What Is...

Clarifying marketing topics and terms

Simplify

VAB Insights. Inspiration. Impact.

Digital Ad Fraud

A Look Into Critical Issues Impacting Marketers Today

October 2023

Digital Ad Fraud

Untangling and simplifying marketing topics and terms

An estimated **$84.2 billion in digital advertising investment will be lost to ad fraud worldwide** during 2023 and **approximately $35 billion in North America** alone, according to Juniper Research.[1] That figure is expected to more than double by 2028, with **advertisers projected to lose upwards of $172.3 billion to ad fraud on a global scale**.[1]

Ad fraud negatively affects publishers and consumers, but it is often advertisers who are hit the hardest. The impact of ad fraud goes beyond 'wasted' ad dollars and unseen impressions delivered to bots. **Ad fraud can also create reputational, financial and legal risks for advertisers.**

These **serious business, brand and legal ramifications associated with ad fraud** within digital video campaigns amplify the value of a heightened sense of scrutiny and overarching **need for greater transparency throughout the digital advertising ecosystem.**

Digital Ad Fraud Defined:

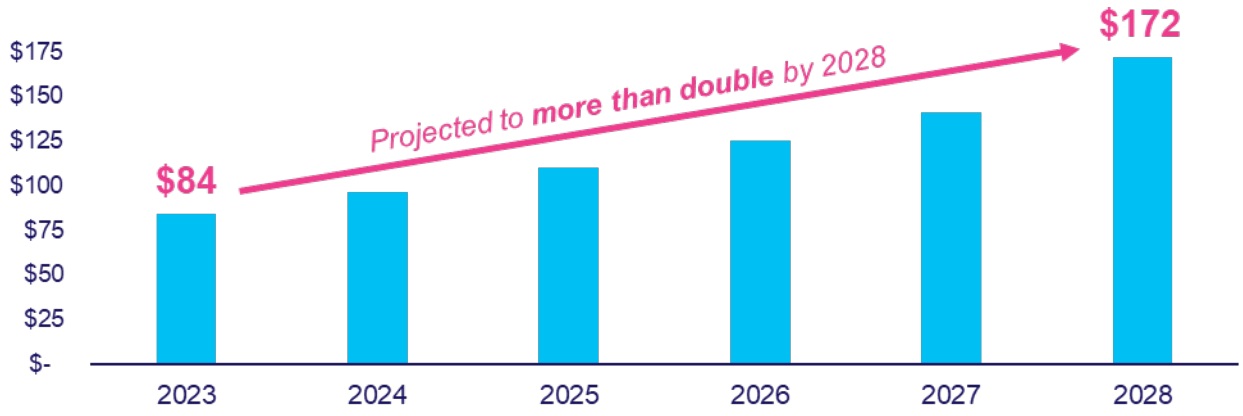
Digital Ad Fraud

Refers to an individual, group or organization maliciously and intentionally falsifying engagement with a digital advertisement, often by impersonating human behaviors or knowingly miscalculating measurement metrics. *E.G., fake clicks, overcounting users, cookie stuffing, domain spoofing, etc.*[2]

Cost of Digital Ad Fraud:

Estimated Global Cost of Digital Ad Fraud[1]

$ in Billions



What Is...

Clarifying marketing topics and terms

Simplify

Types of Fraudulent Traffic:

Invalid Ad Traffic (IVT)

Fraudulent or illegitimate website visits that artificially inflate impressions and clicks on a website.

- Includes non-human traffic (spiders, bots, etc.), accidental clicks from humans, repeated clicks from one or more users, and automated clicking tools.
- There are two types of Invalid Ad Traffic: General Invalid Traffic (GIVT) and Sophisticated Invalid traffic (SIVT).

General Invalid Traffic (GIVT)

Traffic generated from non-threatening sources such as measurement and analytics crawlers, data and brand safety bots or traffic from unknown (but real) browsers.

- Considered the least risky form of invalid traffic because while they are non-human hits to a website, they serve a purpose in the ecosystem.
- Typically, **easier to identify and filter out** with regular audits, invalid IP blocking or fraud detection partners.

Sophisticated Invalid Traffic (SIVT)

Malicious web traffic generated to click/view ads to increase ad revenue, hijack devices, manipulate location data, spoof domains, and more.

- Can include traffic from crawlers, bots and scripts that pretend to be genuine users, malware, hacker used sessions and devices as well as illegal substitute traffic.
- Presents a bigger threat as it is typically **much more difficult for fraud detection partners to identify** and requires advanced means of detection and analysis.

