Ad Fraud 101

eBook

Table of Contents

Ad Fraud 101 Overview

Online advertising is a massive market. Global digital ad spending is expected to top **$650 billion by 2023.** This is great news for advertisers – but also great news for fraudsters.

Unfortunately, wherever there's a lot of money to be made, fraud often follows. Advertising fraud can be a big problem for those working in all areas of the market, diluting the efficacy of results and squandering opportunities for the companies trying to play by the rules.

In 2020, advertisers lost a whopping $87 billion to ad fraud, and the problem is only getting worse.

More granularly, research suggests **25 percent of all digital marketing spend is fraudulent,** which is a nice way of saying that bad actors put one out of every four dollars you spend on advertising in their own pockets.

Add it all up, and it comes as no surprise that more than one-third of marketers agree that ad fraud is becoming a bigger and bigger problem every day - a number we suspect will only continue to increase over time.

The risks and consequences of ad fraud can be costly, so advertisers are encouraged to know the signs and understand the ramifications. This guide will tell you what you need to know about ad fraud, from what it is to how it works - and what you can do about it.

What Is Ad Fraud?

Ad fraud is the practice of viewing, clicking, converting, or generating false interactions with any web asset for the sole purpose of earning money directly or indirectly. These actions are solely profit-driven and have no ties to the actual content of the advertising. Fraud can involve bots, malware, humans, or a combination, depending on the end goals of the fraudsters.

From web scripts designed to increase clicks to human fraud farms, there are a lot of opportunities out there for advertisers to find themselves swindled by less-than- scrupulous sources.

Fraudsters hide in or mimic legitimate traffic. On the surface, many of them appear to be legitimate sources of advertising. Advertisers are encouraged to trust these fraudsters and are then swindled by forms of fraud that don't appear illicit until it's too late. This costs advertisers a significant amount of money, and all without any benefit.

Not sure how it works? Here's just one example:

A fraudster can set up a fake website designed to do little more than host ads. By populating the site with as many ads as possible and using bots, malware, or human effort to repeatedly click ads and drive an inflated number of impressions, fraudsters can then sell impression volume to ad exchanges for high profits. Advertisers who place ads on these kinds of sites will assume high traffic and thus high engagement, but none of the site activity is authentic and thus won't yield any sales.

While there's a lot to be gained from digital advertising, especially in today's web-driven era, it's not all sunshine and roses. The more advertisers know about common areas of fraud, the easier it is to avoid problematic and costly situations.

Common Types of Ad Fraud

Ad fraud comes in all shapes and sizes. It's a complex and ever-changing world you must navigate. Here are many different forms of ad fraud you need to know about.

Ad Hiding

Ad hiding is a strategy that involves hiding ads in some way on a website. In this scenario, user traffic is legitimate, but the ads are never seen. There are a few techniques that fraudsters use to hide ads, including pixel stuffing and ad stacking.

Ad Injection

Ad injection is a more nefarious pathway for fraud. This method uses malware to infect a website to override normal ad placement protocols. This opens a site up to unwanted advertising, which can be placed in spots that haven't been paid for or, worse, were purchased by legitimate advertisers. Most injected ads are irrelevant to the website in question or feature inappropriate content. Due to the malware required to achieve this strategy, ad injection poses a significant risk to the sites in use. This scam can affect companies of all sizes.

Ad Stacking

Ad stacking is a way to hide ads on a page for the sake of maximizing the number of impressions while saving website real estate. Using this strategy, ads are stacked on top of one another so that only the top ad is visible. While all of the ads register impressions when users visit the website in question, the user will only see one ad per stack. All of the other ads included in a stack will fail to perform as they can't be seen by visitors to the site. This technique implies that a site provides a large number of impressions, even though traffic is largely worthless.

