



FRAUD PREVENTION TACTICAL GUIDE

Scaling Secure E-COMMERCE OPERATIONS

An Actionable 3-Part Guide



PART 1	Tracking Risk: Fraud's Downstream Impact on Operational KPIs	3
PART 2	Spotting Hidden Fraud: Threat Signals Posing as Success	6
PART 3	Actioning Identity Trust: 5 Strategies for Driving Fast, Secure Growth	11

PART 1

Tracking Risk: Fraud's *DOWNSTREAM IMPACT* on Operational KPIs

When ops leaders feel forced to choose between stopping fraud or preserving the user experience, metrics suffer. Tracking fraud's downstream impact on KPIs uncovers hidden revenue losses, but more importantly, it surfaces gaps in the mitigation system itself.

This allows for refinements to thresholds and custom models that might inadvertently be disrupting the path from login to transaction.



Calculating Risk Through Fraud Ops KPIs

METRIC	POTENTIAL RISK	NEGATIVE KPI IMPACT
Conversion Rate	Are false positives causing cart abandonment?	Lower revenue; lower overall ROI across channels
Manual Review Load	Is fraud review slowing fulfillment?	Increased operational costs; lower acceptance rates; higher cart abandonment and churn
Chargeback Rate	Are ATOs and promo abuse slipping through?	Higher dispute fees, lost revenue, and potential processor penalties
Customer Satisfaction/NPS	Are fraud policies hurting experience?	Lower NPS; increased churn; negative customer reviews
False-Positive Rate	Are you declining more legitimate users than you realize?	Lost lifetime value (LTV); significantly higher or wasted customer acquisition costs (CAC)

When e-commerce operations stop relying on blanket friction to protect individual user touchpoints, and instead approach the customer journey holistically, growth is the natural outcome. KPIs are more likely to be positively impacted as overall costs, churn, and fraud rates go down, while ROI, acceptance rates, and revenue increase.

Instead of treating each touchpoint in isolation, businesses should map the full lifecycle—from account creation and login to checkout, loyalty, and post-purchase interactions—identifying where friction occurs and which points create unnecessary drop-offs. By analyzing funnel performance alongside fraud system logs, teams can pinpoint where trusted customers are being slowed down and where risk truly exists.

The next step is to replace static, one-size-fits-all defenses with dynamic, risk-based orchestration. Rather than forcing every user through the same verification flow, organizations can apply real-time risk scoring at sign-up, login, and checkout. Low-risk users move through seamlessly, while medium- and high-risk users receive escalating verification or are blocked entirely. This adaptive approach relies on device intelligence, behavioral analytics, and identity linking across accounts and sessions, enabling teams to detect subtle fraud patterns like synthetic accounts, policy abuse, and coordinated refund schemes that traditional rules miss.

Success requires continuous measurement and optimization against key KPIs like chargeback rate, manual review volume, approval rate, and net revenue. Feeding dispute outcomes and fraud signals back into machine learning models allows for automated improvements, while cross-team dashboards keep marketing, CX, and fraud operations aligned on growth and risk reduction. Over time, this shift not only lowers fraud and operational costs but also boosts conversion rates, customer trust, and overall ROI—making growth the natural outcome of a smarter, holistic approach to e-commerce risk management.

The most sophisticated fraud strategies are built with the full customer and business journey at the center of every decision.

By aligning fraud prevention efforts with operational KPIs, teams can protect revenue and retention even as growth expands and risks change.



PART 2

Spotting Hidden Fraud: *THREAT SIGNALS* Posing as Success

As generative AI and sophisticated automation shape attacker behavior, the line between legitimate activity and abuse is harder to see (and even harder to act on). What looks like customer growth might be synthetic account creation. What looks like strong engagement could be promo abuse at scale. And when fraud tactics blend in with normal user behavior, they have more time to spread and more opportunity to cause downstream damage.

Teams can't prevent or resolve risks that they can't see—first, emerging and evolving threats need to be identified.

Here's what to watch for.



Generative AI and **FRAUDULENT BOTS**

Allow bad actors to log in and inject scripts that mimic trusted behavior and evade static defenses, allowing them to blend in while quietly scaling the attack.



What it looks like

- 🔍 Logins, signups, or transactions that appear human, complete with realistic typing patterns, browsing behavior, and device fingerprints.