Online Traffic Fraud:

Over 40%

Of all online traffic is invalid

According to research from cybersecurity firm CHEQ [3]

Different Types of Bots:

An internet bot is a software application that runs automated tasks over the internet. Bots are used by both good and bad actors to automate and complete tasks.

- **Bot Attacks:** Automated attacks set up by bad actors and cyber criminals using bots that mimic and duplicate online human behavior. Bot attacks can be leveraged on thousands of websites at once and at various touchpoints including ad clicks, sign ups, logins and payments.
- **Botnet:** A collection of internet connected devices (desktops, laptops, mobile devices etc.) that have been infected and controlled with malware to enact large scale attacks and fraud.
- **Fraud Bots:** Bots that run through real devices or servers while masquerading as legitimate users by simulating tasks such as generating fake ad impressions, fake ad clicks, fake in-app engagement and even fake purchases.

What Is...

Clarifying marketing topics and terms

Simplify

Different Types of Bots (continued):

- **Spambots:** Bots that are used to inflate website traffic for the purpose of increasing page rank within a search engine.
- **Web Crawler:** An internet bot used by search engines to scan websites and index content.
    - **Related Term:** Web Spider
- **Web Scraping:** The process of using bots to copy and gather data and code from a website to store in a central database for future retrieval or analysis.
    - **Related Terms**: Web Harvesting & Web Data Extraction

Bad Bot Traffic:

From 2021 to 2022, an **increase** in **bad bot traffic** coupled with a **decrease** in **legitimate human traffic** meant the percentage of overall traffic that's bad bots increased even more rapidly[4]

102%

Increase in **bad bot traffic**[4]

28%

Decrease in **legitimate human traffic**[4]

Three Tips for Recognizing Digital Ad Fraud:

Review Site Lists

Audit your site-level reporting and look for suspicious unrecognizable sites. Fraud has a higher likelihood of coming from obscure sites.

Examine IP Address

Review IP address reporting and look for non-residential IP addresses. Fraud has a much higher likelihood of coming from Data Center IP addresses.

Analyze Key Metrics

Abnormally high or low click-through rates (CTRs), cost per action (CPA) as well as large spikes or drops in traffic, conversions, or installs can be signs of foul play and warrant further investigation.

21 Common Types of Digital Ad Fraud:

1. **Ad Laundering:** The practice of safe washing or laundering funds gained through illicit ways via digital advertising on fake sites with fake impressions.

2. **Ad Stacking:** A type of ad fraud in which multiple ads are layered or 'stacked' on top of each other in a single ad placement. Only the top ad will be visible to the user, however a click or impression is registered for every ad in the stack, leading advertisers to pay for fake impressions and/or clicks.

3. **Ads to Server, Not to Screen:** When an ad is delivered to the ad server, but not to the intended screen/audience.

4. **Affiliate Marketing Fraud:** Occurs when the 3rd party websites or individuals who are paid a commission to generate traffic or leads to the company's products or services, use fraudulent tactics to generate revenue for personal gain.

5. **Authorized Push Payment (APP) Fraud:** Occurs when a bad actor tricks someone into purchasing goods that don't exist or will never be received.

6. **Clickbait:** An advertisement designed to entice readers to click on a hyperlink which often leads to dubious content.

7. **Click Farm:** A physical location with a large amount of exploited, low-paid workers who manually click on online ads to fraudulently increase the clickthrough rate, boost engagement metrics, and inflate impressions.
    - **Related Term:** Device Farm

8. **Click Fraud:** Occurs when fake clicks target pay-per-click ads to create the illusion that a large number of potential customers are clicking the advertiser's links when in reality they are not. Click fraud is done to drive profits for the ad hosting site's revenue or to exhaust the advertiser's budget.

9. **Dark Patterns:** A user interface that "tricks" users to agree to click or do something through unclear design or terminology. Can be used by publishers to pump up figures for key advertising demographics; i.e., a prompt would appear before posting with a large blue button to agree and consent as well as an obfuscated hyperlink to decline.

9. **Domain Spoofing:** The goal of domain spoofing is to trick a user into interacting with a malicious email or a phishing website as if it were legitimate. Ad fraud perpetrators fake the name of websites they own to obscure the real source of their traffic and offer their spoofed domains for bidding by advertisers. The display ads then end up on an undesirable website instead of the website that advertisers wanted.

10. **Device Spoofing:** A tactic in which mobile or other digital devices are used to impersonate real devices to make money off false impression delivery when in reality, no ads were served to real viewers.
    - **Related Term:** Device Impersonation

11. **Fake Impressions:** The result of fraud when an ad is not viewable to the human eye, but still counted and reported as an impression.

