AD FRAUD:
WHY TRAFFIC SCORING ACCURACY IS THE MOST IMPORTANT THING

A Year Long Study in Ad Fraud.

anura

© 2017 anura.io

CONTENTS

EXECUTIVE SUMMARY 2

3 INTRODUCTION

WHAT IS AD FRAUD 4

5 HOW BIG IS THE ISSUE

TRAFFIC SCORING SOLUTIONS 7

8 WHY ACCURACY MATTERS IN TRAFFIC SCORING

THE BLACK BOX TEST 11

14 ANURA PERSPECTIVE

© 2017 anura.io

EXECUTIVE SUMMARY

- The cost of ad fraud is estimated at **$7.2 billion**, or approximately 5% of the total global digital media market.[1]
- The advertising industry faces $8.2 billion in corruption annually.[2] This comes from:
  - Invalid traffic contributed $4.6 billion (56%) in loss.
  - Malvertising suffered a cost impact of $1.1 billion (13%) in loss.
  - Infringed content, which is primarily comprised of lost ad and pay-for-content revenue, contributed $2.5 billion (31%) in loss.
- Ad fraud will reach **$50 billion by 2025**.[3]
- **Bad bots generate about 19%** of the total internet traffic globally.[4]
- Bad bots aren't the only source of bad traffic. **Humans also generate fraudulent traffic and impressions** in the form of click farms, ad stacking, ad injection, domain spoofing, etc. This type of ad fraud is harder to detect when traffic scorers are only looking for bad bots.[5]
- Traffic scoring systems are attempting to mitigate the problem through a variety of different means and methods.
- When a company knowingly serves ads that drive impressions and revenue from ads that are never seen, **they're committing ad fraud**.
- To combat ad fraud, **different traffic scoring approaches must be taken**.
- **It's impossible to benchmark something if you have no data to benchmark against**. When a company who provides traffic scoring has never sold traffic to a client, they have no way to validate their methods to an advertiser's point of view. This leads many companies to mismarking good traffic as bad, and bad traffic as good.
- Anura is a traffic scoring solution developed using client feedback since 2005 to provide accurate filtering from an advertiser's point of view by validating the user and not the ad unit.
- The higher the percentage of ad views by real people, the higher the conversion rate.

"Through this extensive year-long study of internet traffic, we proved that looking at a visitor through the eyes of an advertiser produces a more accurate score and an improved ROI for clients that care about true performance."

-Rich Kahn

[1] George Slefo, "Ad Fraud Will Cost $7.2 Billion in 2016," AdvertisingAge, Jan. 19, 2016, retrieved Feb. 6, 2017 from http://www.adage.com/article/digital/ana-report-7-2-billion-lost-ad-fraud-2015/302201

[2] "What Is An Untrustworthy Supply Chain Costing the US Digital Advertising Industry?" IAB US Benchmarking Study, November 2015, retrieved Feb. 24, 2017 from http://www.iab.com/wp-content/uploads/2015/11/IAB_EY_Report.pdf

[3] "Compendium of Ad Fraud Knowledge for Media Investors," World Federation of Advertisers and The Advertising Fraud Council, 2016, page 3

[4] "Bot Defense: Insights Into Basic and Advanced Techniques For Thwarting Automated Threats," Distil Networks, Enterprise Management Associates, Inc., retrieved Feb. 6, 2017 from https://resources.distilnetworks.com/i/740931-bot-defense-insights-into-basic-and-advanced-techniques-for-thwarting-automated-threats/3

[5] Ratko Vidakovic, "The Many Faces of Programmatic Ad Fraud," Marketing Land, Sept. 28, 2015, retrieved Feb. 21, 2017 from http://marketingland.com/many-faces-programmatic-ad-fraud-142335

© 2017 anura.io

INTRODUCTION

THE DIGITAL LANDSCAPE IS GROWING

With demographic and cultural differences, digital media is seeing an evolution that affects advertising purchasing patterns. The variety of search engines coupled with changing access to online websites, the digital landscape is expected to continue to evolve. As such, advertising will continue to make a seismic shift from traditional means to digital.

