FRAUD PREVENTION TACTICAL GUIDE

Building Seamless, Secure Product Experiences

An Actionable 3-Part Guide for CPOs

Fraud doesn't always introduce itself with a spike in chargebacks or flagged transactions. Instead, it quietly degrades the product experience, injecting friction at sign-up, breaking trust at login, and falsely inflating growth metrics.

And when fraud is treated as a back-office issue, the product pays the price through blocked conversions, broken customer journeys, and delayed feature delivery.

With actionable insights for digital commerce CPOs and product leaders, this guide explores how fraud prevention is both a UX imperative and a product growth enabler. It outlines key strategies for embedding trust, minimizing friction, and driving sustainable scale through smarter, real-time risk decisioning.

PART 1

Tracking Risk: Fraud's *Downstream Impact* on Product KPIs

Beyond causing revenue loss, fraud distorts the very metrics product teams rely on to measure adoption, retention, and satisfaction. Left unchecked, these misrepresented metrics can send product roadmaps in the wrong direction, mask friction in user journeys, and undermine confidence in new launches.

By examining how fraud impacts core KPIs, CPOs can separate true customer behavior from abuse, ensuring that decisions are based on clean, reliable product data.

Calculating Risk Through Product KPIs

METRIC	POTENTIAL RISK	NEGATIVE KPI IMPACT
Customer Satisfaction (NPS)	Poorly-tuned defenses create churn and negative reviews.	Increased churn, negative reviews, and erosion of trust in the product experience.
False-Positive Rate	Legitimate users declined during sign-up, login, or checkout waste CAC and interrupt product adoption.	Wasted CAC, reduced adoption, and distorted signals around product-market fit.
Conversion Rate	Unnecessary step-up authentication and manual reviews inflate cart abandonment.	Higher cart abandonment, lower approval rates, and lost revenue at checkout.
Manual Review Load	High review volume is a signal of poor product integration with risk systems.	Slower time-to-fulfillment, delayed user journeys, and added operational costs.
Chargeback Rate	Revenue leakage from missed ATOs, disputes, or promo abuse erodes confidence in new launches.	Revenue leakage, processor penalties, and reduced confidence in scaling to new markets.

Build fraud prevention into your product strategy, and your KPIs will reflect true customer behavior—not artifacts of digital fraud.

PART 2

Surfacing Silent Threats: How Risk *Disguises Itself* in the Product Experience

For product leaders, fraud often looks like success—at least at first. As attacks grow more sophisticated, the product surface becomes equally more difficult to defend without upending the user experience.

Threat tactics increasingly mimic the very signals used to define legitimate behavior, making them harder to detect, easier to scale, and more costly to ignore.

Here's what to look for.

HIDDEN THREAT #1

Synthetic Accounts

Rapid new user signups

What it looks like

A surge in new sign-ups that resemble legitimate customers, often with real-seeming data and plausible behavior.

Why it hurts

Inflates acquisition metrics, wastes CAC, and corrupts growth reporting. Accounts eventually monetize through promo abuse, ATO, or chargebacks, making it harder to trust adoption signals.

What to do

✓ Surface synthetic identities early by linking behavior across devices, geos, and login patterns. Use cross-network machine learning to spot subtle signals that static rules miss.

HIDDEN THREAT #2

GenAI BOTS

Engaged & repeat customers

What it looks like

- Engagement patterns that mimic authentic user behavior, from realistic typing speeds to browsing habits and device fingerprints.

Why it hurts

- Degrades UX, overwhelms systems, and erodes trust by exploiting product features. Legitimate users face stricter safeguards as a result, while bots distort product engagement metrics.