12. **False Redirects:** Occurs when bad actors insert code into a website that sends visitors to a different website with the intention of generating advertising impressions.
    - **Related Term:** Malicious Redirect

21 Common Types of Digital Ad Fraud (continued):

13. **Geo-masking:** Technique used by fraudsters to hide or spoof the location of the clicks that they generate, allowing them to appear as genuine traffic.

14. **IP Address Spoofing:** The creation of IP packets that have a modified address in order to hide the identity of the sender, to impersonate a computer system, or both. It is often used by bad actors/cybercriminals to carry out malicious acts without detection.

15. **Malvertising**: The deployment of malicious code on a publisher's web page that targets individual users through deceptive ads, which are then unknowingly displayed to users, leading them to unsafe destinations that can risk their online security.

16. **Malicious Software (Malware):** Malwares intend to harm computers and computer users by stealing information, corrupting files or mischievous activities to annoy users.
    - **See Also:** Botnet

17. **Piracy Websites:** Websites that enable the use, download or sale of unauthorized duplications of copyrighted content. Piracy networks can be included into programmatic buys.

18. **Software Development Kit (SDK) Spoofing:** Occurs when bad actors manufacture legitimate looking installs of apps with data of real devices without the presence of any actual installs. Bad actors utilize this technique to fraudulently consume an advertiser's budget.

19. **Spam:** Fake user registrations and comments useless to a business or other readers. Can cause overloading on the website servers, as well as lead to data theft from comments, feeds and live chats, which may negatively impact brand safety.

20. **Server-Side Ad Insertion (SSAI) Spoofing:** Occurs when fraudsters set up fake SSAI servers to generate fake ad inventory across apps, IPs and devices.

21. **Website Spoofing:** Occurs when an attacker builds a website with a URL that closely resembles, or even copies, the URL of a legitimate website that a user knows and trusts. In addition to spoofing the URL, the attacker may copy the content and style of a website, complete with images and text.

Mitigating the risk of ad fraud begins with the partnerships you make

Establishing and activating direct relationships with trustworthy and premium publishers can reduce and even eliminate your risk of fraud.

Ad Fraud Detection & Specialist Firms:

As ad fraud grows each year, so does the amount of ad fraud detection companies who are working to detect and reduce fraud

FOU ANALYTICS · HUMAN · fraudlogix™ · KOCHAVA
CHEQ · mFilterIt Adding Trust to Digital · imperva · AppsFlyer

Learn more about these ad detection providers by clicking the logos above

High Profile Instances of Digital Ad Fraud:

Facebook Video: $40M Settlement (2016)

Facebook **knowingly inflated their video metrics by 150% to 900%** through falsely calculated viewership which inflated the advertiser metrics by 60% to 80%, leading to a $40 Million settlement.[5]

Methbot: $5 Million a Day Lost Through Fake Video Views (2016)

Aleksandr Zhukov, the self-proclaimed "King of Fraud", and his group of fraudsters were discovered to have been making **between $3 and $5 million a day by executing fake clicks on video advertisements**. "Methbot" was a sophisticated botnet scheme that involved defrauding brands by **enabling countless bots to watch 300 million video ads per day on over 6000 spoofed websites**.[6]

Ad Networks: $100 Million of Wasted Ad Spend by Uber on Fraud (2021)

Uber filed a lawsuit against five ad networks in 2019 – Fetch, BidMotion, Taptica, YouAppi, and AdAction Interactive – and won. Uber claimed that its ads were not converting, and ultimately **discovered that $100M of their ad budget wasn't needed because retargeting companies were abusing the system by creating fraudulent traffic**.[7]

VASTFLUX: Millions of iOS Devices Affected (2023)

A malvertising attack that injected malicious JavaScript code into digital ad creatives, allowing **fraudsters to stack numerous invisible video ad players behind one another and register ad views**. VASTFLUX accounted for more than 12 billion bid requests a day. **More than 1,700 apps and 120 publishers were spoofed, and the scheme ran inside apps on nearly 11 million devices**.[8]

Industry Perspectives:

1. "**Marketers should continue to call for third-party, MRC-accredited validation of anti-fraud on all platforms and publishers, including the big digital platforms**. Until that happens, we cannot be certain that marketers are not wasting money on fraudulent ads." – *Mark Pritchard, Proctor & Gamble's Chief Brand Officer* [9]

2. "As malicious software and bot programming gets more and more sophisticated, this number (cost of ad fraud) only stands to rise…**with the U.S. being the biggest market for ad fraudsters, the issue has now been recognized by digital media professionals as one of the major challenges facing the industry**." – *Josch Chodakowsky, ANA Senior Manager of Research and Innovation* [10]

