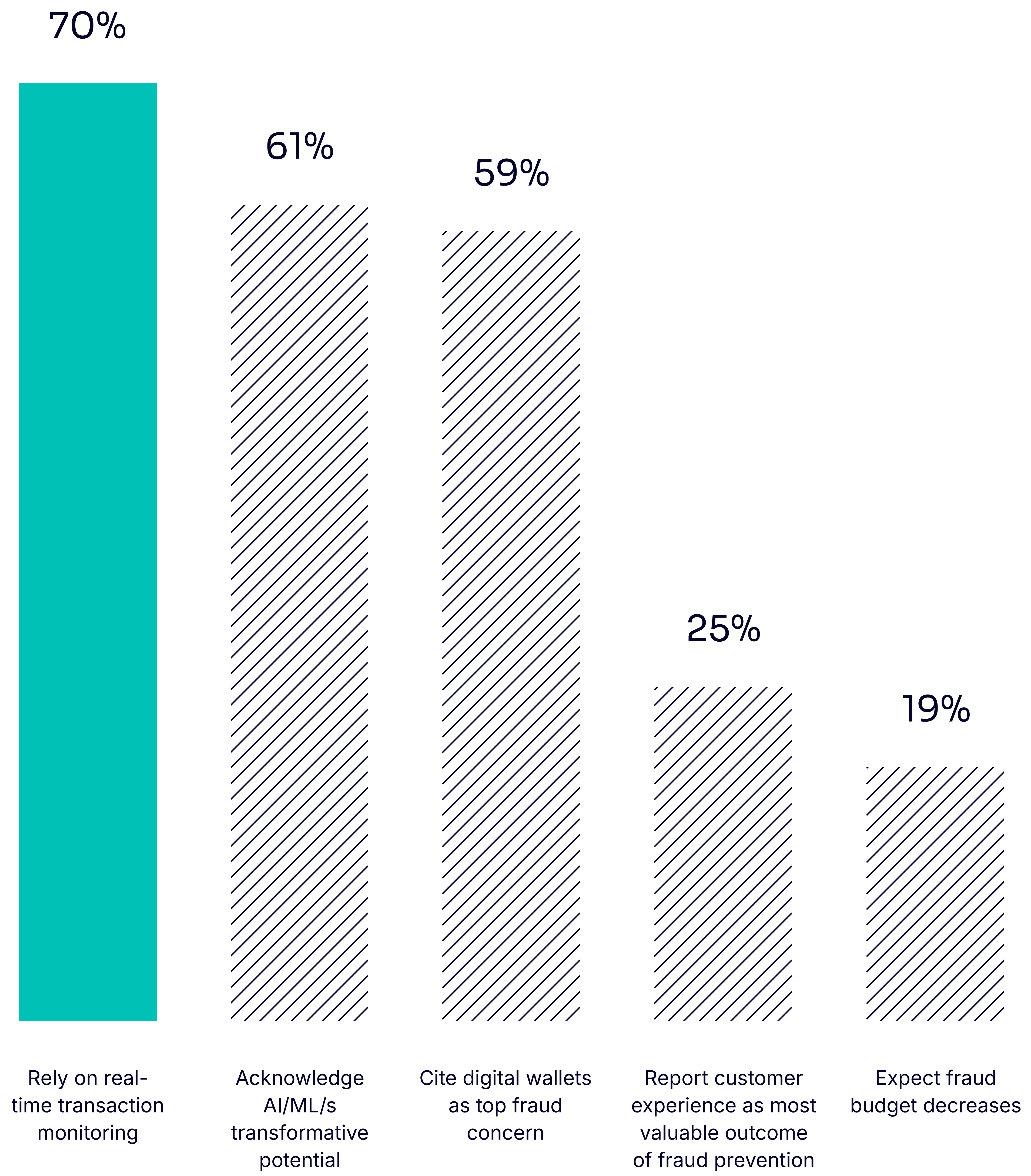
→ **Real-time transaction monitoring is non-negotiable**
70% of eCommerce organizations now classify real-time transaction monitoring as their most effective anti-fraud tool, the highest adoption rate across all industries surveyed. This shift reflects the sector’s need to match the velocity of modern payment systems, where one-click checkouts and instant refunds demand sub-second risk assessments.