Why it hurts

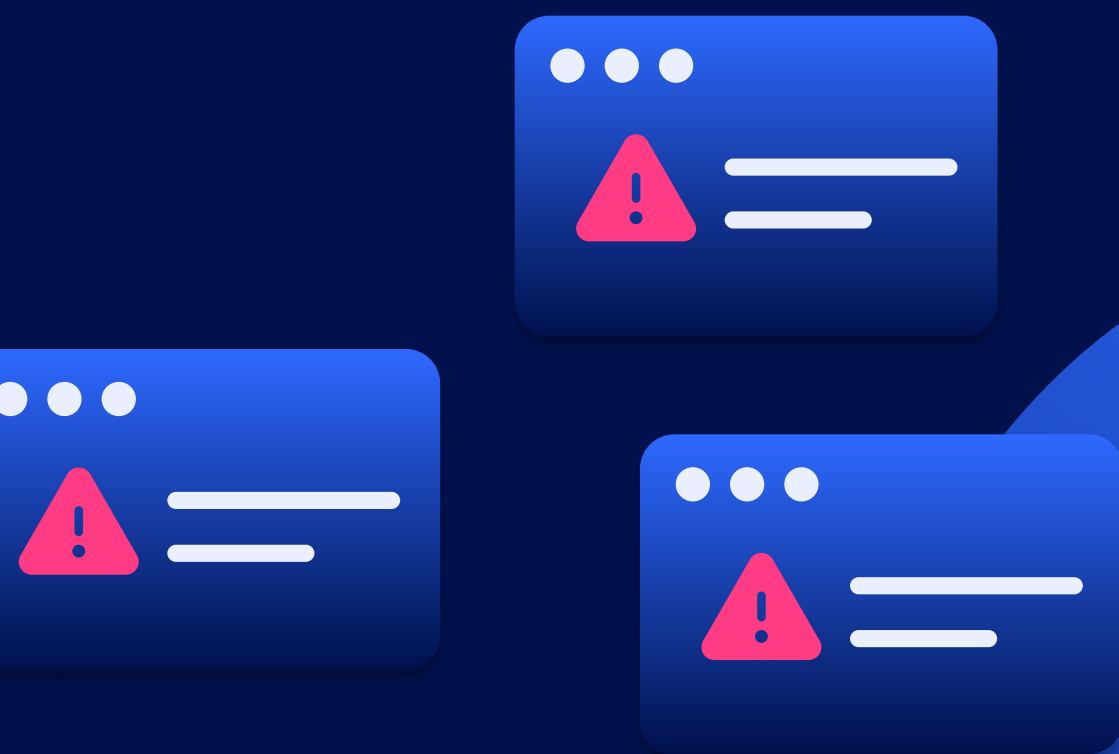
- ❗ Bots can overwhelm systems with fake accounts, test stolen credentials at scale, or exploit referral and promo programs, leading to chargebacks, skewed growth metrics, and degraded customer experience.
- ❗ Increased review queues and harder manual detection.

What to do

- ✓ Use dynamic behavioral detection that goes beyond static rules.
- ✓ Identify subtle inconsistencies in session behavior, decision velocity, and user journeys.
- ✓ Leverage real-time machine learning tuned to human patterns.

Slow and steady *CREDENTIAL STUFFING* & synthetic accounts

Allows ATOs to unfold over time,
bypassing rate limits to appear legitimate.



What it looks like

- 🕒 Legit-looking accounts stitched from real data with odd behavior and inconsistent signals.
- 🕒 Spread-out logins from multiple IPs or devices, low and slow.

Why it hurts

- ⚠️ Attackers often **farm trust** on these accounts before monetization, making eventual fraud harder to tie back.
- ⚠️ These accounts inflate acquisition metrics, abuse promos, and trigger chargebacks.
- ⚠️ ATOs with no clear login spike are harder to flag or investigate.

What to do

- ✅ Surface synthetic identities early by analyzing behavior across devices, geos, and login patterns.
- ✅ Use cross-network ML, that correlates signals across a wide merchant or user network, to detect subtle attack patterns others miss.

HIDDEN THREAT #3



Unnaturally high engagement with **LOYALTY PROGRAMS**

What looks like successful customer retention efforts can be attackers exploiting discounts and referrals at scale.



What it looks like

- 💡 Customers who appear high-LTV repeatedly push return and discount limits.

