E-BOOK

Anura

AFFILIATE MARKETING FRAUD 101

2020 will be remembered for many things, and perhaps one of the biggest marketing milestones is this: the internet will account for more than half of both US and worldwide ad spending. Equally remarkable, experts forecast worldwide ***digital ad spending will reach $326 billion in 2020, an increase of 11.1 percent.***

Although these are certainly trends worth noting for marketing teams across all industries, the amount of money flowing into online advertising platforms is also being noticed by those looking to make extra money with more nefarious motivations. ***Enter: ad fraud.***

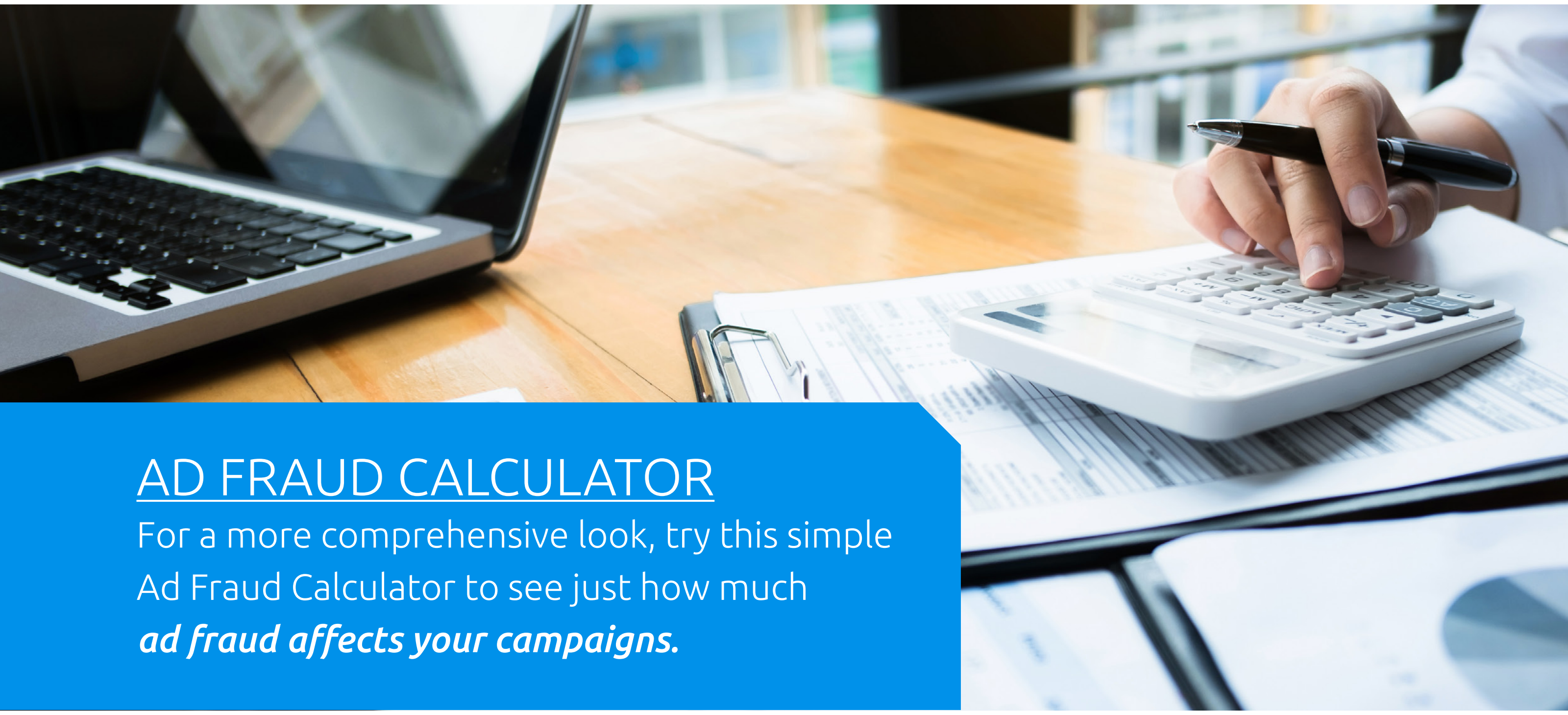
WHAT IS AD FRAUD?