3. "One rule we keep across all of our ad operations team is to never "set it and forget it." We leverage key insights from our custom dashboards, but **we make sure each campaign has human-powered monitoring on a daily basis. It's important for our team to look into any anomalies over historic and projected performance**. We encourage a thorough investigation into any unusual spikes in activity." – *Michael Kalman, Media Crossing Inc. Founder and CEO* [11]

Future Outlook:

As digital advertising continues to evolve, the threat of ad fraud will follow suit. **Fraudsters will continue to develop and implement a multitude of ways to defraud marketers,** putting the efficacy of their campaigns at risk. In response to the increase in ad fraud there is **a growing ad fraud detection industry,** which was valued at $2.5B globally in 2021 and is projected to reach $9.4B globally by 2031.[12]

Despite the promise of greater protection from ad fraud detection firms, it is paramount that advertisers **develop a multi-pronged digital ad fraud prevention and mitigation strategy**.

Education
Develop an approach that includes **educating and informing internal teams** on the types of digital ad fraud that exist and how they negatively impact business.

Action
Take action by closely analyzing campaigns, **demanding transparency from partners along the digital video supply chain** and partnering with high quality and independent vendors to assist you in protecting and validating the results of a campaign. Additionally, working directly with publishers can lessen the likelihood of digital ad fraud by reducing the steps in the chain and the opportunity for fraudulent practices.

Future Facing
New and exciting technologies are reshaping the advertising ecosystem. Innovations like blockchain, artificial intelligence and machine learning are currently, and will continue to play a larger role in fraud detection and prevention systems. **Research and development of new technology** will empower marketers to stay ahead of digital ad fraud.

Related Digital Advertising Terms:

- **Ad Networks:** Aggregated ad inventory from sources on the supply-side (publishers) of an ad exchange that are matched with sources on the demand-side (buyers). The two most common ways ad networks gather inventory is by collecting inventory from publisher sites, or by purchasing bulk impressions and reselling them.

- **Audience Networks:** Serve as a way to expand the reach of a digital campaign with a single publisher by using cookies to identify and track user's activity on other websites/apps and then serving ads on those 3rd party websites/apps to the same audiences using the same targeting and measurement tools.
    - **Related Term:** Audience Extension
    - **Examples**: Facebook Audience Network, Google Search Partners, Google Video Partners Network, Pangle (TikTok), LinkedIn Audience Network, Spotify Ad Network, Passport Ads (Expedia)

- **Audience Retargeting:** A digital advertising method that utilizes cookies to identify and advertise to users who have previously visited a website with the goal of driving them to return to that website.

- **Brand Compliance:** Guidelines that brands implement to ensure messaging across all channels is in line with core brand standards, values and identity.

- **Delivery Site:** Website or app on which your ad ran.

- **Digital Ad Network:** A technical platform that mediates and facilitates the sale of ad inventory between publishers and advertisers. Digital Ad Networks are an integral component of the programmatic advertising ecosystem.

- **Exclusion Lists:** A list of website domains, content owners, publishers and creators that a marketer wants to avoid sending advertisements to. Marketers use exclusion lists to avoid placing ads in spaces that are not in alignment with their brand such as those that display inappropriate content, or engage in fraudulent practices.

- **IP Address:** The unique identifying number assigned to every device connected to the internet.
    - **Residential IP Address:** an address that is assigned from an ISP to a homeowner and is associated with a single owner and location
    - **Datacenter IP Address:** an address that isn't owned by an ISP and not associated with a homeowner. Often connected to a cloud service provider and assigned to a datacenter.

- **IP Packet:** Unit of data used for transmitting data across computer networks that includes the sender's IP address, the recipient's IP address, and other information. Sending and receiving IP packets is the primary way in which networked computers and other devices communicate.

- **Inclusion List:** A list of website domains, content owners, publishers and creators that a marketer wants to send advertisements to. Marketers use inclusion lists to ensure their ads run in spaces that align with their brand.

