sift

FRAUD PREVENTION TACTICAL GUIDE

Securing & Scaling Operational Efficiency

An Actionable 3-Part Guide for Ops Executives

Fraud is rarely just a hit to revenue. More often, it undermines operations—slowing fulfillment, driving up manual reviews, and triggering rigid controls that disrupt efficiency and frustrate legitimate customers.

For COOs, fraud directly impacts margins, automation, and the customer experience they're responsible for.

This guide equips operations leaders with strategies to reduce friction, synchronize cross-functional execution, and scale growth by integrating fraud prevention directly into core business operations.

sift

PART 1

Fraud's DOWNSTREAM IMPACT on Operational KPIs

Beyond exposing companies to exponential risk, fraud undermines the accuracy of key metrics COOs depend on for efficiency, scalability, and customer satisfaction.

Calculating Risk Through Operational KPIs

METRIC	POTENTIAL RISK	NEGATIVE KPI IMPACT
Operational Efficiency	High manual review volumes and reactive controls.	Increased headcount costs, slower order flow, and strained operations.
Profitability & Margins	Chargebacks, disputes, and false declines eat into revenue.	Lower margins, higher dispute fees, wasted CAC.
Customer Experience (CX)	Friction from step-up auth or review delays.	Churn, lower NPS, and reduced repeat purchase rates.
Scalability	Fraud defenses that don’t adapt to volume or new markets.	Headcount-driven growth, inconsistent processes, and operational bottlenecks.
Visibility & Control	Siloed fraud processes and inconsistent KPIs.	Gaps in oversight, compliance risk, and difficulty measuring ROI.

Fraud prevention is an operational catalyst. When trust is embedded into workflows, businesses reduce costs, scale efficiently, and protect margins without compromising CX.

PART 2

How Risk BOTTLENECKS Efficiency

Fraud often hides within normal operational flows, disguised as volume or customer engagement. Left unchecked, it becomes an obstacle to fulfillment, creating unnecessary escalations and driving up costs.

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.

HIDDEN THREAT #1

Synthetic Accounts

Rapid increase in new user signups

What it looks like

A surge in signups that look legitimate but strain onboarding and fulfillment.

Why it hurts

Inflates acquisition numbers, leads to downstream chargebacks, and creates wasted operational effort.