Ad fraud is the practice of generating fake interactions with a web asset—through views, clicks, and conversions, for example—for the sole purpose of directly or indirectly funneling money away from the advertiser and to the fraudster. Both malicious bots and malware can execute these attacks, but they can also be conducted by humans in the form of "fraud farms." Making matters worse, the con has evolved so much that many of these forms of ad fraud often appear legitimate because they are so organized.

Just how big of a problem is ad fraud to global advertisers? One study by Adobe found that about 28 percent of website traffic is fraudulent, meaning that bots or click farms were behind a significant amount of views coming into online platforms. Put another way, fraud could have cost businesses around the world $42 billion of ad spend in 2019, a dramatic 21 percent increase from 2018. The same Juniper Research forecast also projects that by 2023, global businesses stand to lose $100 billion due to sophisticated ad fraud.

What do all of these percentages and billions mean for your budget? Here are some figures you may find more relatable:

- If you spend $100,000 a month on advertising, your losses total about $28,000 per month.
- If you spend $1 million a month on advertising, you are losing $280,000 a month to fraud.



AD FRAUD CALCULATOR

For a more comprehensive look, try this simple Ad Fraud Calculator to see just how much ***ad fraud affects your campaigns.***

WE ALL KNOW THAT FINANCIAL LOSSES ARE EASILY QUANTIFIABLE NEGATIVE EFFECTS.

Other business resources could also be added to the equation, like staff time lost to researching and addressing potential ad fraud. Similarly, ad fraud can affect the relationships that businesses have with their publishers, affiliates, and other large websites that participate in marketing campaigns, which ultimately tarnishes their reputations.

Just think of how difficult it is to have conversations with your existing or new affiliate partners about their ad fraud prevention strategies and what forms of proof reviewed at what frequency are "good enough," not to mention the staff time required to handle these efforts. Despite all of this research, you still might question how effective—or honest—your partners are about preventing or performing ad fraud. Needless to say, questions like these can put a strain on existing long-term relationships and prevent new ones from growing.

The Many Faces of Ad Fraud

Unfortunately, cybercriminals use a variety of techniques to steal money from advertisers. These include:

- Impression fraud: When ads are viewed not by actual humans, but are fraudulently displayed digitally to collect money
- Click fraud: Either human- or software-driven click farms or botnets that fraudulently click on advertisements
- Affiliate fraud: Affiliate marketing campaigns influenced or designed to generate false clicks, leads, or sales
- Lead fraud: When cybercriminals organize groups of humans to complete lead generation forms and then pay for each finished "lead"
- E-commerce fraud: A fraudulent transaction generated from an affiliate link that pays the publisher for generating a sale before the chargeback happens; this form of fraud is common with affiliate marketing scams
- Sourced traffic: When fake traffic is purchased to make a website appear more popular than it actually is, or to participate in digital advertising campaigns to generate clicks or impressions.
- Fake websites: Fraudulent websites that look legitimate enough to sell advertising space

These various forms of fraud all share certain warning signs, and they also rely on groups of either botnets or human fraud farms. Botnets are collections of computers infected with malware that controls a portion of their activity, like perpetrating ad fraud. In turn, these botnets can control infected computers to visit websites, generate page views, or click on digital ads, even if the infected computers reside in homes, businesses, or schools. Botnet groups are relatively cheap to set up or rent, but they can be very effective.

Human fraud farms are more complex to establish and run, but they are equally hard to parse out from legitimate web traffic because authentic human characteristics and behaviors make them better at avoiding fraud detection solutions. This is, of course, because human fraud farms are collections of real people employed to commit acts of ad fraud on behalf of the cybercriminals that pay them.

