cleartrust

Global Ad Fraud Report 25-26

This report reflects patterns observed within the traffic ClearTrust analysed through 2025 and does not represent the entire digital advertising landscape or ecosystem.

We read invalid traffic like no one else. 2025 was a watershed year for digital advertising, from the highly publicised Meta ads fraud fiasco covered by Reuters, to the quiet but massive surge in Lead Generation abuse. While the industry focused on high-level trends, ClearTrust dug deeper. We didn't just look at the surface; we analysed the DNA of the traffic. This report isn't just about problems, it's about the **46 billion signals** we analysed to find the truth.

cleartrust

2025 PERFORMANCE

ClearTrust by the Numbers

46.11B

Total Scans Conducted

Every single request fingerprinted and evaluated in real time.

11.78B

Invalid Traffic Detected

Confirmed IVT removed from advertiser budgets before damage was done.

67

New Fraud Traps Deployed

More than one new defence mechanism every single week of the year.

In 2025, the fraud landscape moved faster than ever. In response, the ClearTrust team deployed 67 distinct new fraud traps, counter-measures against evolving threats such as sophisticated scraping, device emulation, and AI-powered behavioural mimicry. Agility wasn't optional; it was the only viable defence.

KEY FINDINGS

The Scale of the Issue

Out of **46,109,313,988** total scans conducted in 2025, ClearTrust uncovered that nearly **25% of all traffic** analysed contained some form of measurable risk, a figure that should alarm every digital advertiser.

High Risk (Confirmed Fraud)

4.71 Billion - 10.2% of total scans. Definitively classified fraudulent activity.

Medium Risk

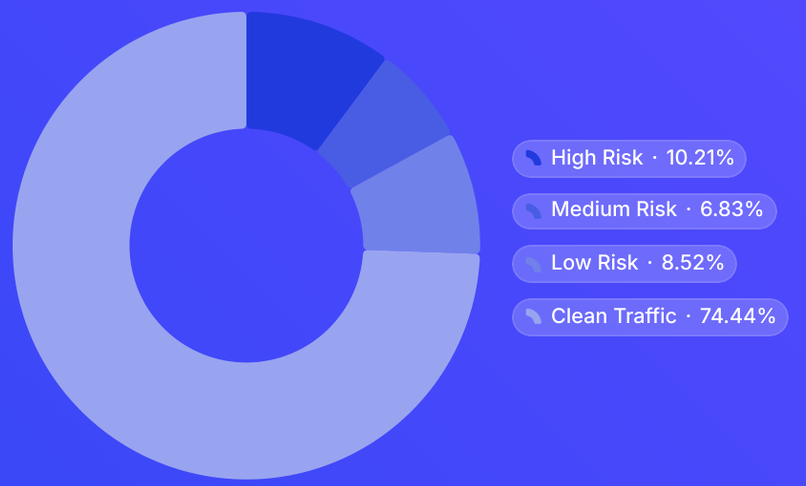
3.15 Billion — 6.8% of total scans. Anomalous signals requiring elevated scrutiny.

Low Risk

3.93 Billion — 8.5% of total scans. Suspicious patterns below confirmed fraud threshold.

Clean Traffic

34.33 Billion verified legitimate impressions and interactions.



2026 Prediction: Based on the surge in "Medium Risk" anomalies and the explosion of AI-generated content, ClearTrust projects that Human-Mimicry Fraud will overtake basic bot attacks by Q3 2026.

GLOBAL IMPACT

Fraud Has a Geography

Fraud isn't uniform it is cultural and infrastructure-dependent. In 2025, distinct **"fraud personalities"** emerged by region, shaped by advertising maturity, mobile penetration, and social media behaviour.

🇺🇸 United States

A dominant location for programmatic and browser-based ad fraud. Its mature ecosystem correlates with sophisticated, infrastructure-driven automation.

🇬🇧 United Kingdom

A notable focus on mobile-first ad fraud. High smartphone penetration correlates with prevalent device emulation attacks.

🇸🇪 Sweden

Social platform fraud (Meta/TikTok) is the primary concern, driven by elevated social media usage and engagement farms.

🇩🇪 Germany

Fraud is predominantly infrastructure and programmaticm highly automated, systematic, and efficient in nature.