Why it hurts

- ⚠️ Your team enforces stricter policies that frustrate real customers.

What to do



- ✅ Segment true loyalty from abuse using real-time behavioral modeling.

Disputes and **CHARGEBACKS**



Drain team resources and revenue as first-party fraud slips past traditional defenses and escalates before detection.






What it looks like

-  New users who convert fast—then dispute charges or abuse returns.
-  Surging “missing item” claims or repeat refund requests.

Why it hurts

-  Marketing celebrates conversion, but ops handles the damage.
-  Manual reviews rise, trusted customers feel the fallout, and margins shrink.

What to do

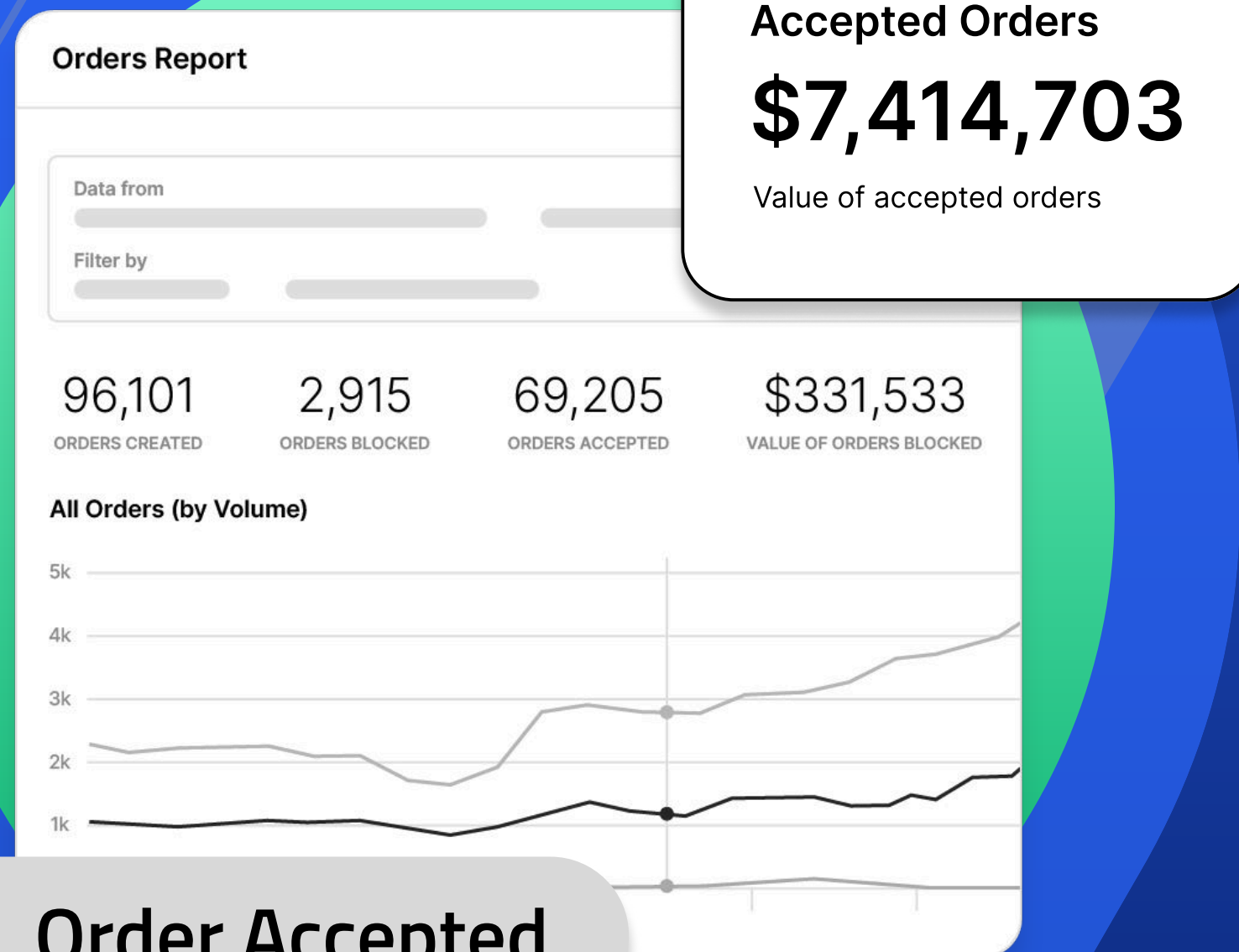
-  Score risk at signup, not just checkout.
-  Use identity signals such as device fingerprinting and IP velocity, not just transaction history.
-  Link behaviors across accounts and sessions to identify organized refund abuse.