Affiliate Marketing Fraud

Affiliate marketing is a marketing avenue in which businesses pay affiliates who can draw in new visitors or customers. Generally, the affiliate receives some sort of kickback for every new action generated, which can be in the form of impressions, clicks, leads, or eCommerce purchases. Affiliate marketing fraud aims to cheat merchants, buyers, orlegitimate affiliates through the use of misleading or fraudulent activity to earn illegitimate commissions.

Auto-Refresh

When a website owner wants to increase the number of impressions they can sell, they can automatically refresh the page, part of the page, or just the ad unit itself to generate more impressions while the visitor is spending time on the site. For example, if a visitor spent an average of three minutes on a site, and if just one ad unit was updated every 10 seconds, this would translate to a sale of 18 ad units instead of just one.

It's important to note that the use of auto-refresh features isn't always fraud. In some cases, web users may utilize auto-refreshing add-ons to check for changing page content. This may be done when trying to purchase tickets to an in-demand show or looking for new posts on a forum.

Bot Fraud

Short for "robot", a bot is an automated software program built to carry out a specific task. Unethical programmers can re-tool bots for malicious purposes in a variety of ways; often designing malicious bots to serve malware, take over networks, steal information, plagiarize content, and steal marketing dollars from unsuspecting advertisers. Bots usually mimic normal activity and can be hard for advertisers to detect. Bot fraud usually involves the use of bot farms or large collectives of bots that act in unison usually referred to as a botnet.

Click Fraud

Pay Per Click or Cost Per Click advertising is where an advertiser can place their ads onto a site or network and they are only charged when someone clicks on their ad. Fraudsters take advantage of this type of marketing by using bots, malware, or humans to click on ads to make money. In some cases, click fraud is committed by competitors who are trying to deplete the competing company’s advertising budget.

Click Spamming

Fraudsters use the concept of a Denial of Service (DOS) to attack networks in order to steal money from their advertisers. With a click spamming attack, the fraudster floods the network with enough clicks to attempt to overwhelm the network billing software and trick it into paying the fraudsters.

Cookie Stuffing

Cookie stuffing is a sub-area of affiliate marketing fraud. Cookies are a big part of tracking web traffic and activities, but cookie stuffing uses this tool illegitimately to tag users. Fraudsters who cookie stuff, tag web users with cookies from unrelated websites that they did not visit without permission. These stuffed cookies affect how the activities of users are seen online. If, for example, an affiliate marketer directs a customer to make a purchase, the cookies will link back to the fraudster, who will receive credit for the sale.

Data Centers

A data center is a physical location that houses the infrastructure to power apps, websites, etc. Since many ad fraud attacks happen from overseas, fraudsters can take advantage of the IPs within the data center to make the traffic appear to be coming from the correct geography.

Device Spoofing (UA spoofing)

In order to hide fraudulent traffic coming from the same device, fraudsters employ technology that will make their one device look like many other devices. This is also referred to as User-Agent spoofing.

Domain Spoofing

Domain spoofing is the act of driving fraudulent traffic to an illegitimate domain and making it appear as if that traffic comes from a trusted domain. Many advertisers build lists of trusted domains. When the fraudster spoofs a domain on that list, their traffic will be accepted. Another way is to use a "look-a-like" domain (aka URL substitution) to trick a user into visiting their site or accepting their traffic because their name looks like a trusted domain.

eCommerce Fraud

eCommerce, or online shopping, is predicated on conversions. When ads don't convert, placement becomes a question. In order to perpetuate eCommerce fraud, some particularly savvy fraudsters will use stolen credit cards to make transactions, creating a false conversion rate that warrants ongoing ad fraud.

Geotargeting Fraud

Geotargeting fraud occurs when an advertiser targets specific geolocation. In this form of fraud, a fraudster sends ads from a different location, masking it to look like the location the advertiser targeted.

Human Fraud

Human fraud is the hardest form of ad fraud to detect as it relies on a network of humans, instead of using bots or malware, to interact with ads and create false transactions. Because actual humans are interacting with the ads, there are no obvious signs that can differentiate normal traffic from human fraud.