🇮🇳 India

Mirroring US trends, ad fraud here involves large-scale automated traffic abuse rather than individual device compromise.

cleartrust

METHODOLOGY

Pulling Back the Curtain

How Our Detection Engine Works

ClearTrust operates a **multi-layered detection approach**. In 2025, we moved decisively beyond simple blocklists, introducing **Human Metrics Detection**, a methodology that analyses behavioural indicators to identify bots that act like people.

> "Transparency isn't a feature; it's the product. In 2025, we didn't just block traffic, we enriched IP data to attribution levels previously unseen, distinguishing between residential proxies and cloud-originated bots."
>
> **— Deepankar Biswas, CEO, ClearTrust**

Signal Ingestion

Every scan fingerprinted across 46+ behavioural and technical dimensions.

IP Enrichment

Residential proxies distinguished from cloud-originated automated traffic.

Behavioural Scoring

Human Metrics Detection flags anomalies invisible to signature-based tools.

Trap Deployment

67 new traps activated in 2025 to capture emerging fraud vectors.

cleartrust

MARKET CONTEXT

Digital Ad Spend: A Growing Target

As global digital ad spend reaches record highs across Meta, TikTok, and programmatic channels, the financial incentive for fraud scales linearly. More budget flowing into unmonitored channels particularly Lead Generation directly equates to higher ROI for fraudsters.

The Multiplier Effect

Every dollar of unprotected ad spend in Lead Gen and Affiliate channels creates a disproportionate return for bad actors operating at scale.

Unmonitored Channels

Standard programmatic fraud tools leave Lead Gen entirely unprotected the fastest-growing attack surface in the ecosystem.

Platform Risk

Meta, TikTok, and open-web programmatic each carry distinct fraud profiles requiring channel-specific detection logic.

cleartrust

FRAUD PATTERNS OVER TIME

The Seasonal Pulse of Fraud

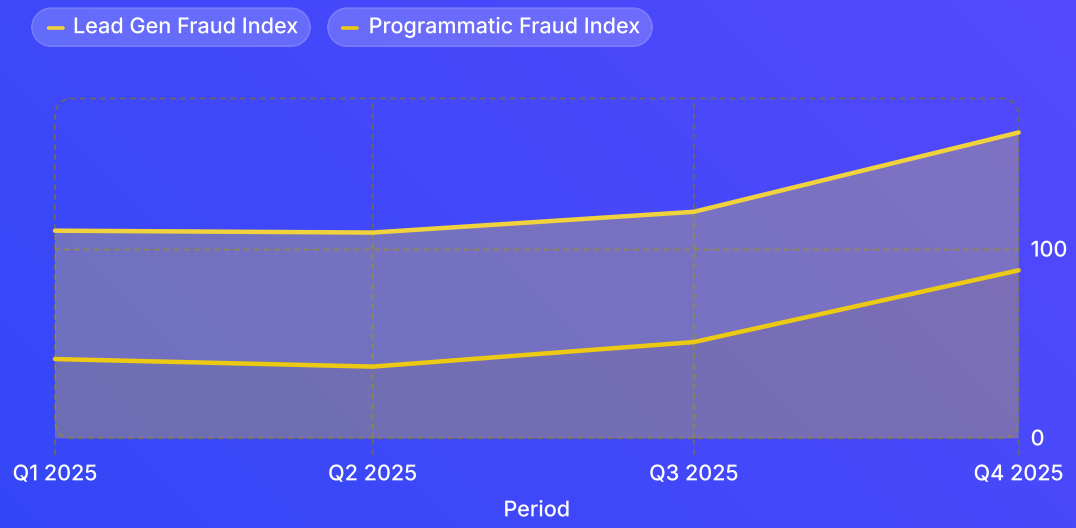
Fraud is not static. Throughout 2025, ClearTrust observed distinct temporal patterns that reveal the strategic behaviour of fraudsters as they align attacks with advertiser spending cycles.

Q4 Programmatic Spike

Programmatic fraud peaked sharply in Q4, aligning precisely with elevated CPMs and holiday season ad budgets. Fraudsters follow the money.

The Constant Hum

Unlike programmatic spikes, **Lead Gen fraud** remained dangerously and consistently elevated throughout the entire year — completely unaffected by seasonality. This makes it the more insidious threat.



