Ad Fraud Detection:

You can't stop what you can't see

Table of Contents

Introduction

In an ideal world, marketers would set aside a certain amount of money for their digital advertising campaigns, and all that money would be spent serving up legitimate ads to real, live human visitors.

Unfortunately, where ill-gotten gains can be made, fraudsters eventually show up.
In the world of online advertising, ad fraud is a massive problem. For example, some accounts estimate that as much as 25 percent of all paid ads are fraudulent. For the average ad campaign, fraudsters end up stealing one out of every four dollars from your budget—and stuffing that cash into their own pockets.

> **Experts forecast that this nefarious trend is set to continue growing at an exponential rate, underscoring the need for immediate, effective countermeasures.**

Ad fraud poses an already significant challenge, with a staggering $100 billion at stake and increasing relentlessly. This escalation is propelled by the rapid advancements in the digital age, the rise of influencers, loopholes in laws and penalties, and the simple lure of easy money. Experts forecast that this nefarious trend is set to continue growing at an exponential rate, underscoring the need for immediate, effective countermeasures.

What is Ad Fraud?

In an ideal world, marketers would set aside a certain amount of money for their digital advertising campaigns, and all that money would be spent serving up legitimate ads to real, live human visitors.

Unfortunately, where ill-gotten gains can be made, fraudsters eventually show up.
In the world of online advertising, ad fraud is a massive problem. For example, some accounts estimate that as much as 25 percent of all paid ads are fraudulent. For the average ad campaign, fraudsters end up stealing one out of every four dollars from your budget—and stuffing that cash into their own pockets.

Ad fraud poses an already significant challenge, with a staggering $100 billion at stake and increasing relentlessly. This escalation is propelled by the rapid advancements in the digital age, the rise of influencers, loopholes in laws and penalties, and the simple lure of easy money. Experts forecast that this nefarious trend is set to continue growing at an exponential rate, underscoring the need for immediate, effective countermeasures.

CLICK FRAUD

This involves the generation of fake clicks on a pay-per-click (PPC) advertisement. These clicks can be generated by human click farms or automated bots and are designed to exhaust an advertiser's budget without providing genuine engagement or potential sales.

IMPRESSION FRAUD OR AD STACKING

This type of fraud involves loading multiple ads on top of each other in a single ad placement. While only the top ad is visible to the user, the advertiser is charged for all the ads.

DOMAIN SPOOFING

Here, fraudsters trick advertisers into thinking that their ads are being displayed on reputable, high-traffic websites when they are, in fact, being shown on low-quality or irrelevant sites.

PIXEL STUFFING

This involves cramming a full-size ad into a tiny, one-pixel square that is invisible to the naked eye. The ad registers as viewed even though it's impossible for users to see it.

AD INJECTION

In this type of fraud, unauthorized ads are inserted into websites without the consent of the site owner, often via malicious browser extensions. These ads either replace existing ads or clutter the site with additional ones, diverting revenue away from the website's owners.

LOCATION FRAUD

This occurs when a fraudster misrepresents the location data associated with an ad impression, making it seem as if the ad is being displayed in a different, often more lucrative, geographic location.

RETARGETING FRAUD

This involves fraudsters tricking advertisers into believing they're targeting users who have previously interacted with their brand when, in fact, they're targeting bots or users who have never engaged with the brand.

AFFILIATE MARKETING FRAUD

This is when fraudulent affiliates generate artificial actions to claim commission payouts. It may involve fake clicks, impressions, form fills, or even sales, using methods like cookie stuffing, where a website or third-party drops a lot of affiliate cookies onto a user's computer without their knowledge.

LEAD GENERATION FRAUD

Here, fraudsters generate illegitimate leads using fake information or identities, with the aim of getting paid for these fraudulent leads. Often, these leads are of no value to the advertiser as they don't represent potential customers.

SURVEY FRAUD

In this case, bots, paid human responders, or fraudulent responders fill out online surveys, giving false information. This fraudulent activity can skew the survey results, wasting both the time and money of the company conducting the survey and offering a false representation of consumer opinion or behavior.