Influencer Marketing Fraud

In marketing terms, an influencer is someone who has a large following socially and can "influence" others to make specific buying decisions. Influencer marketing fraud occurs when an influencer is either using bots or other techniques to artificially inflate their engagement with the advertiser. Sometimes, the influencer isn't even a real person.

Invalid Traffic (IVT/GIVT/SIVT)

Invalid traffic, often known as IVT, refers to any form of web traffic that is derived from a non-human source. In some cases, this kind of traffic exists for a good reason, like search engine crawlers. However, most of the time, IVT is used to refer to fraudulent traffic.

IVT comes in a few different forms, including General Invalid Traffic, or GIVT. GIVT refers to bots, crawlers, spiders, or any of the kind of non-human traffic routed from a data center IP address. GIVT can also apply to activity-based filtration or browsers that pre-render pages. Most of the time, GIVT is easy to identify and exclude from results.

SIVT stands for Sophisticated Invalid Traffic. SIVT techniques are far more challenging to detect. This can include bots that closely mimic human traffic, hijacked devices, invalid proxy traffic, or cooking manipulation techniques, like stuffing.

Lead Generation Fraud

Lead generation is one of the primary objectives of digital marketing. In a lead generation-focused ad, online advertisements take users to a landing page where they can sign up to request more information.

In order to commit lead generation fraud, a fraudster will use a bot, malware, or humans to fill in the lead forms using stolen information, in order to bypass detection. This will create a myriad of issues for the advertiser.

Malware Ad Fraud

Malware is malicious software installed on an unsuspecting user's computer, either desktop or mobile, that is designed to perform specific tasks. For example, it can be used to steal personal information from the user or commit ad fraud. Malware ad fraud hijacks a unique device, mimicking a real user to perform tasks that steal advertising dollars by viewing or clicking on ads, watching videos, filling in forms, and other unsavory activity unbeknownst to the user.unsavory activity unbeknownst to the user.

Mobile In-App Advertising Fraud

Mobile apps are a huge source of advertising. Many apps are fully ad-sponsored, providing a free platform for fun or function for users willing to put up with ads from time to time. There are a few different ways in which fraudsters can use apps to defraud advertisers, but the primary method involves hiding ads to generate false impressions. Instead of making ads noticeable, like in video or banner form, ads are hidden in places users won't see, collecting impressions but without any user engagement.

Pay Per Call Fraud

Also called cost per call, pay per call is an agreed-upon rate paid by an advertiser for a call that meets minimum call duration. In most cases, a duration of at least two minutes is required for a call to be considered a billable event, but this can vary based on advertiser needs and preferences. While more difficult to defraud an advertiser than web advertising, some fraudsters do target pay per call models. Calls are typically generated from landing pages that contain phone numbers but can also be bought and sold through call networks. Two techniques used to commit Pay Per Call Fraud are using an overseas call center or an avatar:

- **Overseas Call Centers**

  With an overseas call center model, call center workers call advertisers and ask relevant questions just long enough to pass the minimum call duration before disconnecting. The advertiser must pay, because the call was long enough, but gained no viable leads in the process.

- **Avatars**

  When using avatars to commit call fraud, advertisers interact with a pre-recorded message that sounds like a real conversation. Unlike a call center model that uses actual people, avatars are all pre-recorded with a local dialect. The fraudster's goal is to keep the advertiser on the phone long enough to hit the call duration threshold. Successful avatars are very difficult to detect as they are often created after vetting an advertiser's phone routine.

Pixel Stuffing

Pixel stuffing is a fraudulent technique in which a standard ad is reduced in size and placed in a single pixel. The ad technically exists on the site and visitors trigger impressions. However, individual pixels aren't visible to the human eye, so viewers aren't able to view these ads. Any impressions generated using pixel stuffing are illegitimate, as visitors are unable to see any advertising in place. Because pixel-stuffed ads take up very little real estate, fraudsters can fill an entire site with pixel-stuffed ads to create the illusion of a significant number of impressions.