BAD BOTS ARE ALSO GROWING

In 2015, **3.2 billion devices** were connected to the internet worldwide.[6] With wide and far access to the internet, an evolution of bad actors are emerging. Bad bots generate about 19% of the total internet traffic globally.[7] These bad actors have leveraged global connectivity to exploit the advertisers and publishers while reaping the benefits.

However, these bad actors are only part of the global problem. It ignores that many advertisers value impressions over all else, real or false. Impressions are notoriously difficult to quantify, let alone qualify. When a company comes up with a new metric like viewability, that metric becomes a new target for bot makers. As proven by Methbot,[8] once bot makers beat the metric, traffic is then easily accepted by both publishers and advertisers, who rely on that metric.

To boot, bots continue to perpetuate because those protecting against bad bots don't share information, as shown with several sources [9,10] who claim they were aware of Methbot long before it became 'a thing.'

BOTS AREN'T THE ONLY FORM OF AD FRAUD

Ad fraud by humans is a big problem, too. Human click farms, invisible ads (ad stacking), domain spoofing, ad injection, and cookie stuffing are powered by humans, which are often overlooked by vendors searching for bot fraud.[11]

AD FRAUD WILL REACH $50 BILLION BY 2025

By the end of 2016, it was projected that overall spending on automated banner displays and video ads would grow to an impressive 18.7 billion worldwide, with U.S. advertising dollars accounting for half of that spend.[12] If a bad actor can slice even the smallest piece of that pie, they're in. Without sufficient countermeasures in place, it's projected that ad fraud will reach in excess of **$50 billion by 2025.**[13]

[6] Sarah Parkes, "ITU Releases 2015 ICT Figures," International Telecommunication Union, May 26, 2015, retrieved Feb. 6, 2017 from http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.WJiSKVUrK73

[7] "Bot Defense: Insights Into Basic and Advanced Techniques For Thwarting Automated Threats," Distil Networks, Enterprise Management Associates, Inc., retrieved Feb. 6, 2017 from https://resources.distilnetworks.com/i/740931-bot-defense-insights-into-basic-and-advanced-techniques-for-thwarting-automated-threats/3

[8] Thomas Fox-Brewster, "Biggest Ad Fraud Ever:' Hackers Make $5M a Day By Faking 300M Video Views," Forbes, Dec. 20, 2016, retrieved Feb. 6, 2017 from http://www.forbes.com/sites/thomasbrewster/2016/12/20/methbot-biggest-ad-fraud-busted/#640cbc284ca8

[9] Timur Yarnall, "Bringing Context to This Week's Methbot News," comScore, Dec. 23, 2016, retrieved Feb. 6, 2017 from https://www.comscore.com/Insights/Blog/Bringing-Context-to-This-Week-s-Methbot-News

[10] Jason Shaw, "Methbot? More Like Mehbot," Integral Ad Science, Jan. 6, 2017, retrieved Feb. 6, 2017 from https://integralads.com/resources/methbot-like-mehbot/

[11] Ratko Vidakovic, "The Many Faces of Programmatic Ad Fraud," Marketing Land, Sept. 28, 2015, retrieved Feb. 21, 2017 from http://marketingland.com/many-faces-programmatic-ad-fraud-142335

[12] Sapna Maheshwari, "Advertising's Moral Struggle: Is Online Reach Worth the Hurt?" The New York Times, Dec. 26, 2016, retrieved Feb. 6, 2017 from https://www.nytimes.com/2016/12/26/business/media/advertising-online-ads-fake-news-google.html?_r=2

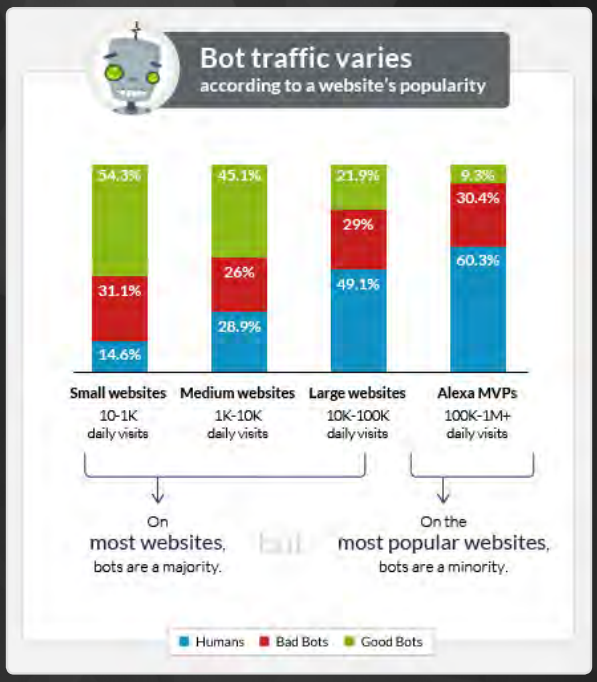
[13] World Federation of Advertisers and The Advertising Fraud Council, "Compendium of Ad Fraud Knowledge for Media Investors," 2016, page 3