INFLUENCER MARKETING FRAUD

An influencer is someone who has a substantial social following and can sway others to make specific buying decisions. Fraud in influencer marketing arises when an influencer utilizes bots or other deceptive techniques to artificially amplify their engagement metrics. In some instances, the "influencer" may not even be a genuine person, but a fabricated digital identity with purchased followers and simulated engagement, all designed to falsely represent influence and demand higher fees from advertisers.

VIEWABILITY FRAUD

The IAB definition defines viewability as "Greater than or equal to 50% of the pixels in the advertisement were on an in-focus browser tab on the viewable space of the browser page, and the time the pixel requirement is met was greater than or equal to one continuous second, post ad render." In essence, this means at least half of your ad is in-view for a minimum of one second. Display ads are sold based on this viewability standard. Fraudsters know how to hide ads and trick the measurement companies into thinking they were in-view when they are not. It's also important to note that the definition of viewability doesn't specify who is viewing the ad. Instead of a legitimate person, it could be a bot, malware, or a human fraud farm.

These are just a few examples of the most common types of ad fraud currently affecting the market. As technology evolves, new methods of ad fraud continue to emerge, making it a continually evolving threat to digital advertising.

Signs You May Have an Ad Fraud Problem

UNUSUAL CLICK SURGE

If your campaign is suddenly subject to an unexpected spike in clicks while it was maintaining consistent levels earlier, it might be indicative of ad fraud. Bots or click farms, employed by fraudsters, can fabricate an illusion of popularity, leading to unnecessary ad spending.

INCONSISTENT CONVERSION RATES

A noticeable increase in clicks without a corresponding rise in conversion rates suggests fraudulent activity. The numbers don't align, hinting that your campaign's performance is being compromised.

ABANDONED SHOPPING CARTS

A pattern of visitors loading their shopping carts but leaving without completing the transaction may indicate bots mimicking human behavior. Since bots can't finalize transactions, they simply abandon the cart.

RAPIDLY DEPLETED BUDGET

If you're spending a significant portion of your budget on advertising but seeing minimal or no return on investment (ROI), you may be a victim of ad fraud. Fraudsters deplete your ad budget by presenting ads to bots instead of real visitors, or by positioning ads where they are not viewable.

HIGH BOUNCE RATES

A high bounce rate, which measures the percentage of visitors leaving your site after viewing only one page, can be a sign of bot activity interfering with your campaigns.

MINIMAL SESSION DURATION

Traffic that lands on your site but leaves almost immediately could be a sign of bot activity. Real visitors typically engage with your content for longer than a fleeting moment, making zero-second sessions a potential indication of bot presence.

UNUSUAL TRAFFIC SOURCES

Inspect your traffic data for any unusual patterns. Illegitimate traffic often comes from large data centers, generating multiple clicks from the same IP address. If you're seeing traffic from areas outside your targeted demographic, it's a cause for concern.

POOR AD PERFORMANCE

If your ads are consistently underperforming, they may have been rendered virtually invisible due to fraudulent practices. Potential customers might be searching for your product or service, but if your ads have been tampered with, they may not be able to find them.

FEW PAGE VIEWS

If a newly launched ad fails to attract attention, it's possible that your ad isn't truly viewable. Fraudulent publishers might use tactics like ad stacking or pixel stuffing to render your ad invisible to the human eye, despite technically being visible.

EXCESSIVE NON-PRODUCTIVE IMPRESSIONS

If your ads are amassing a large number of views but are failing to produce meaningful engagement, you could be experiencing bot-generated traffic. Bots can overwhelm your web pages, artificially increasing the impression count without initiating any real actions.

CONFUSED CUSTOMERS

If you receive inquiries from customers who don't remember or never recall filling out your lead generation form, it may signal fraudulent activity. Bots or fraudsters could be filling out forms to blend in with legitimate traffic, creating confusion among your potential customers.

If you notice these or other suspicious patterns, it's important to investigate further.

What Is Ad Fraud Detection?