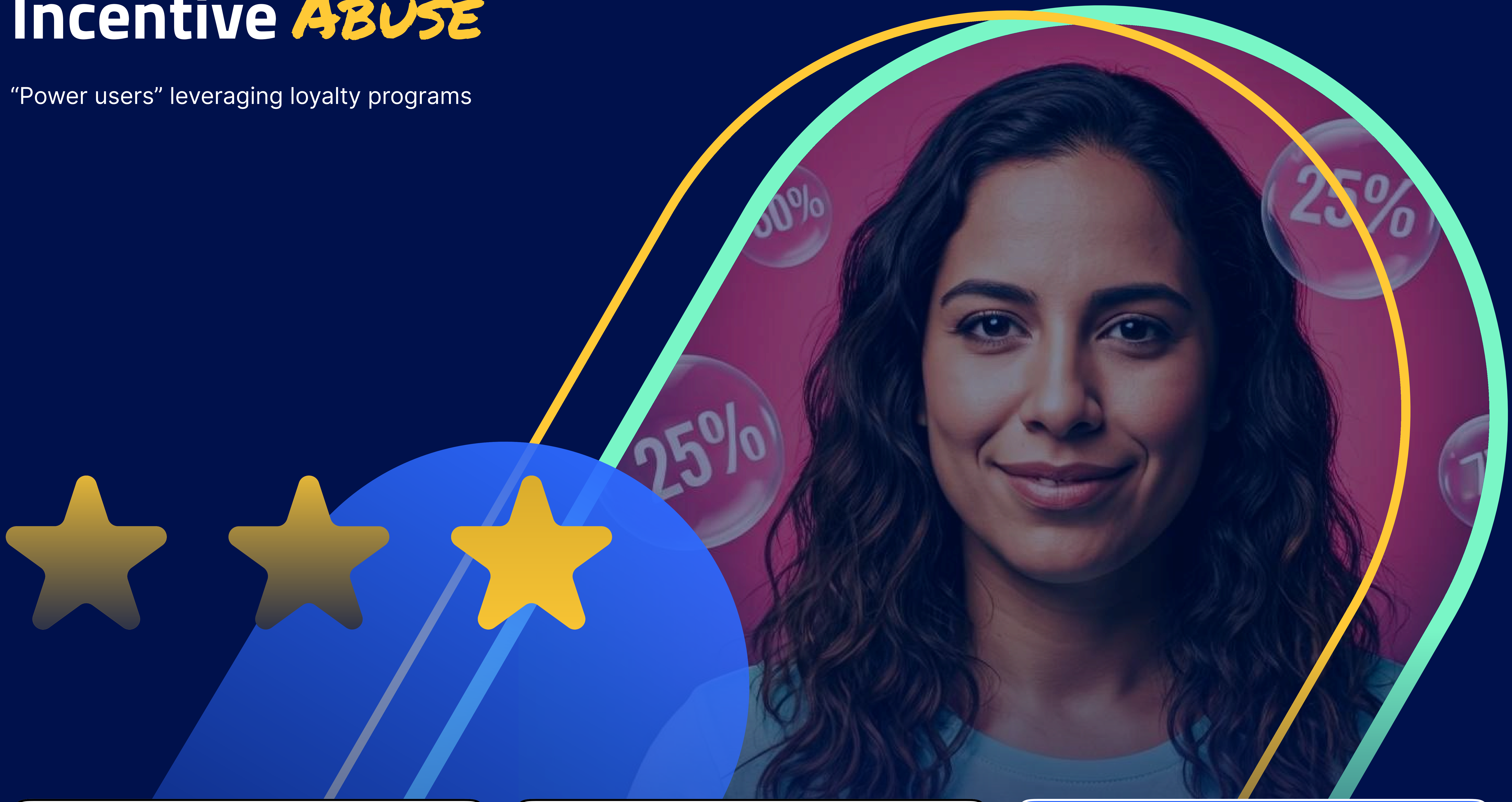
What to do

- ✓ Deploy behavioral detection tuned to human patterns, not just static rules. Identify inconsistencies in decision velocity, journey flow, and session behavior with real-time ML.

HIDDEN THREAT #3

Incentive *Abuse*

“Power users” leveraging loyalty programs



What it looks like

Customers who repeatedly max out referral programs, discounts, or loyalty rewards, appearing highly engaged and high-LTV.

Why it hurts

Forces stricter policies that frustrate real customers, undermines genuine retention, and inflates what look like positive engagement signals.