FINANCIAL IMPACT

The Cost of Inaction Is Rising

2025 Actuals

ClearTrust detected **11.78 Billion** invalid hits within its analysed traffic alone. Referencing industry baselines — Anura's estimate of **$140 billion** in global ad fraud losses for 2024 — the wasted spend across the open web is staggering and accelerating.

2026 Projections

With AI-powered fraud lowering the cost and technical barrier for bad actors, and with Lead Gen remaining the dominant attack vector, industry fraud losses are projected to climb further in 2026. Budgets that go unprotected today will cost significantly more tomorrow.

The cost of ad fraud is not just wasted impressions — it is corrupted conversion data, inflated CPAs, and strategic decisions built on a foundation of fake signals.

cleartrust

AI-DRIVEN FRAUD

GIVT vs. SIVT in the Age of LLMs

General Invalid Traffic (GIVT)

GIVT including known bots, crawlers, and data centre traffic, remains relatively straightforward to identify and filter. Standard detection tools handle it adequately.

Sophisticated Invalid Traffic (SIVT)

SIVT is being **supercharged by AI**. Fraudsters are no longer merely writing scripts, they are **training models** to browse, scroll, hover, and click with convincing human variance. These bots don't just look like humans; they are statistically engineered to pass as them.

The inflection point: When LLMs are applied to traffic generation, the gap between GIVT and SIVT collapses. The industry needs detection frameworks built for behavioural analysis, not just signature matching.

cleartrust

AI FRAUD DEFENCES

Fighting AI with Behavioural Science

Human Metrics Detection

ClearTrust is currently beta-testing **Human Metrics Detection**, a paradigm shift away from signature-based blocking towards deep behavioural analysis. We look for the **"micro-hesitations"** and imperfections that define genuine human users: the slight pause before a click, the irregular scroll velocity, the organic variance in interaction timing.

Why This Works

AI bots are trained to optimise. That optimisation is their flaw. Overly consistent behaviour too-perfect mouse paths, uniform timing intervals, absence of error, becomes the signal. What looks like competence to a human eye looks like fraud to our detection engine.

Move beyond blocklists

AI can trivially rotate signatures, IPs, and user agents.

Analyse micro-behaviours

Timing, hesitation, and interaction entropy reveal true identity.

Continuously retrain models

As fraud evolves, detection logic must evolve in parallel.

EXPERT PERSPECTIVE

The Absence of Human Randomness

> "We aren't just looking for bad actors anymore; we are looking for the **absence of human randomness**. AI bots are too perfect. That is their weakness."
>
> **— Raja TN, CTO, ClearTrust**

This insight reframes the entire discipline of fraud detection. The question is no longer *"does this traffic look suspicious?"* it is *"does this traffic look human enough?"* Perfection, in the context of user behaviour, is the red flag. ClearTrust's Human Metrics Detection framework is built on precisely this inversion of logic.

COMPETITIVE POSITIONING

Where ClearTrust Wins: The 53% Gap

The Industry Blind Spot

Most competitors in the fraud detection space have optimised their tooling for **Programmatic (RTB) fraud** impression-level protection within display and video environments. These tools are well-suited for the channels they were built to serve.

But with **53.51% of 2025's detected fraud** originating from Lead Generation and Affiliate channels, standard programmatic blockers would miss **more than half the problem entirely**.

The ClearTrust Advantage

ClearTrust is architected for **performance channel integrity** the space between impression delivery and conversion validation. We bridge the gap that programmatic-only tools cannot address.

Impression Protection

Covered by most tools in the market.