The Evolution of Affiliate Fraud

Fraudsters aren't necessarily picky about their ad fraud victims; big brands, small businesses, and the organizations that support them are all on the table for exploitation. However, out of all of these groups, affiliates prove particularly vulnerable because they serve as intermediaries or indirect participants in larger digital marketing campaigns, and they are often small businesses themselves.

Given the business model where affiliates earn a significant percentage of money from each transaction, in addition to the growing use of online influencers and web and blog platforms, affiliate marketing is an attractive target for cybercriminals. On top of it all, downstream risks and financial impacts may also affect partner businesses.

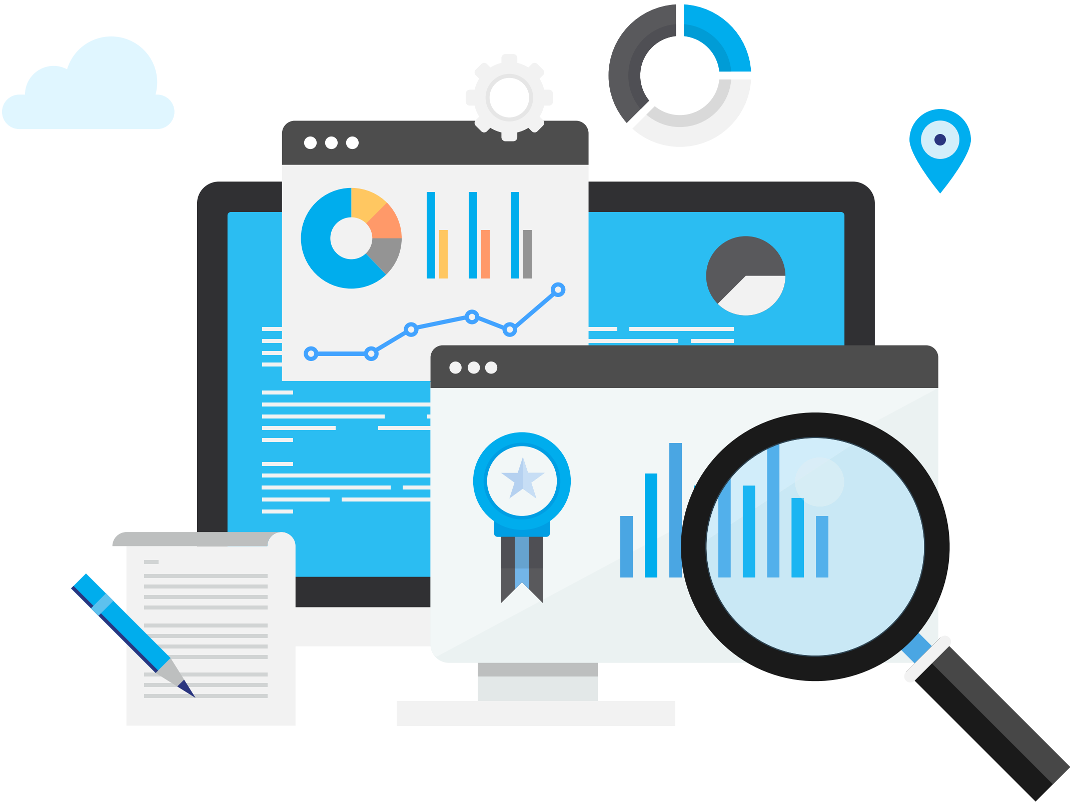
HOW AFFILIATE MARKETING FRAUD IS DIFFERENT

Before we attempt to solve the problem, we first need to make sure we understand it and how it works.

Affiliate Marketing Basics

Affiliate marketing is the process by which an affiliate—an individual, company, "influencer," web platform, or other marketing organization—earns a percentage of a sale or a similar commission for marketing another company's products. The sales resulting from their marketing efforts are digitally tagged, tracked via affiliate links from one website to another, and passed on to the business selling the product or service.

Put another way, affiliate marketing involves external parties sharing the responsibility for product marketing. The producers get to take advantage of their affiliates' platform, reputation, and online presence. The affiliate contributors get a share of the profit from the product sales.