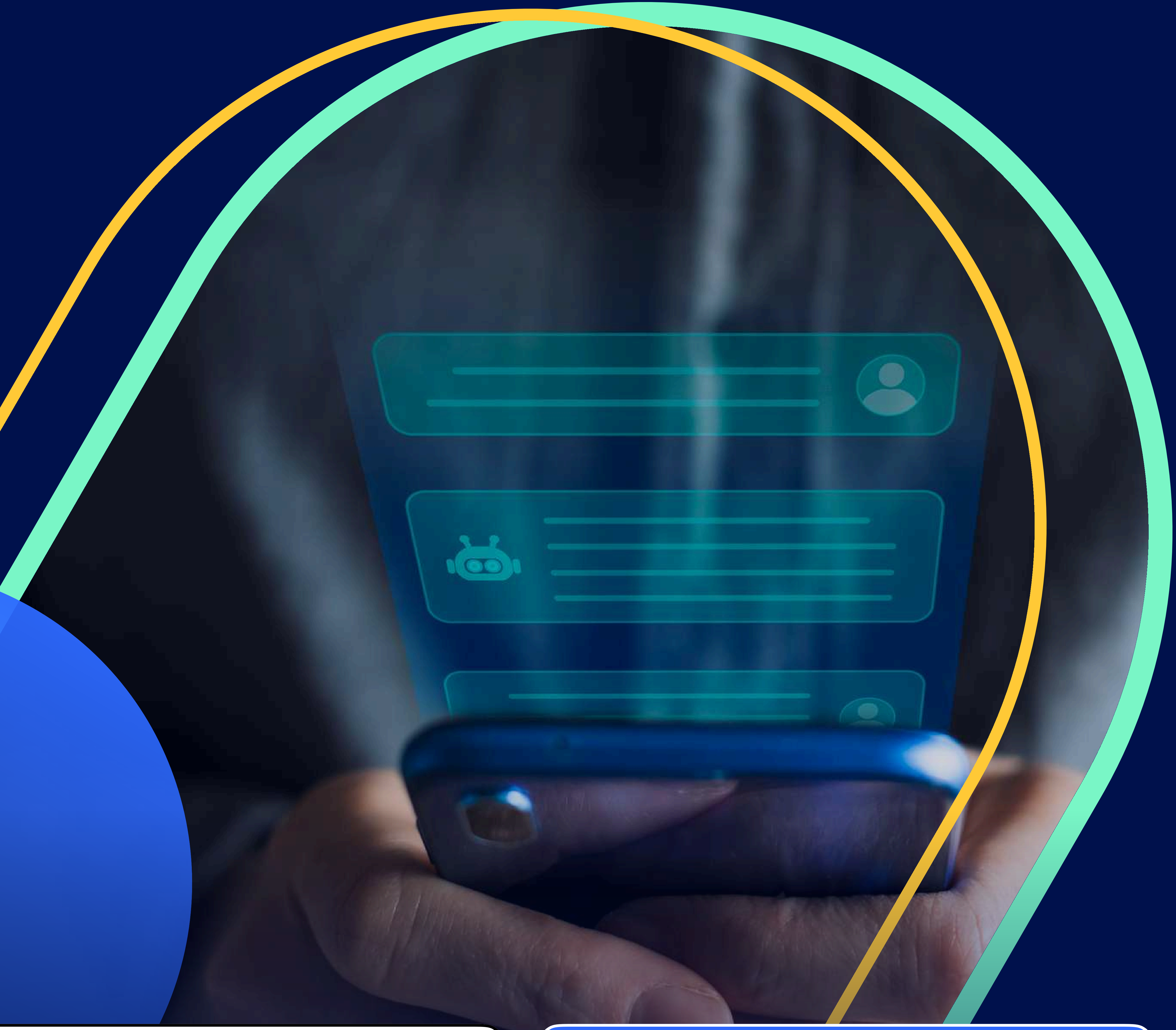
What to do

✓ Segment true loyalty from abuse using real-time behavioral modeling and identity-linking across accounts.

HIDDEN THREAT #4

First-Party *Fraud*

High-LTV users frequently requesting refunds



What it looks like

- New customers who convert quickly and appear valuable, only to later dispute charges or repeatedly file refund/return claims.

Why it hurts

- Creates revenue leakage, inflates conversion metrics, and drives negative customer experience as stricter rules are applied across the board.

What to do

✓ Score risk at account creation, not just checkout. Leverage device intelligence and IP velocity, and link behaviors across accounts/ sessions to identify coordinated refund abuse.

PART 3

Actioning Identity Trust: 5 STRATEGIES for Product-Centric Growth

Optimize the product experience and accelerate launches, all without delaying time-to-market or introducing friction throughout the customer journey.

1

Move trust upstream to stop fraud earlier. Delaying risk checks until checkout increases false declines and slows conversion. Scoring users earlier—at signup, login, or loyalty access—catches abuse before it spreads and protects high-value customers from unnecessary friction.

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

TUTORY CASE STUDY

2

Embed modular, API-driven fraud logic. Hard-coded rules slow launches and create UX friction. Modular APIs and plug-and-play integrations let product teams secure new features, payment types, and markets.

TapTap Send used cross-device and account linking to expand securely into new markets without exposing fraud gaps.

TAPTAP SEND CASE STUDY

3

Balance risk with UX. Unnecessary step-up authentication frustrates customers and lowers adoption. Adaptive decisioning approves low-risk users in real time while escalating only the riskiest behaviors.

Atom Tickets improved conversion by using transparent ML decisions that minimized false positives while keeping checkout seamless.

ATOM TICKETS CASE STUDY

4 **Design trust-centric user journeys.** When product, fraud, and CX teams define "trusted users" differently, inconsistency creeps into the entire experience. Shared KPIs and trust models align flows to protect conversions and reduce risk simultaneously.

Link Money leveraged real-time identity signals to align product and risk workflows, protecting new launches while keeping UX consistent.

LINK MONEY CASE STUDY →

5 **Support expansion without exposing gaps.** New features, payment methods, and geographies open doors for growth—and new fraud vectors. Linking identity across sessions and networks allows for early detection of synthetic accounts, promo abuse, and coordinated attacks.

Sift's Identity Trust XD connects intent, behavior, and device intelligence in real time to protect new markets at scale.

EXPLORE IDENTITY TRUST →

Digital risk has evolved from a standard security problem into a direct challenge for product innovation and growth. For CPOs, the priority isn't just stopping abuse, but safeguarding the integrity of product signals, preserving frictionless customer journeys, and ensuring that launches aren't derailed by hidden fraud.

Reactive fraud prevention erodes adoption, distorts KPIs, and weakens user trust. Building risk mitigation into the product experience creates an opportunity to turn trust into your company’s core competitive edge—accelerating launches, enabling global expansion, and driving long-lasting customer loyalty.

Book a demo to explore how Sift can reduce fraud and friction in your product and go-to-market processes.