Conversion Integrity

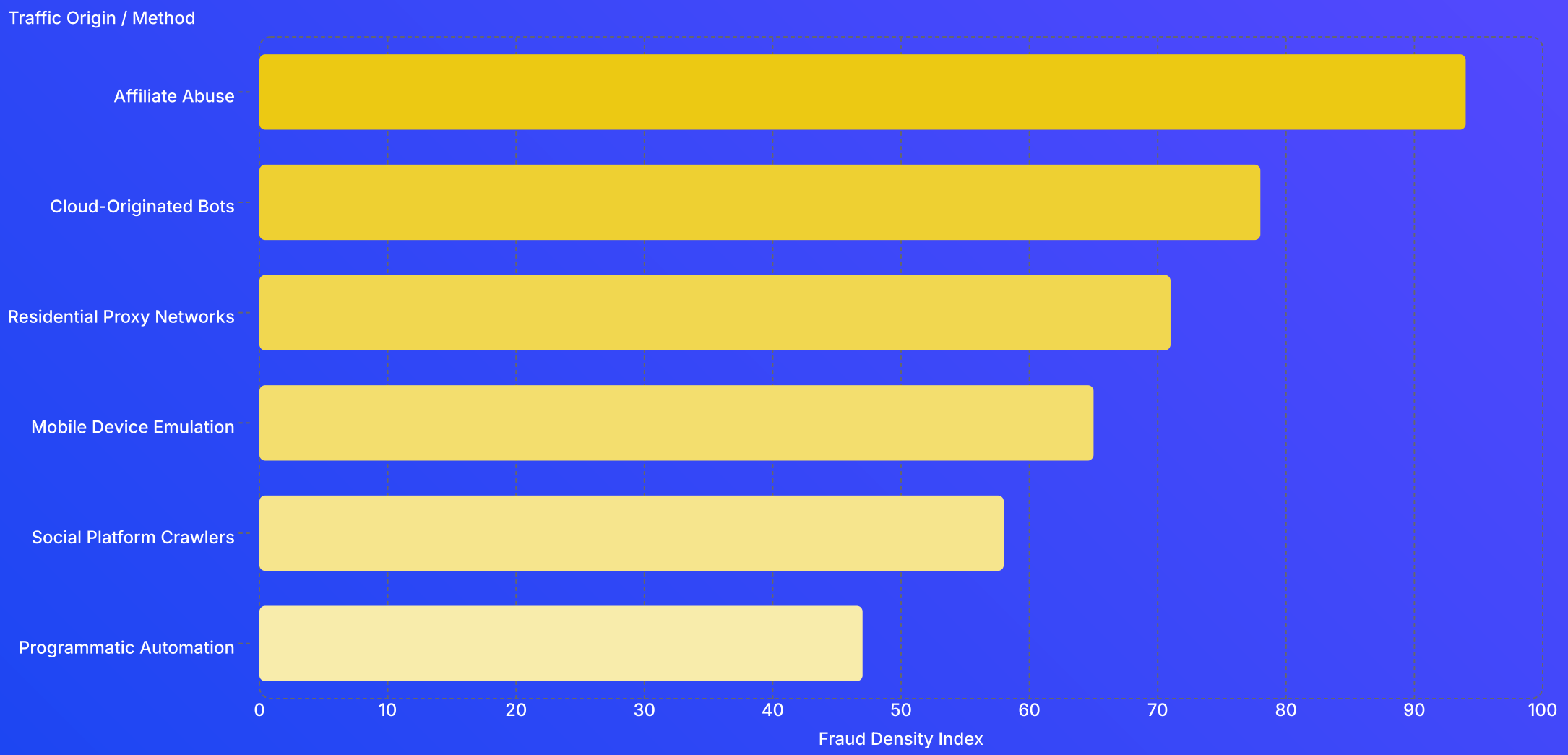
ClearTrust's core specialisation — where the majority of fraud lives.

cleartrust

TRAFFIC ORIGIN ANALYSIS

Highest-Ranked Fraud Traffic in 2025

Traffic origin analysis in 2025 revealed a clear structural divide: **residential and mobile traffic** resolved to granular regional locations, while **automated crawler and cloud-originated traffic** was attributed at the country level. The single most impactful fraud vector was not a country — it was a method.



Key insight: Affiliate Abuse was the single dominant fraud method of 2025 not attributable to one geography, but to a systematic exploitation of performance incentive structures across the open web.

COUNTRY-LEVEL INTELLIGENCE

Fraud Density Rankings by Geography

🇺🇸 USA — Rank #1

High volume, high sophistication. Programmatic automation at infrastructure scale defines the US fraud profile. Mature ad ecosystem = mature fraud ecosystem.

🇬🇧 UK — Rank #2

High mobile density fraud. Device emulation attacks exploit the UK's exceptional smartphone penetration and mobile-first advertising ecosystem.

🇸🇪 Sweden — Rank #3

High social platform crawler density. Elevated Meta and TikTok usage creates fertile ground for engagement farms and automated interaction abuse.