However, a buyer (or potential buyer) does not always need to purchase a product for an affiliate to receive a reward. Depending on the relationship between the publisher/affiliate and the product creator, an affiliate's role in a seller's overall sales for a given period can be measured in a variety of ways.

- Per lead: An affiliate receives compensation when a consumer visits a seller's website and completes a certain action, such as filling in a lead form, beginning a product trial, signing up for a newsletter, or downloading a document
- Per sale: The traditional affiliate model; an affiliate receives a percentage or set rate of the sale price of a product or service when a consumer completes a sale as a result of the affiliate's marketing efforts
- Per click: An affiliate directly routes a consumer to a seller's website, increasing the amount of traffic or impressions

When done correctly, both parties experience a profit advantage in an affiliate relationship. These lucrative arrangements are big business, with the overall industry forecasted to surpass the $8 billion mark by 2022, more than double the affiliate market worth in 2015.

TRANSFORM THE IMPACT, ACCURACY, AND PERFORMANCE OF YOUR AD CAMPAIGNS.

AD FRAUD HURTS YOUR COMPANY IN MORE WAYS THAN JUST MONEY SPENT ON BAD CLICKS

Types of Affiliate Fraud

Plain and simple, affiliate fraud aims to cheat merchants, buyers, or legitimate affiliates through the use of misleading or fraudulent activity to earn illegitimate commissions.

Given the structure of these various payment and incentive models, it is easy to see how a deceitful affiliate or cybercriminal can use a range of techniques to manipulate behaviors—manually or through software—to maximize their own profits. At the end of the day the goal remains the same: tricking businesses and advertisers into thinking that a real consumer completed a specific action, including making a purchase, that results in a reward for the affiliate.

Because of the mechanics behind affiliate programs, where "tags" are placed in browsers or in referral links that identify the referrer, it can be difficult to monitor all of the various incoming traffic for validity. This presents fraudsters with many opportunities to hijack the process. These methods include:

- **Cookie stuffing:** A malicious affiliate loads a modified cookie onto a potential customer's computer after they interact with a part of the affiliate's online platform. Whenever that user visits other websites to make purchases, the affiliate is associated with the referral.
- **Bots:** Code-driven, autonomous programs that use victim computer networks to perform activities like spamming forms, watching videos, faking website visits, clicking ad links, or other functions that skew traffic metrics.
- **Click farms:** Through the use of large groups of individuals, fraudsters perform coordinated activities such as clicking on ads, filling out forms, signing up for newsletters, or following website referral links to generate impressions. This more nuanced human behavior makes it harder for fraud detection methods to succeed.
- **Malicious browser extensions:** Malicious software or extensions are loaded onto a user's computer, where they add tags to URLs, intercept browser requests, modify traffic, monitor user activity, or perform other activities that reward the fraudster.

- **Domain squatting/spoofing:** A fraudster replicates an existing valid website and publishes it to several similar domains with slightly different spellings or punctuation in an attempt to refer customers to the legitimate merchant and receive credit for future sales.

- **Fake websites/influencers:** Businesses unknowingly associate with fake websites or online personalities that use bots or purchased followers to build their persona.

- **Fake leads:** A fraudulent affiliate takes advantage of the cost-per-lead model by automatically or manually filling out lead forms with fake or stolen information, which awards the affiliate with a commission for each completed document.

- **Fraudulent purchases:** Often the most costly for businesses, this occurs when an affiliate fakes a sale (often with stolen credit card numbers) and collects the commission for the sale before the fraudulent purchase is flagged or the product returned. The victim business may also face chargebacks and additional shipping fees.

DECEITFUL AFFILIATES OR CYBERCRIMINALS *can use a range of techniques* to manipulate behaviors—manually or through software.

HOW AFFILIATE FRAUD AFFECTS YOUR BOTTOM LINE

Earlier, we discussed just how much ad fraud will cost global businesses in terms of lost digital advertising dollars. Unfortunately, those estimated numbers only capture the potential impact to your budget. As fraudsters grow more sophisticated and their methods evolve, the extent of their impact will continue to go up. At the same time, ad fraud hurts your company in more ways than just money spent on bad clicks.

