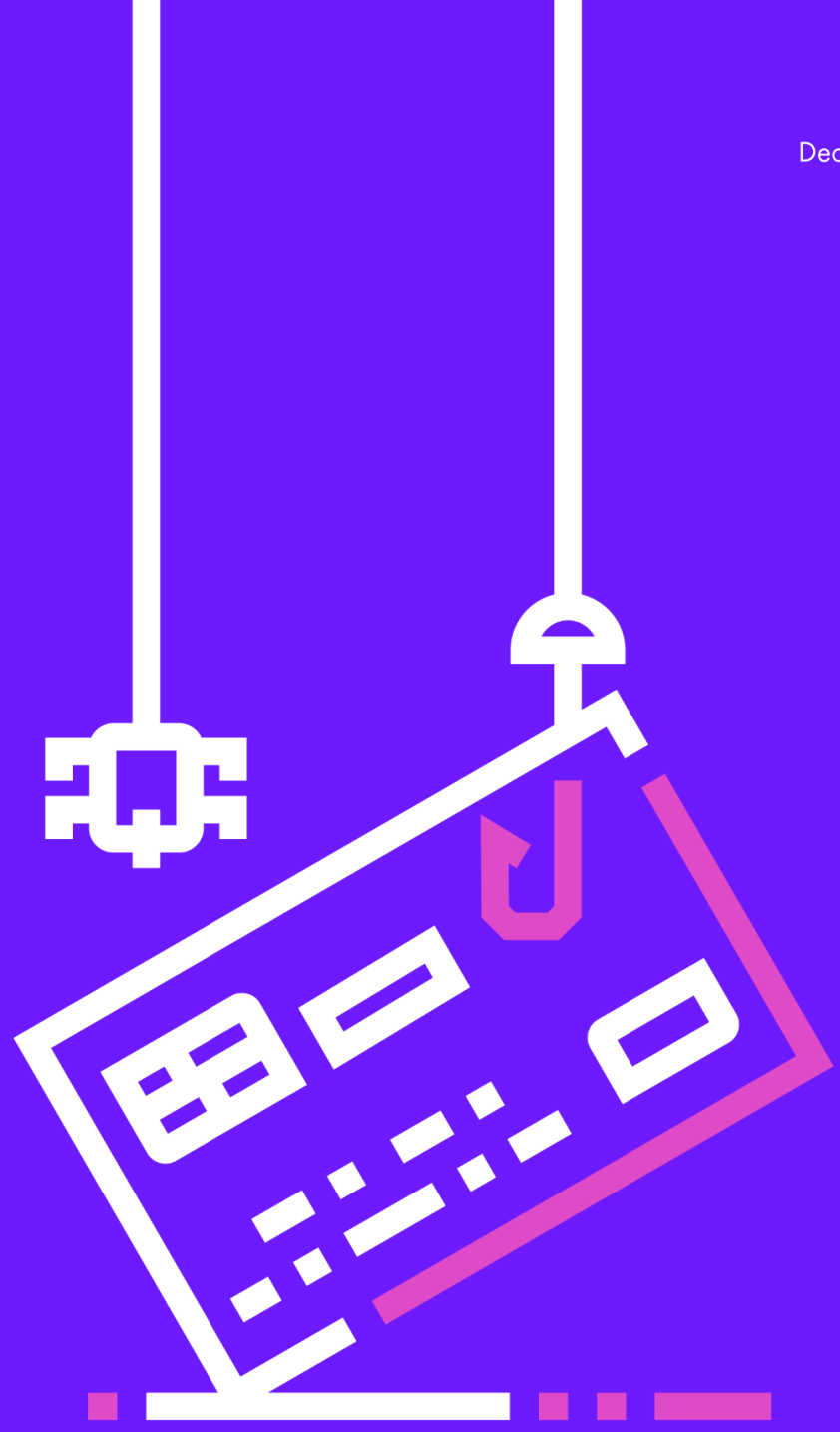
iab europe

December 2020



THE IAB EUROPE GUIDE TO AD FRAUD

iabportugal.net

iab portugal
interactive advertising bureau

Contents

Section 1. Introduction

According to the World Federation of Advertisers (WFA), it is estimated that by 2025, over $50 billion will be wasted annually on ad fraud. As advertising spend continues to shift to digital media, ad fraud has proven to appear in many different forms: bots, pixel stuffing, malicious apps, and more. Ad fraud has evolved in such a way that it can impact every element of digital advertising. Even though it is pervasive, there continues to be general confusion around how detrimental ad fraud is for the digital advertising ecosystem.