→ **AI is viewed with both optimism and caution**
While 61% of eCommerce leaders acknowledge AI/ML’s transformative potential, skepticism persists. 48% report measurable value from current implementations, and 56% believe AI won’t significantly reduce human oversight needs.

→ **Digital wallets and cryptocurrencies are top fraud concerns**
Digital wallets (59%) and cryptocurrencies (40%) are seen as the most vulnerable services, reflecting the complexities and risks of new, less-regulated payment ecosystems.

→ **Customer experience drives ROI**
Improved customer experience is the most valuable outcome of fraud prevention for 25% of respondents, ranking above loss reduction (22%) or improving detection accuracy (19%).

→ **Budgets don’t match ambition**
eCommerce leads all verticals in reporting expected budget decreases (19%) for fraud prevention.



How eCommerce Differs From Other Sectors

Fraud prevention in eCommerce isn’t just a security function; it’s a brand promise. As such, the customer experience is paramount, meaning that fraud teams must constantly weigh the trade-offs between friction and risk.

The Unique Dynamics of eCommerce:

→ **Security must be invisible**
Any added friction to the customer experience can result in churn. To counter, many teams are turning to technology such as device intelligence, behavioral biometrics and digital footprint analysis, which won’t disrupt legitimate buyers.

→ **Emerging payments = emerging threats**
From loyalty and rewards programs to tokenized assets, BNPL (Buy Now, Pay Later) to decentralized finance platforms, new methods are driving innovation and attracting sophisticated fraud rings or Fraud-as-a-Service (FaaS) offerings.

→ **Operational data is fragmented**
Cost tracking remains inconsistent across the industry: while 61% track direct revenue loss due to fraud, few tie in churn, inefficiencies or reputational risks to their total calculations to obtain comprehensive view.

→ **Customer experience is the ultimate ROI metric**
eCommerce professionals rank customer experience higher than fraud loss reduction or detection accuracy when assessing their programs’ success.

High-Risk Frontiers: Emerging Fraud Threats & Impact

As eCommerce platforms innovate with faster payments, one-click checkouts and digital rewards, fraudsters exploit every new feature.

The fastest rising fraud risks include:

59%

Digital wallets
Targeted through phishing, device takeovers and fake refund claims.

40%

Cryptocurrencies
Exploited via scams, chargebacks and synthetic identities.

30%

Peer-to-peer payment fraud
Abused for money laundering and refund fraud.

15%

Loyalty and rewards abuse
Driven by stolen accounts, bots and bonus abuse.

17%

Tokenized asset fraud
Including the resale of fake NFTs or loyalty credits.

Top 5 Fraud Trends

1 AI: Hype, Hesitation & Necessity

Despite industry-wide optimism (84%) that AI will reduce the need for human oversight, eCommerce is more cautious. Only 48% believe AI currently delivers measurable value, and 56% think it will not significantly reduce the need for human intervention. While 61% agree AI will have the greatest future impact on fraud prevention, 19% still expect budget decreases for these tools and others in the coming year. The sector remains vulnerable to AI-enhanced attack vectors, yet internal debate and integration challenges persist.

2 Experience First, Strategy Second?

Customer experience is the primary ROI for eCommerce fraud teams: 25% rank it as the most valuable outcome, ahead of loss reduction (22%) and detection accuracy (19%). This friction-averse approach often leads to compromises on stronger rules or new tools if there's any risk of increased customer friction. However, 43% believe fraud is growing faster than revenue, suggesting this strategy may not be sustainable.