© 2017 anura.io

WHAT IS AD FRAUD?

Ad fraud is the practice of exposing advertisements to bots, human fraud, and other bogus methods for the sole purpose of earning money directly and/or causing harm to another company's advertising campaign.[14]

There are many types of ad fraud that plague advertisers. Other types include click fraud, search ad fraud, cookie stuffing or affiliate ad fraud, impression ad fraud, ad injections, domain spoofing, traffic fraud (CPM), lead fraud (CPL), etc. Each type of fraud drains precious dollars from advertisers' budgets.



Source: Incapsula

The common perception is all ad fraud is committed by bots - nonhuman programs that generate fake ad impressions or serve hidden ads to trick browsers into downloading malware or spreading spam. However, ad fraud can also be fueled by humans (e.g. human fraud), which is just as serious. Since most systems focus on catching bad bots, not human-fueled fraud, they're leaving themselves vulnerable.

The point of ad fraud is to get paid for doing very little, simply by stealing advertisers' money without them knowing about it.

[14] Direct quote from Rich Kahn, CEO of Anura.

© 2017 anura.io

HOW BIG IS THE ISSUE?

The cost of ad fraud is estimated at $7.2 billion,[16] or approximately 5% of the total global digital media market in advertising. Although this is a huge sum, ad fraud isn't illegal. In fact, there's no legal recourse for committing ad fraud. It's no surprise the low risk and huge payoff makes ad fraud a lucrative form of fraud.

Even private exchanges aren't immune to ad fraud.[17] Just because you're working directly with specific publishers won't stop fraudsters. Anyone who pays someone for traffic is at risk for ad fraud.

In a report from Hewlett Packard, ad fraud is classified as having a higher potential payout than virtually any other form of digital crimes.[18] If no actions are taken, ad fraud could exceed $50 billion by 2025, one-tenth of the $500 billion that the digital ad market is projected to be worth at that time.[19]

Without legal recourse, ad fraud will run rampant and is projected to more than double by 2025. This must be addressed.