To make digital campaigns successful, marketers need to ensure their ad spend is being used to reach real people. But, whether we like it or not, ad fraud exists in the digital ecosystem. Digital ad fraud is any deliberate activity that prevents the proper delivery of ads to the intended audience, in the intended place. Most commonly taking the form of bots, or domain spoofing, ad fraud thrives by siphoning off money from advertising transactions. It can come in many forms, pretending to be humans browsing the internet or falsely representing low quality inventory as high quality, are some of the more common occurrences.

So, where are we at right now with ad fraud, why has it not been resolved, and what action can we all take to help stop it?

Considering brands in Europe are spending around €4.7 billion on digital advertising, understandably they want to know their significant investment in digital is not going to waste. Fraudsters, however, have a slightly different idea. According to IAB Europe, €3.1 billion was spent on display ads in 2019. Considering that fraud hovers around the 1% mark even when campaigns are optimised, we can estimate at least €31 million of that European ad spend was potentially intercepted by fraudsters.

Fraud fluctuates depending on the country and the device. Integral Ad Science (IAS) found from its H1 2020 Media Quality Report that fraud fluctuated from 0.4% - 11.7% depending on whether buyers implement an ad fraud prevention or detection strategy. Unsurprisingly, campaigns that do not utilise any ad fraud mitigation strategy attract the most fraud globally.

Ad fraud is a problem that shows little sign of disappearing any time soon, but there are ways you can help the industry to beat the bots.

This guide is intended to our define specific types of fraud in our industry and outline how companies like DoubleVerify (DV), IAS and Oracle Data Cloud work to combat new and emerging types of ad fraud across all channels, helping to drive media quality and effectiveness.

Section 2. Demystifying Ad Fraud – What it is and How it Happens

2.1 What it is

Ad fraud, also referred to as invalid traffic (IVT), is the fraudulent representation of online advertising impressions, clicks, conversions, or data events, in order to generate revenue. These activities manipulate delivery channels, significantly impacting an advertiser's return on media investment, often jeopardising brand reputation.

Fraud usually presents itself in three ways:

1. Site Fraud occurs on a website including, but not limited to, indications of impression laundering, hidden ads and non-human traffic.

Examples include:

- **Impression Laundering.** Domain spoofing fraud (also known as ad impression laundering) is often challenging to detect and prevent. It is also one of the most lucrative types of fraud to perpetrate. With a simple line of code, fraudsters can change the URL of a site to make advertisers think lower quality sites (e.g., copyright infringement, gambling, pornography etc.) are reputable publishers.

- **Stacked and Hidden Ads.** Ads that are either layered on top of each other or difficult/impossible to view.

- **Traffic Acquisition Manipulation.** Publishers utilise and pay-out fraudulent traffic drivers to increase visitor volume — often unaware that the traffic is non-human.

2. App Fraud, occurs on mobile, tablet or CTV devices and is broken down into these known schemes:

- **Spoofed Apps.** Intentional misrepresentation of the app's BundleID to trick advertisers into spending money on low-quality or non-brand safe placements.

- **Hidden Ads.** Ads that run unbeknownst to the user while the app is open or in active use.

- **Background Apps.** Ads loaded when the app is not active or being used.

- **Measurement Manipulation.** Apps that engage in automated browsing and/or invalid manipulated incentivised activity.

3. Device Fraud, like Bots and Hijacked Devices, it manifests in a number of different ways:

- An automated browser instance that can visit websites, get served ads and perform simple actions like clicking on ads or mimicking humans.
- Impressions that are served to a fraudulent, non-human requestor.
- Impersonating a user to manipulate ad serving and inflate the amount of ads served to a domain.

Before advertisers can identify and prevent fraud, they first need to recognise the way in which it is reported.

2.2 Invalid traffic (IVT)

Ad fraud is often referred to as invalid traffic (IVT). Invalid traffic is a broad term describing online activity that does not always come from a real user, therefore the impressions do not represent legitimate advertising consumption. IVT generates actions that take away from the proper delivery of an ad and it can impact every type of advertising — display, video, mobile, audio, search, and social. The landscape of fraud is always evolving and can impact all players in the ecosystem — even the most premium publishers. Every traffic source requires constant re-evaluation. Since the term IVT refers to both unsophisticated and sophisticated, the Media Rating Council (MRC) decided to create two sub-categories, General Invalid Traffic (GIVT) and Sophisticated Invalid Traffic (SIVT), to distinguish between the two.

