sift

Get the Fraud Out: A Checklist for Fraud & Risk Teams

Fraud doesn't wait. It evolves, scales, and adapts to find the path of least resistance. Getting the fraud out isn't a one-time fix. It's an ongoing commitment to smarter detection, faster decisions, and full-journey coverage that keeps trusted users moving while blocking bad actors at every stage.

Use this checklist to evaluate where you stand, and where fraud still has the upper hand.

1 | Know What You're Up Against

Fraud teams can't fight what they can't see. Start by mapping your exposure across attack types and customer touchpoints.

- ❒ **Audit your full attack surface:** Identify every entry point where fraud can occur: account creation, login, checkout, payments, stored value, refunds, and payouts.
- ❒ **Understand your most common attack types:** Know whether your top threats are account takeover (ATO), payment fraud, promo abuse, bot activity, credential stuffing, card testing, or multi-accounting.
- ❒ **Track how fraud patterns are evolving:** Review historical attack data alongside emerging trends from industry benchmarks and peer networks.
- ❒ **Map friction to risk, not to assumption:** Confirm that every checkpoint across your customer journey is backed by real risk signals.
- ❒ **Quantify the cost of fraud beyond chargebacks:** Account for false positives, manual review costs, customer churn from over-friction, and revenue lost to declined legitimate transactions.

2 | Stop Fraud Earlier in the Journey

The earlier you detect fraud, the less damage it can do. Upstream signals reduce downstream exposure.

- ❒ **Protect account creation, not just checkout:** Detect synthetic identities and bot-driven registrations at the front door.
- ❒ **Score every login event in real time:** Surface account takeover attempts before attackers can act on compromised credentials.
- ❒ **Use behavioral, device, and network intelligence:** Layer signals across device fingerprinting, IP reputation, velocity patterns, and behavioral anomalies to catch threats that rules alone miss.
- ❒ **Leverage consortium data to recognize known bad actors:** Network-level intelligence extends your detection to fraud patterns your own data has never seen.
- ❒ **Make fraud decisions in milliseconds:** Target sub-150ms decision latency at scale so trusted users never feel the friction of your fraud controls.

Get the Fraud Out: A *Checklist* for Fraud & Risk Teams

3 | Keep Trusted Customers Moving

Getting the fraud out doesn't mean slowing everyone down. Risk-based friction is the difference between blocking bad actors and losing real customers.

- ❒ **Apply step-up authentication only when risk warrants it:** Trigger additional authentication based on suspicious signals, not blanket policies.
- ❒ **Minimize manual review as a default response:** Automate routine decisions so analysts can focus on complex, high-value cases.
- ❒ **Measure and reduce false positive rates:** Blocking trusted users is a cost, not a safety margin. Track false positive rates alongside fraud block rates.
- ❒ **Optimize approval rates without increasing fraud exposure:** Find the right balance between revenue capture and risk. Both metrics should be actively managed.
- ❒ **Maintain consistent experiences at scale during peak events:** Decisioning should remain fast and accurate under load, without forcing a tradeoff between fraud protection and customer experience.

4 | Build Operational Resilience

Fraud teams are only as effective as their tools, processes, and visibility. Operational gaps become attacker opportunities.

- ❒ **Give analysts clear, actionable risk signals:** Consolidate device, behavioral, and transaction signals so investigators spend time on decisions, not data gathering.
- ❒ **Enable policy changes without engineering dependencies:** Teams that need a deploy cycle to update thresholds or workflows will always be behind the curve.
- ❒ **Define escalation paths before incidents happen:** Know who owns critical fraud decisions, when controls should tighten or relax, and how cross-functional teams coordinate under pressure.
- ❒ **Monitor performance metrics in real time:** Track approval rates, block rates, manual review queue depth, authentication challenge rates, and velocity anomalies continuously.
- ❒ **Have access to fraud expertise when you need it:** Access to industry experts who have seen similar attacks across hundreds of businesses accelerates response to novel attack patterns.

5 | Make Every Signal Work Harder

Fragmented tools mean fragmented signals. A connected platform turns data into decisions, not noise.

- ❒ **Unify payments fraud, account defense, and abuse prevention:** A single platform with a shared user view catches coordinated attacks that cross product boundaries.
- ❒ **Connect account signals to payment signals:** An account flagged for suspicious login behavior is also a payment risk. Cross-product signal sharing improves decision accuracy across the board.
- ❒ **Use ML models trained on network-scale data:** Models trained across trillions of events recognize patterns your own transaction data cannot.
- ❒ **Reduce tool sprawl and integration complexity:** Every additional vendor is an integration burden and a data gap. Consolidation reduces operational overhead and improves signal fidelity.
- ❒ **Continuously improve fraud strategy with outcome data:** Use outcome feedback loops to sharpen model accuracy and policy effectiveness over time.

Ready to GTFO?
See how Sift helps you get the fraud out

REQUEST A DEMO

sift