3 Underinvestment in the Face of Escalation

eCommerce businesses are underinvesting in fraud prevention at the worst possible time. While most industries allocate 3–4% of revenue to protect against escalating threats, 35% of eCommerce companies spend just 1–2%, a gap that leaves them increasingly vulnerable. Only 16% anticipate meaningful budget increases, and 60% expect their fraud budgets to stagnate or shrink. Headcount growth is minimal, often just patching holes left by staff turnover and not building resilience. All of this spells potential major problems for businesses and consumers alike.

4 Fragmented Tracking, Fragmented Response

Fraud tracking is nearly universal (93%), but KPI adoption is inconsistent and often poorly structured. Only 16% embed fraud into product responsibilities, and many treat it as a non-revenue-driving function.

Top tracked costs include direct revenue loss (19.5%), technology costs (19.1%), operational inefficiencies (17.7%), compliance (17.9%), human capital (17.9%), customer churn (17.9%) and reputational damage (17%). Notably, 70.8% of employees are unsure or do not track fraud and financial crime losses, and 20% have no trackable KPIs.

5 Emerging Needs, Unrealized Potential

As fraud schemes grow more complex, eCommerce teams know what’s required; they just need to operationalize prevention:

The skills gap is real, too. eCommerce fraud professionals cite advanced data analytics (37%) and AI/ML expertise (39%) as top hiring priorities, but also stress the need for cross-functional collaboration — an area where most feel under-resourced.

61% want to improve real-time monitoring

60% prioritize AI/ML investment despite persistent doubts about its current value and automation potential

43% plan to upgrade automation tools

39% seek tighter integrations with CRMs, payment gateways and case management

11% Plan to reduce human intervention, revealing limited faith in AI autonomy

The Fraud Narrative: What the Data Tells Us

Retailers are not just defending checkout pages; fraud can strike across the entire journey: sign-up, login, rewards redemption and even post-purchase support.

- Real-time fraud detection across the customer lifecycle should be a baseline.

- AI is viewed as essential, but explainability and confidence remain issues.

- Disjointed data leads to disjointed decisions — consolidating signals is essential to spot fraud across platforms and moments.

- Despite nearly universal fraud tracking, only a minority correlate metrics like churn, operational costs or support overhead into a unified cost.

What eCommerce Must Do Next:

Move at the Speed of the Modern Shopper

⟶

Real-time risk scoring is no longer a luxury. With digital wallets, instant refunds and fast checkouts becoming table stakes, fraud prevention must operate just as quickly and across the entire journey, from account creation to returns.

Leverage AI — But Keep It Explainable

⟶

Blackbox algorithms won't fly. Retailers need transparent AI that balances automation with interpretability, especially when justifying decisions to internal teams, regulators or affected customers.

Track Signals Across Silos

⟶

Fraud signals are scattered across product, payments, marketing and support. Teams that unify device intelligence, behavioral data and user context will unlock faster, more confident decision-making.

What eCommerce Must Do Next:

Define ROI in Customer Terms

→

In eCommerce, experience is ROI. The most successful fraud strategies reduce false positives and manual reviews, without increasing friction.

Don’t Let the Budget Flatline

→

With fraud threats rising, underinvestment could undo hard-won trust.

Operationalize the Total Cost of Fraud

→

Move beyond tracking chargebacks. Fraud drains brand equity, delays product launches, increases support costs and damages loyalty. Track it all.

This year, eCommerce fraud prevention will define who scales and who stalls. The retailers that embed adaptive, explainable and cross-functional strategies will win customer trust and market share.

SEON

About SEON

SEON helps risk teams detect and stop fraud and money laundering while ensuring regulatory compliance. By combining real-time digital footprint analysis, device intelligence and AI-driven rules, SEON empowers thousands of businesses globally to prevent threats before they occur. With integrated fraud prevention and AML capabilities, SEON operates from Austin, London, Budapest and Singapore. Learn more at seon.io.

This report is based on insights from a survey commissioned by SEON, gathering perspectives from fraud prevention professionals across industries. Research and analysis were conducted by Christina Brichetto & Katy Chrisler.

Learn more at seon.io