General invalid traffic (GIVT)

The Media Rating Council (MRC) definition of GIVT is invalid traffic that can be identified through routine means of filtration, executed by using lists or other standardised checks.

Types of GIVT:

- IAB bots/spiders
- Unknown browsers
- Known fraud sites

- Known data-centre traffic
- Activity-based filtration

Sophisticated invalid traffic (SIVT)

The Media Rating Council (MRC) definition of SIVT is invalid traffic that is more difficult to detect, requiring advanced analytics, multi-point collaboration, and/or significant human intervention in order to identify.

Key examples:

- Non-human data-centre traffic - impressions that originate from facilities used to house computer and server systems.

- Injected ads - a technique by which ads are surreptitiously inserted into web pages without getting the permission of site owners or paying them.

- Hijacked devices - calls that are unknown to the user, such as opening a hyphen browser and clicking on ads.

- Emulators - impressions that appear to be coming from mobile devices, but are not.

While GIVT includes neutral and fraudulent activity, SIVT represents activity that is intentionally fraudulent. The aim is to generate fraudulent revenue by mimicking human traffic in order to evade detection. For this form of invalid traffic, it is best to employ third-party providers with dedicated resources that can be as responsive as the bad actors themselves.

2.3 How it Happens

The aim of advertising is to deliver the right message to the right person in the right environment. Fraudsters use various techniques to compromise all of these three core values across various platforms and devices, resulting in wasted advertiser spend and damaged reputations for susceptible publishers. Below are the top 10 most common types of fraud detected.

1 - BOTS

Short for robots, bots are software programmed to intentionally view ads, watch videos, click on ads, and will be used as a tactic to siphon off money from advertising

transactions. Malicious bots are becoming more sophisticated; they are even forming networks, with each running one or more bots. The recently discovered 404bot fraud operation is a prime example of this.

These bots are viruses that can be installed unknowingly on a computer and then use computer resources in an unnoticeable way. Most people with infected computers are completely unaware.

Bot traffic is a useful tool for fraudsters as it is hard for the industry to identify who is behind this traffic.

2 - DOMAIN SPOOFING

Domain spoofing is a form of fraud where a fraudster impersonates a company's domain in order to pass off low quality inventory as high quality. Fraudsters fool buyers into thinking their ad is going to a premium site, when in reality it's going to a low-quality website. The impressions and the users are real, but the inventory is falsely represented and therefore purchased at a much higher cost.

Domain spoofing is also commonly used to mask unsafe sites. Brand safety is a huge concern to advertisers, and fraudsters take advantage by spoofing the domains of sites, like video piracy sites, in order to conceal their real identity and monetise the traffic.

Domain spoofing falls into four main categories, two of which are fairly simple and two of which are more sophisticated:

Simple Domain Spoofing - Cross-domain embedding

Fraudsters pair together two sites, one with high traffic and low quality content and another with low traffic and totally safe content. Using a custom IFrame they are able to open an ad-sized version of the safe site within the unsafe site, exposing the ad to that site's higher traffic volume. This tactic is favoured by publishers who own sites containing unfavourable material like pornography, fake news, or hate speech communities, all of which can attract large amounts of traffic but are difficult to monetise with traditional brands. Operators either partner with low-traffic sites in a profit sharing arrangement or simply operate the low-traffic site themselves as a front.

Complex Domain Spoofing - Custom Browsers

Using a custom browser, bots can visit any site on the internet, including sites that aren't reachable using commercial browsers. These bots can make the URL of the site that a user is visiting appear to be a different, seemingly premium site. So when an ad reads the URL from the browser it will be served on, it reports back the spoofed URL.

Complex Domain Spoofing - Human Browsers

This type of domain spoofing is similar to common forms of adware. When a human browser visits a premium site on an infected machine, malware will inject an ad inside the page. Operators of premium sites aren't paid for these injected ads. Instead, fraudsters collect the revenue.

3 - PIXEL STUFFING

Serving one or more ads, or an entire ad-supported site, in a single 1x1 pixel frame so ads are invisible to the naked eye.

4 - AD STACKING

Placing multiple ads on top of each other in a single placement, with only the top ad being viewable. The advertiser is paying for impressions even if the user is not seeing the ads.

5 - LOCATION FRAUD

Advertisers pay a premium for their ad to be served in a particular region, but fraudsters will send false location information so the ad actually serves elsewhere. For example, users might be surfing the web on their mobile device in New York City, and see ads for last minute tours of Alcatraz, California nearly 3,000 miles away.