Viewability

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, in reality, 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 human fraud.

Ad Fraud and the Law

As illustrated above, ad fraud is a big problem that affects many different parts of the market and advertising strategies. Many fraudulent activities are easy to carry out and can garner big profits for moderate effort, giving those without scruples plenty of opportunities.

For advertisers who have lost significantly due to fraud, it's natural to assume there may be legal recourse available. However, this generally isn't the case. There are currently no laws related to ad fraud, so advertisers who lose out are expected to live with the loss. And that loss can add up: by 2023, experts estimate that ad fraud will cost advertisers $100 billion.

With so much to lose and plenty to gain by making a legal case, why aren't advertisers going after fraudsters? There may be a few reasons in play here.

First, legal resources come at a price. Hiring an attorney to attempt to identify the source of fraud – which is often easier said than done, due to the many ways in which fraudsters can mask an online identity – can be very costly. In addition, prosecuting someone for theft requires evidence, and this can be a challenge to pin down. If evidence isn't available, companies may be spending excessively on legal fees for no reason.

Even if a crime is apparent, finding out who is behind it can be almost impossible. There are many avenues in which to commit fraud, and many of them manifest in the same way. This means that determining how fraud is occurring or who is behind it often isn't entirely possible. For companies with ads running on many different platforms, pinning down the problem may take more time or effort than it is worth. Even things like unearthing a masked IP address can take far longer than an ad campaign will run. With these hurdles in place, most advertisers are more likely to eat the loss and change procedures for the future than attempt to prosecute.

Unfortunately, there are millions of fraudsters on the internet looking for a quick buck. Identifying a single source of fraud may alleviate financial pressure in the immediate future but arresting one person won't solve the problem on the whole. No one has the time or money necessary to track down every fraudulent source. Sooner or later, attempting to hold a fraudster accountable will start to feel like a game of whack-a-mole: as soon as you hit one, another pops up.

Identifying an Ad Fraud Problem

Do you have an issue with ad fraud? If you're not familiar with the signs, you may never know. Beyond the types of fraud you just learned about, it's important to understand the symptoms of an issue with ad fraud in addition to the ways in which fraud can be committed. These are some of the most common signs that a fraudster is affecting your ad campaigns:

Abandoned Shopping Carts:

While abandoned shopping carts are a common issue in eCommerce, too many shopping carts left unpurchased could be a sign of fraud. In these cases, fraudsters mimic normal human behaviour. However, since they typically don't purchase anything, they'll bounce and abandon their cart.

Client Complaints:

Angry clients are far more likely to be vocal than pleased clients. If you are suddenly facing a barrage of complaints related to things like lead generation or affiliate behaviour, there may be fraud lurking under the surface.

Clicks Without Conversions:

If a campaign launches that is getting a significant number of clicks but little to no conversions, fraud could be the culprit. Clicks are only as valuable as the customers they convert. While not all clicks on an ad will yield a conversion, a percentage will.

Clicks on Unusual Links:

There are plenty of links that exist on a website, like a privacy policy or terms and conditions. Few, if any, users click these links on a regular basis. However, if these kinds of links have an obvious increase in click rates, fraud could be the cause.

Confused Leads:

In most businesses, calling or emailing new leads is a normal part of creating connections with customers. Lead generation fraud may be the source if contacting prospective clients results in confusion or an absence of familiarity. This is particularly true if a lead claims they never filled out a form or expressed interest in products or services.

Drained Budget:

If you're spending a ton of money but getting little to no ROI, you could be experiencing fraud. Fraudsters can burn through your ad budget through a variety of techniques including the use of bots, malware and human fraud.

eCommerce Chargebacks:

For fraudsters to commit ad fraud, their traffic must show some level of conversions. To do this, they use stolen credit cards to complete eCommerce transactions. If custome chargebacks start to increase you may be dealing with fraud.

