spec

HOW TO STOP BAN EVASION

www.specprotected.com

HOW TO STOP BAN EVASION

spec

Bans Don't Fail — Detection Strategies Do

You banned them. And yet... they're back. This guide isn't about awareness. It's about fixing a known failure point. Ban evasion isn't a rare edge case. It's the default playbook for repeat abusers, fraudsters, and policy violators.

What needs to change? Not stricter rules or heavier friction, but better memory.

Shift Your Strategy

Stop relying on what users present. Start recognizing how they behave, and when it looks familiar.

Why Static Signals Lose

Most teams have likely tried static signals:

- Blocking IPs, emails, or device IDs
- Adding friction with CAPTCHA
- Tuning signup flows tighter and tighter

These signals can be reset, spoofed, or cycled. You can't win the fraud arms race by playing their game.

What Repeat Abuse Actually Looks Like

Ban evasion often hides in plain sight. The attacker changes the identity. The pattern stays the same. It's not about catching a user. It's about spotting the loop they run over and over again.

Familiar journey sequences

Chargeback or promo cycling

Dormant accounts reactivated

Cross-account behavior overlap

HOW TO STOP BAN EVASION

spec

Step 1: Turn Every Ban Into a Signal

Most teams treat bans as the finish line for fraud. But they're actually a starting point.

Log the full behavior trail leading up to the ban

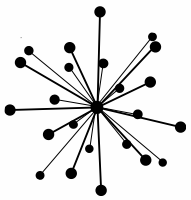
Feed behavioral signals into your detection logic

Use them to flag lookalikes in real time

Banned User Logs

- ✓ Session flow
- ✓ Navigation events
- ✓ Interaction timing
- ✓ Device and browser characteristics
- ✓ Actions taken (e.g., signups, checkouts, promos used)
- ✓ Referrers and traffic sources

Step 2: Link Behavior Across Sessions and Accounts



Fraud doesn't start from scratch. It repeats familiar motions.
Behavioral linking means identifying when two or more sessions follow the same path, regardless of the credentials attached. How to do it:

Track full user flows across different IDs

Assign behavior scores based on journey similarity

Flag high-risk flows that match previously banned sequences

HOW TO STOP BAN EVASION

spec

Step 3: Detect Abuse Before the Account Exists

Ban evasion often begins before signup. You can catch it by analyzing:

- User journey anomalies during the signup process
- Automation-style flows with irregular speed, repetition, etc
- Behavior that is similar to prior abusers and offenders

Pro Tip:

Pre-account behavior is one of your richest underutilized signals. Don't wait until the login wall to start detecting abuse.

Step 4: Catch Account Takeovers As a Ban Evasion Tactic

When creating new accounts gets too risky, attackers get clever. They hijack old ones. These "trusted" accounts slip through basic filters, unless you compare their current behavior to historical norms.

- Measure flow, speed, and intent against the account's baseline
- Flag sharp deviations: faster checkouts, different promo use, unusual geolocation or timing

Signs of ATO Evasion

- ✕ Sudden account reactivation after long dormancy
- ✕ New behavior that doesn't match user history
- ✕ Logins from unknown devices or traffic sources

HOW TO STOP BAN EVASION

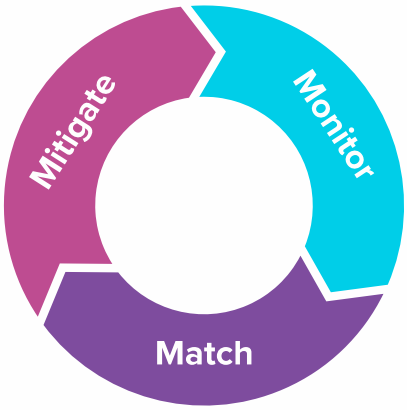
spec

Step 5: Operationalize Memory-First Detection System

Stopping ban evasion takes more than rules. It takes structure. Use the 3M model to guide your detection system.

- **Monitor:** Track user journeys across accounts, devices and sessions.
- **Match:** Link behavioral patterns, even when identifiers change.
- **Mitigate:** Disrupt abuse flows in real time, before damage is done.

The 3M Model



Implementation Tips

Team Ownership
Fraud owns strategy. Data owns signal logic. Platform owns deployment.

Model Tuning
Continuously retrain models based on newly flagged behavior.

Mitigation
Decide when to block, when to redirect, and when to trigger manual review.

Is Your Team Built to Stop Ban Evasion?

- ✓ Are you linking behavior across multiple identities?
- ✓ Do bans inform future detection logic?
- ✓ Can you detect repeat abuse before signup?
- ✓ Are you surfacing ATOs via behavior baselines?
- ✓ Are you making decisions on context, not credentials?

HOW TO STOP BAN EVASION

Don’t Ban the User. End the Pattern.

Ban evasion isn’t a user problem. It’s a pattern problem. You don’t need heavier friction to stop it. You need stronger memory.

With Spec, your team can identify abuse at the behavioral level, before it escalates.

Want to see what repeat abuse looks like on your platform?
➔ **Get a behavior-level fraud analysis with Spec.**

GET YOUR BEHAVIOR-LEVEL ANALYSIS