Credit Card Chargebacks

As alluded to earlier, credit card chargebacks take advantage of the turnaround time (usually 60-120 days) between an affiliate being paid out for their fraudulent referral and the resolution of the charge between your business and the payment card processor. These charges occur when a cybercriminal makes a fraudulent purchase, the affiliate receives payment, and the victim requests that their bank return funds by disputing the transaction. When the victim's bank cannot facilitate the resolution and refund with the business, the bank can forcibly take their money back.

If a business has too many of these chargebacks leveled against them, not only will their cost per transaction go up and their advertising ROI go down, but their ability to use that payment processor may be shut down too.

Revenue Stream Losses

Another way that ad fraud indirectly affects your bottom line actually occurs when your business tries to fight back. One common technical solution attempts to block traffic from known or suspected fraudulent sources, identifying them by IP address or suspicious behaviors, such as the amount of time spent on a website or their global location.

However, when you use this method of ad fraud detection, it can backfire and block activity that looks fraudulent but is actually legitimate. This will hurt your business if real customers cannot buy from you because your fraud detection tool suspects an abnormality and prevents the transaction. The way around this false-negative dilemma is to use an ad fraud detection solution that investigates e-commerce fraud, eliminates false positives, and continuously updates data points populated from sources around the world—features built into the Anura solution.

The Danger of Noncompliance

Failing to inhibit affiliate fraud can also lead to eventual regulatory compliance issues and even hefty fines. Although federal laws like the Telephone Consumer Protection Act (TCPA) were written in the early 1990s for a very different world and a very different advertising age, non-compliance with the TCPA can still put your business in a very costly position.

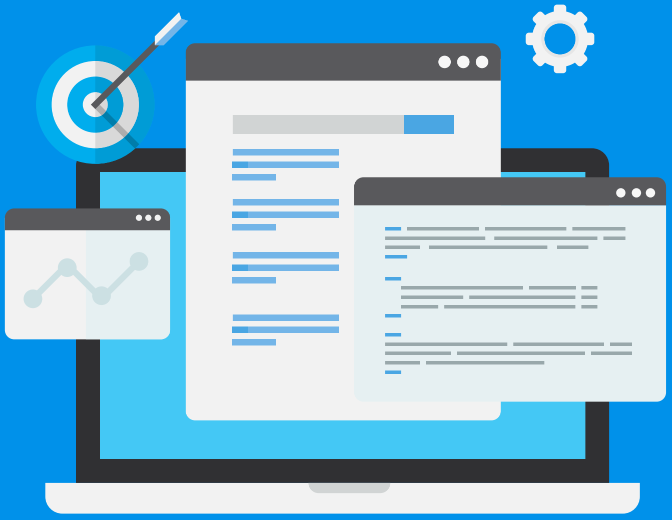
Back then, the telemarketing industry used improvements in autodialing technology to allow marketers to reach thousands of people per day, spamming consumers with prerecorded sales pitches and robocalls. Consumers became frustrated, and Congress passed the TCPA to ease their pain.

Over 30 years later, the TCPA still applies to the digital advertising world. In this case, when a business does not properly research or vet a lead from affiliates or lead forms, and they then contact the individual to follow up (in any form) using fraudulent data, it could create a TCPA compliance issue. Frequent TCPA rule violations can lead to hefty fines, ranging from $500-$1,500, should the victim decide to file a complaint.

A Tarnished Reputation

After costly chargebacks, the fear of compliance issues, and lost revenue and marketing dollars, the last thing a business needs is a damaged reputation. Consumers, publishers, and affiliate partners do not want to do business with a brand associated with e-commerce fraud or ad fraud.

With the ubiquity of stolen personal and credit card data, fraudsters don't hesitate to use it for financial gain. And if that fraudulent gain involves your company, even if the data theft wasn't your responsibility, chargebacks or even unsolicited calls from your brand can result in customers forming a bad association or feeling harassed. This is not the type of connection you want with your reputation.