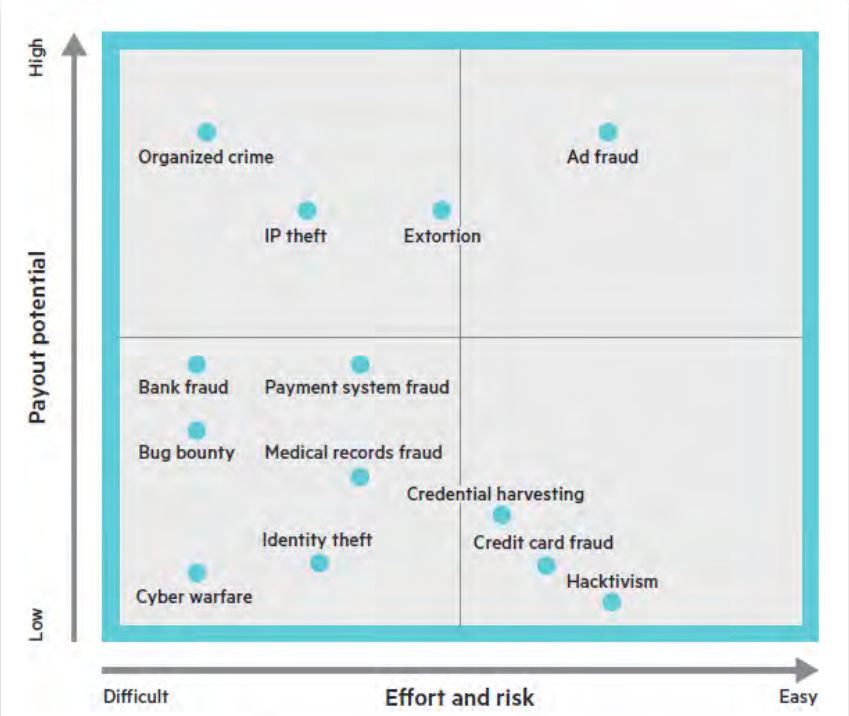


Figure 1: Attractiveness of hacking based on financial gain and effort

Source: Hewlett Packard Enterprises

[16] George Slefo, "Ad Fraud Will Cost $7.2 Billion in 2016," AdvertisingAge, Jan. 19, 2016, retrieved Feb. 6, 2017 from http://www.adage.com/article/digital/ana-report-7-2-billion-lost-ad-fraud-2015/302201

[17] AdExchanger, "Private Exchanges Aren't Immune to Ad Fraud," July 9, 2015, retrieved Feb. 7, 2017 from https://adexchanger.com/data-driven-thinking/private-exchanges-arent-immune-to-ad-fraud/

[18] "The Business of Hacking," Hewlett Packard Enterprises, May 2016, retrieved Feb. 6, 2017 from http://www8.hp.com/us/en/software-solutions/hacking-report/

[19] Patrick Kulp, "Ad Fraud Could Become the Second Biggest Organized Crime Enterprise Behind the Drug Trade," Mashable, June 9, 2016, retrieved Feb. 6, 2017 from http://mashable.com/2016/06/09/ad-fraud-organized-crime/#927wT5zPGsqC

© 2017 anura.io

As cybercrime continues to grow, and ad fraud becomes more sophisticated, the digital advertising industry will remain exposed. To mitigate the fraud, the Trustworthy Accountability Group, in a joint effort between the ANA, IAB, and the American Association of Advertising Agencies, is setting their own industry standards to combat ad fraud.

They're fighting back with a 'Verified by Tag' system, which includes a two-piece support system:

- A payment IR system to prevent payments to the bad actors.
- A registry of tag-approved advertisers and publishers.

There are also traffic scoring solutions, designed to aid in the identification of bad internet traffic and that focus on eliminating fraud BEFORE the advertisements are exposed.

© 2017 anura.io

TRAFFIC SCORING SOLUTIONS

Several companies have emerged that are able to review the quality of the traffic received and determine if the traffic quality is good, bad, or indifferent. These traffic scoring solutions use data collected to make determinations on the likelihood that the traffic is real or fake, or some other metric that they use.

COMPANIES PLAY BY THEIR OWN RULES

Each traffic scoring solution has its own set of rules and criteria with an internal tolerance level for discrepancies with the traffic scored. Some rules allow for no tolerance and will automatically tag the traffic as 'bad' while others have more flexibility.

SCORING ISN'T UNIVERSAL EITHER

Since these rules are proprietary, each traffic scoring solution may judge and view the traffic differently, meaning what is considered 'bad' with one vendor may fall within an acceptable tolerance level with another vendor and be marked as 'good.' But they're all judging traffic so, as an advertiser, accuracy matters.

SOMETIMES "THE BABY IS THROWN OUT WITH THE BATH WATER"

In the quest to remove bad traffic, sometimes good traffic is thrown out, too. Traffic scoring solutions build a rule, but have no benchmark to truly base it on, resulting in complicated algorithms that lead to inaccurate traffic scoring.

© 2017 anura.io

WHY ACCURACY MATTERS IN TRAFFIC SCORING

Traffic scoring is based on rules with complicated algorithms. But when a traffic scoring company has never sold traffic to a client, they don't truly know if their rules accurately work.

Third-party ad fraud solutions available today make a scale dictating the good traffic from the bad and expect you to trust it. Then Methbot comes along and gives you every reason not to trust their scoring methods.

Having never sold traffic to a client, there's no client feedback, which means there's no benchmark results. Without a benchmark to base metrics on, traffic can get mismarked, resulting in good traffic labeled as bad and bad traffic as good.