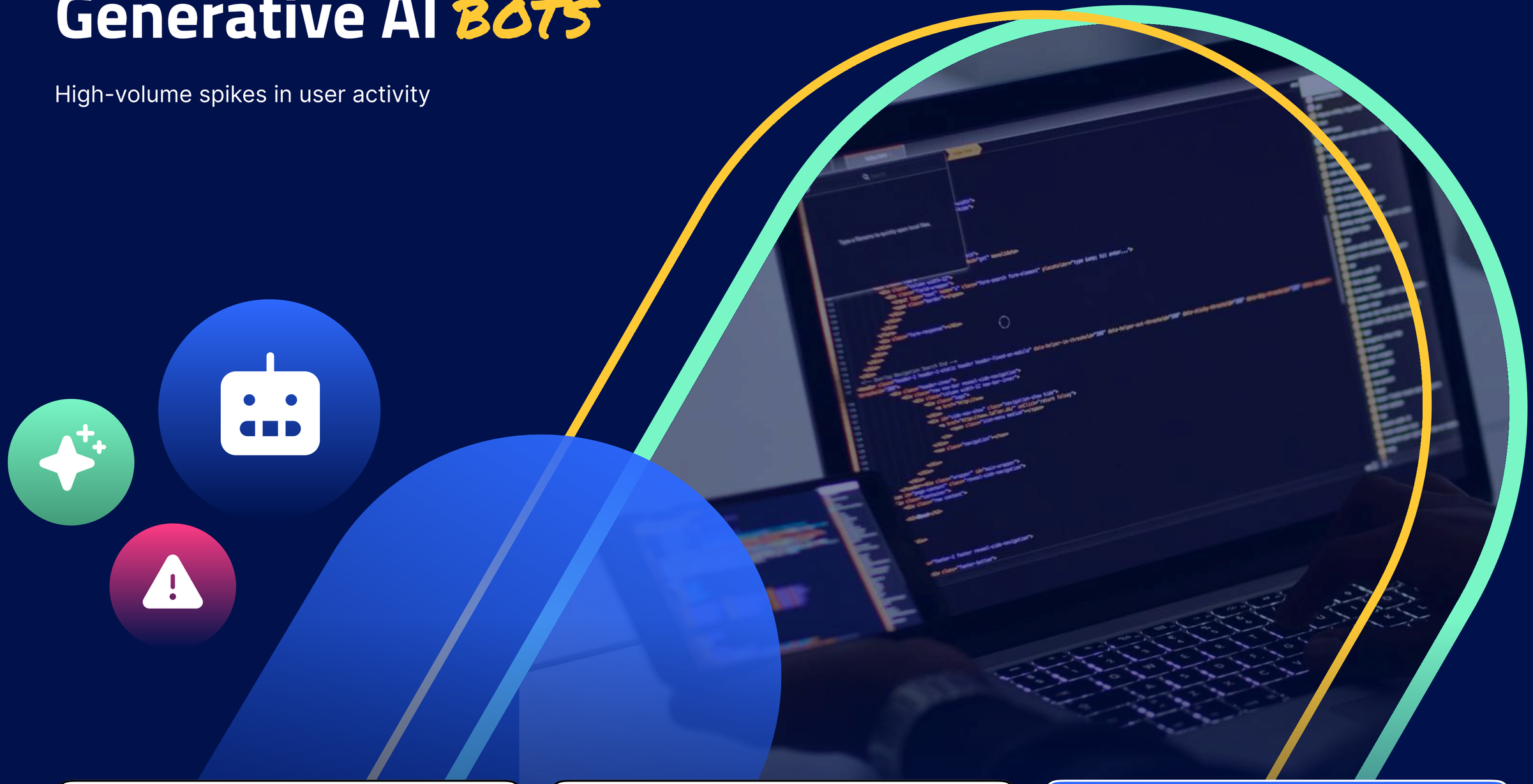
What to do

Detect synthetic identities by linking behaviors across accounts, devices, and sessions, removing friction for trusted customers.

HIDDEN THREAT #2

Generative AI BOTS

High-volume spikes in user activity



What it looks like

Activity patterns that mimic authentic users, overwhelming systems with high-volume traffic.

Why it hurts

Overloads review queues, consumes operational capacity, and forces broad safeguards that slow fulfillment.

What to do

Use behavioral analytics and ML tuned to human patterns to detect bots without blocking real customers.

HIDDEN THREAT #3

Incentive ABUSE

Significant, sustained engagement in loyalty programs

What it looks like

“Power users” maxing out promos, referrals, or returns.

Why it hurts

Forces operations teams to enforce stricter policies, hurting genuine customers while increasing costs.