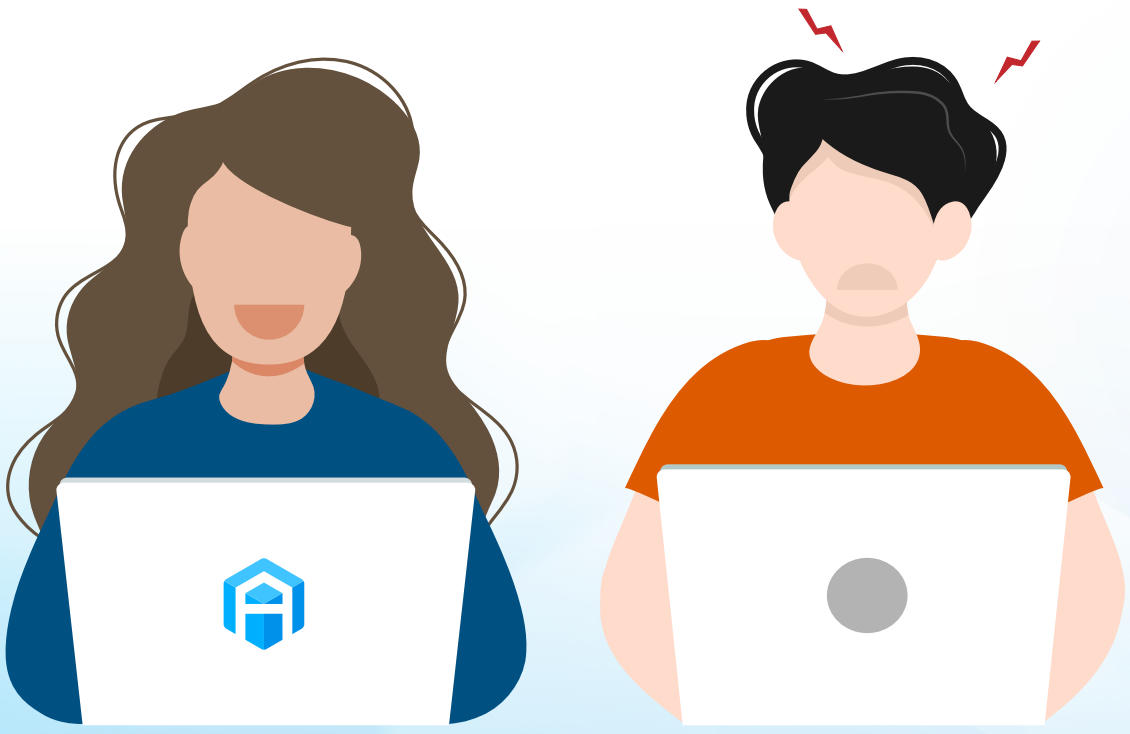
It is clear by now that ad fraud is a pervasive problem — one that is anticipated to become progressively more severe. Businesses are susceptible to numerous fraudulent tactics. So, how does one tackle this issue? When equipped with the right knowledge, you can identify if you have become a victim of ad fraud.

As highlighted, there are multiple signs hinting at potential ad fraud victimization, and this list is not exhaustive. With limited hours in the day and the myriad of responsibilities you shoulder, it might seem daunting to consistently monitor all these metrics to safeguard your marketing budget.

Fortunately, you don't need to manually shoulder the burden of ad fraud detection. By investing in an ad fraud solution, technology can undertake much of the task, streamlining your efforts.

For instance, Anura's ad fraud solution empowers you to verify your traffic in real-time. This software operates discreetly in the background, informing you about the authenticity of your visitors — whether they are genuine or fraudulent. With such insights at your disposal, you can strategically plan the optimal way forward for your business.

While ad fraud solutions can provide robust protection for your business against fraudulent activities, not all solutions are created equal. Subsequently, we will delve into why Anura is currently the most efficacious ad fraud detection solution in the marketplace.



How Can Anura Help with Ad Fraud Detection?

Anura's ad fraud detection solution is built on years of industry experience and a staunch commitment to client success. Its unique approach to detecting and mitigating ad fraud sets it apart from other solutions on the market.