© 2017 anura.io

IT'S NOT WHAT SCALE LOOKS BEST, IT'S WHAT SCALE IS MOST ACCURATE

Let's say, you have a scale at the gym and one at home, which one do you choose to believe? Typically the one that gives you the more favorable results. Traffic scoring companies have essentially built a scale for traffic scoring. Whether it's accurate or not, it doesn't matter as long as everyone uses the same scale. So, traffic scorers build a scale, and market to everyone that they have the best scale, even if it has never been validated by an advertiser. That's how traffic scoring is currently working.

But what's most important is not what scale looks best, it's what scale is most accurate. Accuracy is based on true performance and true conversions. True performance is king.

SIMPLE ANSWER TO A COMPLEX AD FRAUD PROBLEM

Billions of analyzed clicks with direct client feedback have resulted in more improved, accurate rule sets based on client performance. However, it's not something that's been done in traffic scoring until now.

Developed by digital security experts and cybersecurity analysts, Anura is a traffic scoring solution based off of more than a decade of data collection of actual client traffic. It isolates and identifies the good traffic from the bad, so advertisers can make more accurate decisions about their traffic sources. While most scoring systems look at the analytics around an advertisement, Anura looks at the actual visitor. This shift in focus is another aspect that helps improve advertiser ROI.

Anura was designed from an advertiser's perspective. When CEO Rich Kahn started buying traffic for his own campaigns (he was the advertiser), it was apparent something wasn't right with the sources of traffic he was buying. As a developer, he started writing code for his website to help narrow down the issue. Ultimately this revealed ad fraud was responsible for the issues. To filter out and block the bad traffic, he built his first full traffic filtration platform.

© 2017 anura.io

As fraud evolved, he built a team of developers to continue improving the platform. Leveraging their decades of ad fraud experience, the team developed Anura as an independent software service that used the same foundation. Anura is a simple interface for advertisers to navigate, but with technology complex enough for engineers to find new threats.

With granular data and decision processes offered in real-time, Anura clients are equipped to analyze and optimize traffic sources to prevent fraudulent traffic and allow publishers and their advertisers a powerful layer of protection.

Although this engine was tested over 12 years, across billions of clicks and tens of millions of dollars in ad spend, the team had to see if Anura offered anything to the market, as there were many other products available.

They decided to do a single campaign control test. After more than a year of testing, almost $23,000 in test budgets, and more than 32,000 clicks, it was proven that Anura was a more accurate solution, and could offer better insight to traffic than what was currently available. To compare how Anura ranks against other traffic scoring solutions, testing was performed and recorded as “The Black Box Test.”

In early testing of the Anura system, the depth and breadth of the information provided on the dashboard has caused some to refer to Anura as the ‘Analytics of Fraud.’

© 2017 anura.io

THE BLACK BOX TEST

Black box testing, also known as behavioral testing, is a software testing method in which the internal structure/design/implementation of the item being tested is not known to the tester. These tests can be functional or non-functional.

OVERVIEW

Starting off as a simple test to compare Anura's engine to others, a website was built to track conversions. MouseFly.com was used to track and confirm the performance and conversions were real by visually confirming the actions and validating results.

Traffic from top tier Google, Yahoo, Facebook, and Bing was purchased and drove to the site during three separate tests that spanned a year, costing a total investment of almost $23,000 that encompassed more than 32,000 clicks. From there, Anura and its other top marketplace solutions judged the same traffic as good or bad; this way each had access to the same clicks and could be accurately compared.

HOW TRAFFIC WAS SCORED

Traffic was independently scored using each of the other top marketplace solutions' scores as well as Anura's, followed by a comparison of their scoring decisions against the true conversions to see who was most accurate. Each one looked at the click and scored the visitor. Anura found its other top marketplace solutions were mismarking good traffic as bad, and bad traffic as good and tossing out traffic that converted. Essentially they were throwing the baby out with the bath water.

TEST DURATION

To test Anura, multiple ad campaigns were run on different networks to gain access to advertising traffic. Ads were placed on premium networks to analyze how each fraud filtration system would handle the traffic.

The final test lasted five weeks, where Anura was compared to three other leading filters in the marketplace, and the results show Anura's technology was the most accurate. Imagine what Anura can do if you're not using a top-tier network? Compared to the other platforms, Anura let through more traffic. These segments of traffic that would have been blocked by other networks, converted when Anura let them through. This tells us either the other networks were getting a false positive.