> "The geography of fraud tells us the motive. Germany's infrastructure fraud is about efficiency; the UK's mobile fraud is about consumer volume. We tailor our traps to the motive."
>
> **— Manish Gadhe, Business and Revenue Head, ClearTrust**

cleartrust

FRAUD CATEGORY DEEP DIVE

2025 Fraud Categories: Full Breakdown

The most significant revelation of 2025 was the **dominance of performance-based fraud** over simple impression fraud. Bad actors have moved up the funnel, targeting conversions, leads, and affiliate payouts, not just ad views.

Lead Generation & Affiliate Fraud — 53.51%

The dominant category by a wide margin. Driven by repetitive device usage and concentrated, patterned submission behaviour targeting CPA and affiliate payout structures.

Mobile Fraud — 25.09%

Approximately one quarter of all classified fraud. Emulated devices and automated mobile browsers continue to exploit mobile-first advertising environments at scale.

Meta & TikTok Fraud — 14.50%

Social-platform fraud driven primarily by automated crawler and engagement amplification activity within Meta and TikTok ecosystems.

Publisher Fraud — 6.80%

Traffic originating from controlled infrastructure and misrepresented publishing environments — often linked to MFA (Made for Advertising) site networks.

Google Ads Fraud — 0.10%

Minimal signals, primarily reflecting automated validation traffic inherent to the Google advertising ecosystem rather than targeted fraud campaigns.

Browser-Based Fraud — <0.01%

Negligible levels observed. Desktop browser automation was not a primary vector in 2025's analysed traffic, indicating a strategic shift toward mobile and server-side methods.

cleartrust

DETECTION PLAYBOOK

How to Catch Ad Fraud

Fraud is complex — but catching it shouldn't be. The principles that underpin effective detection are consistent, regardless of channel, geography, or fraud type.

Scan Everything

100% traffic coverage not sampling. Sampling leaves gaps that sophisticated fraudsters actively exploit. Every request must be evaluated.

Look for Behaviour, Not Just User Agents

Bots change headers trivially they rarely change their objective. Analyse what traffic *does*, not just what it claims to be. Intent leaves traces.

Deploy Rapid Traps

As proven by ClearTrust's 67 new traps in 2025, agility is the only sustainable defence. Static blocklists are obsolete within days of a new fraud vector emerging.

cleartrust

BUSINESS RISK

The Repercussions of Ad Fraud

Ad fraud isn't merely a budget problem. The downstream consequences extend into legal liability, brand equity, and strategic decision-making — making it a board-level concern, not just a media-buying footnote.

📊 Skewed Analytics

When fake traffic contaminates your data, you optimise campaigns based on fabricated signals. Every budget decision downstream becomes structurally flawed amplifying waste rather than eliminating it.

⚖️ TCPA Liability

Fake leads submitted through fraudulent form fills can result in serious legal exposure. Dialling non-consenting numbers generated by bots carries direct TCPA liability regardless of advertiser intent.

🏷️ Brand Reputation

Appearing on MFA (Made for Advertising) sites, a hallmark of publisher fraud directly degrades brand equity. Adjacency to low-quality, fraudulent inventory is a reputational risk with lasting effects.

The true cost of ad fraud is not the wasted impression. It is the compounding damage of every business decision made on corrupted data.

CREDIBILITY & RESOURCES

Proof, Trust, and Next Steps

ClearTrust's findings in this report are backed by 46 billion data points, industry-recognised certifications, and the operational track record of a team that deploys more than one new fraud trap every week. The numbers speak, but so do our clients.

> "**T**he results from the post-bid implementation have been so successful that we are now planning to upgrade and implement ClearTrust's pre-bid solution. It's no longer just about identifying issues, it's about optimizing our demand and scaling our business with a unified platform we can actually trust.."
>
> **— Manimaran Babu, Director of CueDart**

> "ClearTrust has been a game-changer for Limelight. Their real-time fraud detection and custom blocklists helped us reduce invalid traffic by 50%, saving us from significant revenue loss. What impressed me most was their team's deep understanding of ad tech and proactive collaboration to address our unique challenges."
>
> **— David Nelson, Co-founder & CEO, Limelight**

Request a scan now

Get in touch with us

Watch more