Here's how Anura works: by installing a piece of code onto your digital properties, Anura collects hundreds of data points on every visitor's environment. This collected data is then run against Anura's extensive rule sets to determine if a visitor is genuine or fraudulent. These rules are continuously updated to combat new emerging forms of ad fraud, ensuring you're always one step ahead of fraudsters.

However, Anura's distinctive advantages do not end here. We present four key features that set Anura's ad fraud solution apart, solidifying its position as the gold standard in the industry.

ANURA DIFFERENTIATOR #1: ACCURACY

The crux of fraud detection lies in its accuracy. Inadequate detection measures can easily overlook signs of fraud. Anura delivers a robust, finely calibrated solution that delivers virtually no false positives. Get the peace of mind knowing you're never blocking real visitors, ensuring no loss of potential revenue from actual customers. By consistently validating rules and heuristics against actual conversion data, we fortify our results and arm you with the confidence to combat fraud.

ANURA DIFFERENTIATOR #2: THOROUGHNESS

A top-tier ad fraud solution demands thoroughness. Anura accomplishes this by collecting an extensive range of data points about your traffic, allowing us to delve deeper into the characteristics of your visitors and offer actionable insights on enhancing performance. Equipped with real-time capabilities, Anura distinguishes genuine visitors from fraudulent ones seamlessly. Our proprietary technology harnesses the power of machine learning along with our amassed years of expertise to identify even the most complex forms of fraud, leaving no stone unturned.

ANURA DIFFERENTIATOR #3: ANALYTICS

Effective fraud identification hinges on robust analytics, which offers evidence of fraud and sheds light on concerning trends of dubious activity. Anura's comprehensive dashboard equips you with the tools needed to analyze traffic as it lands on your web asset, providing customized reporting and multi-level drill-down capabilities. This empowers you to pinpoint the exact origin of the fraud, enabling future defensive strategies.

ANURA DIFFERENTIATOR #4: EXCEPTIONAL CUSTOMER SUPPORT AND ONGOING ASSISTANCE

Adopting a new technology often brings with it a learning curve. Understanding the challenges that might arise as you become familiar with a new system, we have invested heavily in our customer support services to ensure you are never left feeling unsupported. We are committed to being there for you whenever you have questions - providing answers and solutions is our top priority.

We offer live phone support from Monday to Friday, 8 a.m. to 5 p.m. EST, straight from our headquarters in Delaware. Our team of software and technology experts is proficient in the field of ad fraud, ensuring you have access to accurate and comprehensive information whenever you need assistance.

Our dedication goes beyond simple troubleshooting. We offer quarterly reviews for consistent performance optimization, integration assistance for seamless setup, and unlimited support, underscoring our commitment to your success. Our comprehensive documentation ensures you can effectively use our tools to combat ad fraud. With Anura, you're not just getting a solution, but a steadfast partner on your ad fraud detection journey.

Ready to Shield Your Business from Fraudsters?

Distinguishing between genuine transactions and fraudulent schemes can be a monumental task. However, with the appropriate monitoring tools, you can proactively mitigate the effects of ad fraud on your business and even potentially eradicate it entirely.

With Anura tackling the hard part, you can optimize your marketing budget, diverting more time and resources to other crucial aspects of your business. Consequently, you'll be able to distinguish between authentic and fraudulent visitors, enhance the efficiency of your campaigns, alleviate potential risks, and yield higher ROI, all while thwarting malicious actors from denting your profits.

Anura understands the importance of making the most out of every marketing dollar. Our mission is simply to "Increase our client's growth and improve their marketing results through accurate and effective ad fraud mitigation."

Our team of ad fraud experts has navigated trillions of requests for our customers, and at the end of the day, our expertise, ethics, and total dedication is the secret sauce to not only our success – but your success.

Contact our team today to learn more about Anura and how we can help your business grow, thrive, and survive in the ever-evolving landscape of digital marketing.

Experience the **power** of Anura to discover just how much fraud you have—and where the fraud is coming from—with a FREE trial!

> Contact Anura today and request a 15-day fully functional trial of our ad fraud solution. Find out how easy it is to put a stop to ad fraud before it eats away at your marketing budget!

Anura

Anura.io
(888) 337-0641
222 Carter Drive, Suite 201, Middletown, DE 19709