STOP AFFILIATE FRAUD AND PROTECT YOUR BRAND

After all of these facts, figures, and potential onslaughts to your bottom line and brand, the fight against affiliate and ad fraud may seem insurmountable. However, businesses around the world know that several key strategies, when implemented correctly, can combat malicious online traffic from both botnets and fraud farms.

More specifically, utilizing a smart, sophisticated ad fraud solution, employing additional technical tools, and conducting necessary due diligence of your affiliate partners can stop illicit traffic from wasting your money and drive business growth by green-lighting legitimate customers.

ANURA'S AD FRAUD SOLUTIONS ARE AN INDUSTRY LEADER WHEN IT COMES TO PROTECTING YOUR BUSINESS

Use an Industry-Proven Solution

First and foremost, the most powerful decision your organization can make in the fight against ad fraud is to implement an ad fraud solution that analyzes hundreds of key *user data points* to determine if traffic is legitimate or not.

Notice that the emphasis here is on the user. Other ad fraud detection methods focus on vanity metrics such as viewability, but these data points are unreliable, inconsistent, and constantly evolving as fraudsters advance their techniques. Instead, effective fraud prevention focuses on a solution that forms an accurate picture of the visitor, identifies their origin, contextualizes their browsing behavior looking for anomalies, and takes action to block them if needed.

For example, web servers collect unique information about each visitor, and these data points can be broken down into meaningful facts about them. Empowered with this data—including an idea of where fake visitors may have originated—you have the ability to stop bad sources, regardless of where they come from.

This is where an ad fraud detection solution comes in. Effective ad fraud software takes all of this information and uses constantly refreshed metrics, rules, and heuristics to determine if your visitors are real or fake. The software might also report that fraudulent visitors are coming from a specific place in the world, or even from a specific source or affiliate.

Anura's ad fraud solutions are an industry leader when it comes to protecting your business from the techniques that criminals use against your brand and your digital advertising. Built by advertisers to stop the fraud they were seeing within their own campaigns, Anura's solutions block malicious activity by using hundreds of data points to identify ad fraud from bots, malware, and human fraud farms, performing this work within milliseconds. Because Anura knows the value of protecting legitimate activity, its solutions eliminate false negatives that would otherwise slow your business down.

Not only that, but Anura allows for flexible integration regardless of the type of site. For platforms that require comprehensive user data collection in real time or conversion and post-click analysis, Anura Script via Javascript integration could be the right fit. For sites that leverage server-to-server communication with limited user information, or for businesses that need to perform click analysis or programmatic campaigns, Anura Direct could be best.

In either case, Anura's dashboard gives your teams the tools to analyze data as it hits your web assets, easily identifying threats so that you can strengthen your defenses and improve your campaign quality and ROI.