- **Keyword Blocking:** A list of keywords that prevents your ads from running alongside and within content that contains those specific words; i.e., during coronavirus pandemic, ads we're being removed from news sites because the word "virus" was included in the article.
    - **Related Term:** Blocklist

Related Digital Advertising Terms (continued):

- **Made for Advertising (MFA) Websites:** Websites that operate with the sole purpose of maximizing ad profits, leaving the actual content and user experience as afterthoughts. They are often filled with spam, clickbait, and stolen content. By industry standards, MFAs do not meet the criteria for invalid traffic (IVT) and are therefore still prevalent in the digital ecosystem.
- **Measured Ads:** Ads where a Javascript tag successfully measured the impression and reported back to the ad servers.
- **Media Transparency:** The ability for marketers to see accurate, recent and robust data on where their media investments were placed, when they were placed and for how much it was bought for. To achieve full transparency marketers should have a clear view of the entire supply chain.
- **Secure Sockets Layer (SSL) Certificate:** A type of encryption used by websites to secure online transactions and keep customer information private and secure. Almost all legitimate websites have an SSL certificate.

Interested in understanding the path of digital ad investments?

Download ***'What Is...The Digital Video Supply Chain'*** below to learn more about the complexities and challenges involved with this ecosystem and the five ways marketers can best navigate it.

Click the cover above to download

What Is...

Clarifying marketing topics and terms

Simplify

VAB Insights. Inspiration. Impact.

Want to learn more?

Click on the images below for the content

Looking for industry terminology? VAB's advertising glossaries cover topics like AI & Machine Learning, Web3, audience-based buying, video measurement, streaming and data.

About VAB

VAB plays a dual role in the video advertising industry. We are leading the change to bring about a more innovative and transparent marketplace. We also provide the insights and thought leadership that enables marketers to develop business-driving marketing strategies.

Drawing on our marketing expertise, we **simplify** the complexities in our industry and **discover** new insights that **transform** the way marketers look at their media strategy.

We are committed to your business growth and proud to offer VAB members, brand marketers and agencies ***complimentary access*** to our continuously-growing Insights library. **Get immediate access** at **theVAB.com.**

Sources

1. Juniper Research, *Quantifying the Cost of Ad Fraud: 2023-2028*, 9/26/2023.
2. HUMAN, *How to Succeed in Ad Fraud by Really Trying*, 1/2/2020.
3. CHEQ, *The State of Fake Traffic 2023*, 3/16/2023.
4. HUMAN Security, *2023 Enterprise Bot Fraud Benchmark*, April 2023.
5. CNBC, *'Facebook knew ad metrics were inflated, but ignored the problem to make more money, lawsuit claims'*, 2/18/2021.
6. HUMAN, *Methbot: Then and Now'*, 7/1/2021.
7. Veracity Trust Network, '*How could Uber cut its ad spend by $100m and see no drop in conversion?'*, 1/7/2021.
8. HUMAN, *'HUMAN Orchestrates Unprecedented Private Takedown', VASTFLUX,* 1/19/2023.
9. Journal of Marketing (Volume 85, Issue 1), *Mark Pritchard Commentary: "Half My Digital Advertising Is Wasted…",* January 2021.
10. Inside Radio, *'Ad Fraud Costing Marketers Over $100 Billion, ANA Report Says',* 6/6/2022.
11. Forbes, *'How To Recognize And Combat Ad Fraud: 10 Best Tips' ,* 10/7/2020.
12. Global Insights Services*, Ad Fraud Detection Tools Market Analysis and Forecast to 2031,* August 2022.

Definition Resources (reference pieces used in the development of several definitions)

- AppsFlyer, *Ad Network Glossary: What is an ad network?,* Retrieved 8/21/2023.
- CHEQ, *Everything You Need to Know About Click Farms,* 3/6/2023.
- CyberNews, *Malvertising: what you need to know to prevent it,* 12/29/2022.
- FTC, *Bringing Dark Patterns to Light,* 2022.
- FTC, *How To Recognize, Remove, and Avoid Malware*, May 2021.
- DataDome, *Ad Fraud: What it is, How it Works, & 13 Common Types,* 9/7/2022.
- Publift, *Ad Fraud: Everything You Need to Know*, 7/23/2023.
- LearnHub, *What is Ad Fraud? How to Strategize and Decrease Risk Factors, 12/2/2022.*
- Singular, *Ad Fraud Glossary*, 2022.
- SemRush, *The Ultimate Guide to Redirects: URL Redirections Explained,* 11/7/2022.
- Oracle Moat, *The history of online ad fraud and what you can do about it*, 6/29/2022.
- MRC, *Invalid Traffic Detection and Filtration Standards Addendum*, June 2020.
- Novatiq, *Digital ad fraud statistics that every brand should know*, 5/11/2023.
- IAS, *The Flavors of Ad Fraid: GIVT vs. SIVT*, 12/20/2017.
- Kaspersky, *What are Bots?,* Retrieved 8/21/2023.
- HUMAN, What is Invalid Traffic, Retrieved 8/24/2023.