A

Ad Fraud and Invalid Traffic: Detection, Investigation, and Prevention

Ad fraud deliberately manipulates advertising events for gain. Invalid traffic is broader and can include bots, accidental clicks, duplicate events, and measurement errors.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Ad fraud deliberately creates, redirects, misrepresents, or attributes advertising activity for financial or competitive gain. **Invalid traffic (IVT)** is broader: it includes fraudulent activity but can also include accidental clicks, duplicate measurements, crawlers, testing, and other events that should not be billed or counted as genuine engagement.

Google likewise defines invalid traffic as clicks or impressions that may artificially inflate advertiser costs or publisher earnings. Calling every anomaly “fraud” before establishing intent can lead to incorrect blocking and contractual disputes.

Common ad-fraud patterns

- **Bot and click-farm traffic:** automated or coordinated activity creates impressions, clicks, installs, or conversions.

- **Domain or app spoofing:** inventory is represented as coming from a different, more valuable publisher.
- **Ad stacking and hidden placements:** multiple or invisible ads register views the user never saw.
- **Ad injection:** malware, extensions, or network software inserts or replaces advertising without publisher approval.
- **Click injection and attribution abuse:** a party claims credit for an install or conversion caused elsewhere.
- **Conversion and lead fraud:** false purchases, accounts, forms, calls, or events create commissions or poison optimization.

Patterns that warrant investigation

- traffic, click-through rate, or conversion volume changes sharply without a matching campaign or business event;
- one placement, app, partner, geography, device, or hour produces implausibly uniform behavior;
- high clicks or installs produce little authenticated use, retention, revenue, or downstream engagement;
- events repeat with impossible timing, device combinations, user-agent properties, or conversion order;
- publisher and advertiser logs disagree about impressions, click IDs, landing pages, or timestamps;
- refunds, chargebacks, fake leads, or account abuse concentrate in the same acquisition source.

No single metric proves fraud. Shared IPs, privacy systems, corporate gateways, accessibility tools, software releases, and measurement bugs can resemble malicious traffic.

Investigation workflow

1. **Define the affected event.** Separate impressions, clicks, video views, installs, leads, conversions, and revenue.
2. **Locate the change.** Segment by campaign, creative, placement, publisher, partner, geography, device, browser, app version, and time.
3. **Compare independent stages.** Reconcile ad-platform events with CDN, server, application, authentication, payment, and CRM records.
4. **Preserve evidence.** Keep campaign and placement IDs, click or impression IDs, timestamps and time zone, referrer, user agent, consented device signals, request logs, invoices, and configuration history.
5. **Check benign causes.** Review tagging releases, redirects, retry logic, server-side event duplication, internal testing, and partner changes.
6. **Contain proportionately.** Pause or cap the narrow source when loss continues, while preserving enough traffic and records to validate the hypothesis.

Controls for advertisers and publishers

- use placement and partner transparency, allowlists where appropriate, and supply-chain standards supported by the platform;
- optimize toward validated business outcomes rather than clicks alone;
- protect ad, analytics, affiliate, and payment accounts with MFA and least privilege;
- sign and validate server-to-server events, rotate secrets, and prevent replay and duplicate processing;
- monitor changes in tags, redirects, creative, domains, application packages, and traffic acquisition;
- define evidence, refund, retention, and investigation duties in partner contracts.

Report a documented pattern through the relevant platform or partner process. Avoid publishing personal data or accusing a party publicly before validation. Measure blocked costs, recovered spend, false positives, downstream quality, and recurrence—not merely the number of events a tool labels invalid.

Reference: Google Ad Manager: Invalid traffic.

Ad fraud FAQ

Are two clicks from one IP fraud?

No. Many users can share an address, and retries happen. Correlate multiple signals and downstream behavior.

Should every suspicious source be blocked immediately?

Contain active loss, but use the narrowest reversible control and preserve evidence so legitimate traffic is not permanently excluded without cause.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com