© 2017 anura.io

LESS TRAFFIC REJECTED

Having a lower percentage of traffic rejected isn't a bad thing, especially when it's not blocking good traffic. Just because some traffic triggered an alarm, doesn't mean it's necessarily bad. Traffic should be blocked when it is unquestionably bad. With Anura, traffic is marked as bad ONLY when it is unquestionably bad traffic. In order to be marked as good, traffic must pass every test Anura has.

For example, some companies have a system to determine if an ad is viewed by bots or humans. However, in the recent Methbot case,[21] it has been proven bots have beaten ad viewability tests.

Let's say your home computer works great. Then you have family over, who inadvertently download malware. Now a system detects your machine is infected. It doesn't matter if you, a real user, uses the machine. The other third-party scoring systems see malware, not the user.

Are you a bot? No, but that system would automatically throw you out as bad traffic. Now that's an issue. Knowing the difference between malware and human with the most accurate solution is very important.

THIRD TEST CONTROL COMPARISON

In the most recent test, 6,105 clicks were purchased for $4,068.42, with 3,900 clicks received. Anura rejected less traffic while producing more approvals and conversions to deliver $0.19 CPA savings which calculates to 3.3% improvement.

	Anura		Control A		Control B		Control C	
Clicks Approved	3,666	96.8%	3,621	95.1%	3,518	92.4%	3,559	94.7%
Clicks Rejected	120	3.2%	185	4.9%	288	7.6%	201	5.3%
Conversions	729	18.7%	715	18.3%	684	17.5%	716	18.4%
CPA		**$5.58**		**$5.69**		**$5.95**		**$5.68**

[21] Eamon Javers, "Cyber Firms Says Russian 'Methbot' Scam Is Defrauding Digital Advertisers," Dec. 20, 2016, retrieved Feb. 7, 2017 from http://www.cnbc.com/2016/12/20/cyber-firm-says-russian-methbot-scam-is-defrauding-digital-advertisers.html

© 2017 anura.io

While the margin may seem small, the difference is huge when applied to a marketing budget. Don't believe it? On a $500,000 annual digital marketing budget in 2016, and a conversion value of just $40.00, a company could realize an increase in monthly revenue just by using Anura over the competition. Check it out for yourself:

WHAT DOES A 3.3% DIFFERENCE LOOK LIKE?

Monthly Digital Marketing Budget	$500,000
Conversion Value	$40.00
Increased Monthly Revenue Using Anura	**$118,025**

Increased Annual Revenue

$1,416,299

Metrics	Old Monthly	Using Anura New Monthly	Old Annual	Using Anura New Annual
Cost Per Acquisition	$5.77	$5.58	$5.77	$5.58
Digital Marketing Budget	$500,000	$500,000	$6,000,000	$6,000,000
# New Customers	86,655	86,606	1,039,961	1,075,269
Conversion Value	$40	$40	$40	$40
Revenue Generated	$3,466,205	$3,584,229	$41,594,454	$43,010,753
Increased Revenue Using Anura		**$118,025**		**$1,416,299**

When using Anura in place of you current ad-fraud filter; Results may vary.

With your monthly digital marketing budget of **$500,000** and a conversion value of **$40.00**, by using Anura as your ad fraud traffic solution instead of other top marketplace solutions, you'd increase top line revenue by over **$1,000,000** during the course of a year as compared to the industry's current popular offerings.[22]

As compared to all control groups, Anura didn't throw out the good traffic and produced more conversions at less cost for increased revenue. For advertisers and publishers, not only does Anura fight ad fraud, it also solves a problem (e.g. throwing away good traffic) that many may not realize was an issue before.

[22] Based on results Anura did across their controlled single campaign.

© 2017 anura.io

ANURA PERSPECTIVE

Digital advertisers and publishers must remain vigilant in the fight against ad fraud. Not only can ad fraud inflect costly damage, it can negatively impact a brand's reputation, too.

It's important to be proactive and fight ad fraud head on. Educating yourself on ad fraud and using tools like companies to filter traffic is just part of the battle. Anura realizes you should have full access to accurate data and analytics to make informed decisions for your account. With that knowledge you'll be able to better protect your customers and your bottom line.

© 2017 anura.io