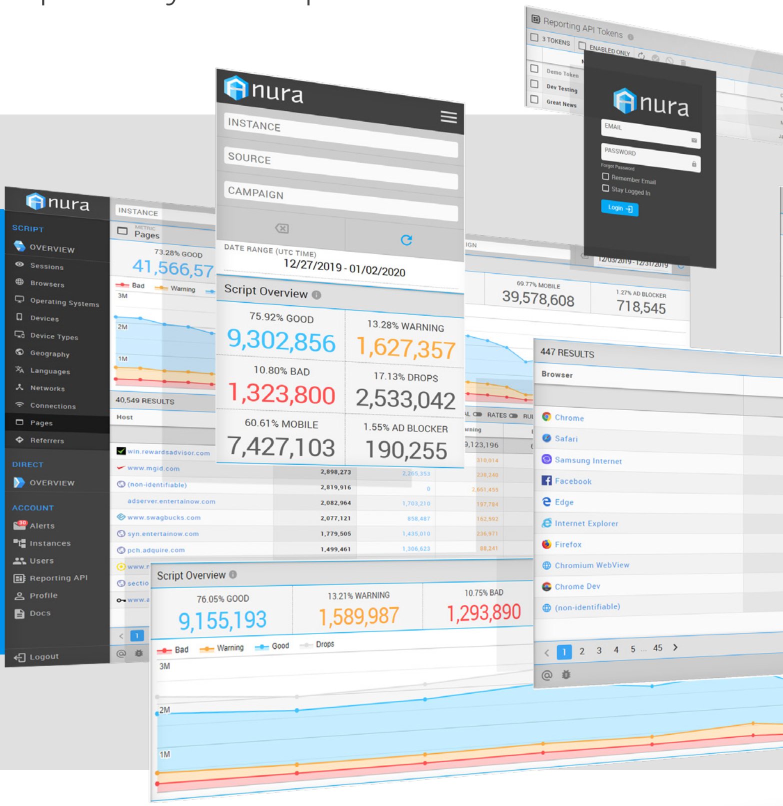
Do Your Due Diligence

Technical tools can go a long way toward helping to prevent ad fraud and catching it before it affects your business, but there is always still room for performing your own due diligence on your affiliate partners and ad networks. Even if your partners have long-standing, solid reputations, you still need to ensure that they are on the up-and-up or that their sources of traffic haven't gone rogue, and balance that with the trust that they have earned.

With this in mind, your own journey toward minimizing ad fraud can become a wider effort with your affiliate partners, helping them check their methods and traffic sources. This indirectly keeps ad fraud from hurting your business, solidifies your partners, and screens out those with newfound suspicious behavior.

Ongoing conversations paired with raw data provided by an ad fraud solution that constantly screens traffic, like Anura, are the best ways to independently validate partners and bolster legitimate transactions.

ANURA'S DASHBOARD
gives your teams the tools to analyze data as it hits your web assets, ***easily identifying threats so that you can strengthen your defenses*** and improve your ***campaign quality and ROI.***



DATE RANGE (UTC TIME)
12/27/2019 - 01/02/2020

Script Overview

75.92% GOOD	13.28% WARNING
9,302,856	1,627,357
10.80% BAD	17.13% DROPS
1,323,800	2,533,042
60.61% MOBILE	1.55% AD BLOCKER
7,427,103	190,255

73.28% GOOD
41,566,57

12/03/2019 - 12/31/2019

69.77% MOBILE	1.27% AD BLOCKER
39,578,608	718,545

40,549 RESULTS

Host			
win.rewardsadvisor.com			310,014
www.mgid.com	2,898,273	2,265,353	238,240
(non-identifiable)	2,819,916	0	2,661,455
adserver.entertainow.com	2,082,964	1,703,210	197,784
www.swagbucks.com	2,077,121	858,487	162,592
syn.entertainow.com	1,779,505	1,435,010	236,971
pch.adquire.com	1,499,461	1,306,623	88,241

Script Overview

76.05% GOOD	13.21% WARNING	10.75% BAD
9,155,193	1,589,987	1,293,890

Reporting API Tokens
□ 3 TOKENS □ ENABLED ONLY
□ Demo Token
□ Dev Testing
□ Great News

447 RESULTS

Browser
- Chrome
- Safari
- Samsung Internet
- Facebook
- Edge
- Internet Explorer
- Firefox
- Chromium WebView
- Chrome Dev
- (non-identifiable)

TAKE THE NEXT STEP

Luckily, just as the tools and methods that cybercriminals use to target your digital advertising have evolved, so too have ad fraud detection tools like those offered by Anura.

Anura's ad fraud solution helps protect your business against the techniques that criminals use to not only perform affiliate fraud, but all forms of ad fraud. Anura was created by advertisers for advertisers, providing a way to fight back by blocking malicious activity using hundreds of data points to identify fraud coming from botnets and fraud farms.

At the same time, Anura knows how important it is to allow legitimate traffic to flow, so we fine-tune our solutions to eliminate false negatives that can slow your growth and hamper your relationships with publisher networks. Anura detects when a human fraud farm fills out your forms or visits your sites versus a visit from a real user, helping to prevent damage to your brand and your bottom line from TCPA violations, chargebacks, and wasted marketing dollars.

REQUEST A DEMO

To find out how Anura can help you ***detect and defend against all forms of ad fraud,*** request a demo for your organization.