High Bounce Rates:

Real visitors intentionally click on an ad, like a banner or a listing in search engine. However, sometimes ads do get clicked by accident. If your bounce rate increases, fraud could be the cause.

Low Click-Through Rates:

If you recently put an ad up, but you aren't getting any response, fraud could be at the source. One possibility is your ad isn't viewable. Shady publishers engage in methods like ad stacking or pixel stuffing, where your ad will be posted but in a way that's invisible to the human eye.

Low Session Duration:

A real visitor will spend some time visiting your website. However, if you're seeing session durations less than a few seconds (low time on site), fraud may be to blame.

Unfamiliar Traffic Sources:

Traffic data should always be a part of the ad analysis process. If something looks off about your traffic sources, you may be facing fraud. Bad traffic can originate from large data centers and send multiple clicks from the same IP address. If your traffic is coming from an area outside of your target audience, this is a red flag.

Unusual Click Rates:

Most advertisers, particularly those who have been running their campaigns for a while, know what results are typical. Some variations will occur from one campaign to another, but in general, performance is consistent. If click rates drop off sharply or explode in volume, fraud is usually to blame.

Let Anura Work for You

There are a lot of ways ad fraud can affect your business, but at the end of the day, the method doesn't really matter: from click fraud to affiliate marketing fraud, your ad dollars are on the line. For most companies, a squandered investment can be very damaging, compromising campaign results and wasting marketing spending that could be better invested elsewhere.

If you're tired of wasting your valuable resources on fraudsters or want to get ahead of ad fraud before it affects you, the right protection tools can be a big benefit. However, the market is large. There are lots of companies offering fraud protection on many different levels. Unfortunately, most only target a few of the most popular types.

When you want results, you want Anura. An industry leader with over two decades of software development practice, trillions of impressions processed, a client list comprising some of the largest names in the game, and tools no one else can rival, **Anura is the best in the business for fraud – guaranteed.**

Anura utilizes best-in-class resources to dig deeper, combining accuracy with analytics to help optimize campaign performance for unparalleled protection. With expertly curated insights that specifically target fraudulent traffic, Anura is able to increase campaign returns and improve ROI by eliminating wasted spending for good.

How Anura Can Help

Plenty of ad fraud protection products are all talk and no action, but we're serious about what we do. Our solutions are designed to help you see results unavailable anywhere else. Here's what sets us apart.

Unparalleled Accuracy

Accuracy is the cornerstone of identifying fraud. When detection measures aren't up to par, it's easy to miss signs of fraud. Anura detects fraud via a robust, fine-tuned solution that delivers no false positives. Get the peace of mind knowing you're never blocking real visitors, ensuring no loss of potential revenue from actual customers. Anura consistently validates rules and heuristics against true conversion data strengthening our results and providing you with the confidence you need to defend against fraud.

Thorough Results

A great ad fraud solution needs to be thorough. Anura captures hundreds of data points about your traffic to learn more about who is visiting your web assets and how you can improve performance. Anura is able to spot the difference between a real visitor and a fraudulent one in real-time. Our solution leverages machine learning combined with decades of expertise to find even the most sophisticated fraud, ensuring no stone is left unturned.

Comprehensive Analytics

Analytics are at the crux of identifying fraud, providing the proof of fraud, and highlighting concerning trends of problematic activity. Anura's extensive dashboard gives you the tools you need to analyze traffic right when it hits your web assets, allowing users allowing users to customize reporting with the ability to drill down multiple levels. This allows you to pinpoint exactly where the fraud is coming from in order to defend against it in the future.

Dedicated Support

When you have questions, Anura has answers. Live phone support is available Monday to Friday, from 8 AM to 5 PM. Anura's software and technology experts are highly experienced in ad fraud detection, ensuring accurate and comprehensive information whenever clients need assistance.

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.

Contact us

www.anura.io/contact-us

☎ (888) 337-0641

✉ sales@anura.io

222 Carter Drive, Middletown, DE, 19709