PART 3

Actioning Identity Trust: *5 STRATEGIES* for Driving Fast, Secure Growth

Scaling trust across the customer journey takes more than toggling fraud thresholds. It requires cross-functional buy-in, measurable outcomes, and tooling that connects identity, intent, and behavior signals across every interaction.

Below are 5 proven strategies to help e-commerce leaders turn risk management into a growth driver.



✓ **Order Accepted**

1

Automate pre-auth decisioning to reduce false declines.

Delaying risk assessments until checkout increases both fraud risk and false declines. Scoring user trust earlier—at signup, login, or loyalty program access—stops abuse before it starts and protects high-value customers from unnecessary friction.

Real-time pre-auth decisioning reduces false positives by up to 80% and protects conversions without guesswork.

TUTORY CASE STUDY →

2

Use real-time identity signals across the user journey.

True identity doesn't come down to an email and password. It's a combination of behavior, intent, device intelligence, and network patterns that emerge and evolve over time.

Connect and analyze signals across accounts, sessions, and devices to identify synthetic users, sleeper accounts, and compromised credentials.

TAPTAP SEND CASE STUDY →

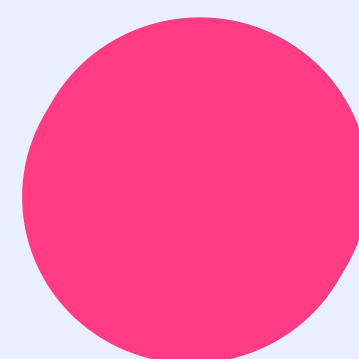
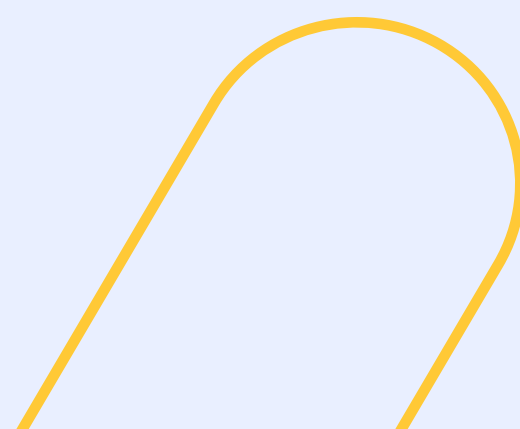
3

Minimize manual review through transparent ML

decisions. Manual reviews often stem from uncertainty around identity. Models that clearly explain why a user or transaction is risky empower teams to make more confident (and accurate) decisions faster.

Equip review teams with decision transparency that shows which identity signals contributed to the risk score.

ATOM TICKETS CASE STUDY →



4

Align fraud, CX, and fulfillment with shared KPIs. When teams define “trusted users” differently, they introduce operational drag. Align fraud prevention, customer experience, and fulfillment teams with shared metrics and an agreed-upon identity trust model.

Regularly review trust thresholds and risk tolerances across teams to ensure consistency and clarity.

[EXPLORE IDENTITY TRUST](#) →

5

Minimize manual review through transparent ML decisions. Manual reviews often stem from uncertainty around identity. Models that clearly explain why a user or transaction is risky empower teams to make more confident (and accurate) decisions faster.

Equip review teams with decision transparency that shows which identity signals contributed to the risk score.

[LINK MONEY CASE STUDY](#) →



Accelerating secure e-commerce growth starts with building identity trust across the entire customer journey. Leading businesses go beyond basic fraud thresholds by connecting behavioral, intent, and device signals in real time to block abuse early and protect high-value customers. Transparent machine learning reduces manual reviews, while aligning fraud, CX, and fulfillment teams around shared KPIs that drive both efficiency and consistency. By continuously testing and refining trust policies, companies lower fraud, improve approval rates, and unlock sustainable revenue growth.



Fraud isn't just a security issue. It's an operational, CX, and revenue issue. But it's also an opportunity to turn trust into your company's core competitive edge.

[Book a demo](#) to explore how Sift can reduce fraud and friction in your funnel.