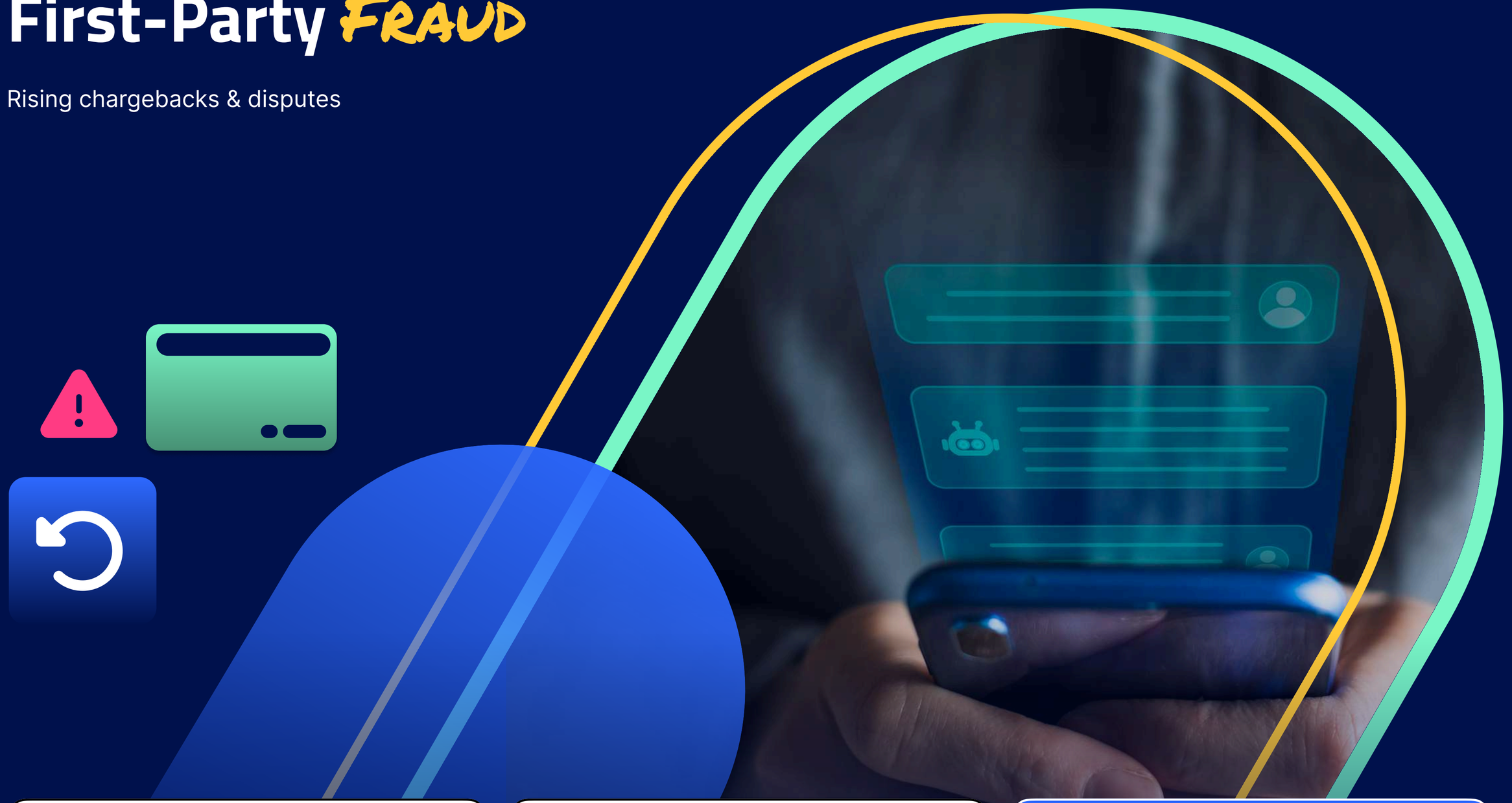
What to do

Segment true loyalty from abuse with real-time identity signals and policy-abuse detection.

HIDDEN THREAT #4

First-Party *Fraud*

Rising chargebacks & disputes



What it looks like

Healthy transaction volumes followed by a rise in disputes and reversals.

Why it hurts

Adds reconciliation work, dispute fees, and escalations that drain operational budgets.

What to do

Apply pre-auth risk scoring, and link disputes back into ML models to reduce future chargebacks.

PART 3

Actioning Identity Trust: 5 STRATEGIES for Operational Excellence

For COOs, success means scaling efficiently, managing operational costs, protecting margins, and assuring a positive customer experience. Identity Trust transforms fraud prevention from a cost center into a key catalyst of operational efficiency.

1

Automate pre-auth decisioning to reduce manual load. Resource-heavy manual reviews and late fraud checks slow operations. Embedding trust earlier streamlines effort and protects approvals.

Real-time pre-auth decisioning reduced false positives by up to 80%, cutting review queues and improving order flow.

TUTORY CASE STUDY

2

Use real-time identity signals across the customer lifecycle. Siloed fraud decisions fracture operations. Connecting identity signals across login, checkout, and post-purchase eliminates duplicate reviews and unnecessary escalations.

Cross-device and session analysis helped uncover sleeper accounts and synthetic identities at scale, streamlining operations.

TAPTAP SEND CASE STUDY

3

Minimize manual review with transparent ML decisions. Opaque rules bog down operations with unnecessary interventions. Transparent machine learning enables teams to move faster and act with confidence.

Transparent decisioning reduced manual review and provided operations clear visibility into risk signals.

ATOM TICKETS CASE STUDY

4 **Align fraud, CX, and operations with shared KPIs.** Mismatched definitions of success create friction and rework. Shared trust metrics directly align fraud prevention with operational performance.

Unified KPIs aligned fraud and ops teams, improving efficiency and consistency across the customer journey.

LINK MONEY CASE STUDY

5 **Scale globally without adding headcount.** Expansion into new markets or payment types often creates operational bottlenecks. Identity trust enables scalable automation instead of headcount growth.

Real-time ML powered global expansion while preserving operational efficiency and CX.

EXPLORE IDENTITY TRUST

sift

Fraud has evolved beyond straightforward security challenge to board-level issue, impacting both operational efficiency and scalability. Every manual review, false decline, and chargeback introduces friction that slows growth, inflates costs, and hurts margins.

Reactive risk mitigation forces teams to scale through headcount and controls. Integrating fraud decisioning into operations gives leaders the opportunity to turn trust into a core activator of scalable efficiency, profitability, and customer loyalty.

Book a demo to discover how Sift accelerates operations and turns risk into a competitive advantage.