6 - COOKIE STUFFING

Cookies are a method of tracking user behaviour, to help determine what advertising effort led to a conversion (click, purchase, etc.) or what a user's interests are.

Cookie stuffing can happen in many different ways. Fraudsters may try to game attribution models by adding a cookie to a user from an entirely different website from the one that the user originally visited. If the user later converts, the website associated with the stuffed cookie gets credit — and gets paid — for that action.

Cookie stuffing can also refers to the practice of placing many cookies on a bot so that they get targeted at higher CPMs, even if they haven't been flagged as potential high-value consumers.

7 - USER AGENT SPOOFING

Every request for a web page is sent with a "header" that provides some basic information about where the page is being loaded. One such piece of information is a description of the browser: its type, version, operating system, even plug-ins.

In user-agent spoofing, this description is modified to obfuscate information about the browser being used, which can interfere with user targeting. It's most often used by bots trying to hide their tracks.

While bots can still wreak havoc on the mobile platform, the more prominent type of mobile fraud involves hiding ads in services or apps running constantly in the background. Location spoofing and app-name spoofing are other costly forms of mobile fraud.

8 - MALICIOUS APPS

Apps that generate fraudulent impressions without the user knowing. This can be thought of as a kind of mobile malware.

9 – CLOUD HOSTING

In-app impressions are displayed on devices hosted in the cloud, generating ad revenue for the app creators. Fraudsters are able to control and change signals such as device ID and geo-location, making it appear as though there are a variety of different devices and therefore users, while in reality there is one hijacked device in the cloud.

10 – APP NAME SPOOFING

Similar to domain spoofing in display, apps can submit a false app identifier to the bidding platform. This interferes with detection of apps utilising background services to load ads, as well as brand safety and contextual targeting.

2.4 Fraud on Connected TV

Whilst it may be early days for connected TV (CTV), CTV represents one of the fastest growing content consumption channels in Europe. In fact, Connected TV viewership has grown to reach 50% of households (representing 61.5 million households) in Europe's five biggest markets, according to a SpotX report. Unfortunately, the popularity of the platform attracts fraud. It is clear however, that certain types of fraud are not possible in this environment. For example, cookies and clicks are not supported in a CTV environment. CTV fraud scenarios include bots, device spoofing (where devices are obfuscating their attributes to maraud as legitimate), browser spoofing, and malicious CTV apps. This fraud is split into four main categories:

- **Spoofing:** Fraudsters may buy lower-price mobile or desktop display inventory for less than a $1 CPM, change the ad calls to resemble premium CTV video inventory, and resell the inventory at CPMs frequently greater than $20.

- **Fraudulent apps:** Fraudsters can easily create their own CTV apps and release them to both open and closed app stores. Hundreds of apps are out there with few downloads, but millions of impressions. Some fraudsters create ostensibly legitimate tech tools that they offer to app creators; these tools are then used as a "trojan horse" that allows them to commit fraud - all unbeknownst to the app developer.

- **SSAI fraud:** Server-side Ad Insertion (SSAI) technology has some amazing benefits - like reducing latency, thereby speeding up delivery and improving the viewing experience. Unfortunately, it can be leveraged to generate fraud at scale. Fraudsters can either create their own servers or buy into cloud space to completely falsify the information about an impression opportunity (app/IP/device/etc.) and generate completely fake traffic. Imagine millions or billions of impressions firing off from a server farm. And because measurement doesn't happen directly on the CTV device, but at the server level, it can be even more challenging to detect.

- **Bot Fraud:** As on other devices, bot fraud occurs when impressions are served to a fraudulent, non-human requestor. Often, bots will target CTV inventory by spoofing the device type to appear as if they are a CTV device.

Section 3. The Importance of Ad Fraud Detection

For advertising to perform, it must be seen by real people. As we know, fraud follows the money. Without ad fraud detection, the impact of fraud can be significant as a brand's advertising efforts are wasted on non-humans.

Fraudulent and invalid traffic are highly prevalent in the online advertising ecosystem, which causes significant negative impact, including:

- Lost revenue for advertisers; decreased yield for publishers.
- Questionable measurement metrics.
- Negative brand association — specifically related to criminal enterprise, malware, poor consumer experience and environments out of alignment with brand positioning.
- Poor consumer experience, making solutions like ad blockers even more attractive.
- Overall lack of trust.

Right now, ad fraud accounts for one out of every three dollars spent by digital advertisers – and unless a dramatic change is made, Forrester predicts that the industry stands to lose $10.9 billion from fraudulent advertising.

Whether malicious or not, as we've shown, undetected IVT can devalue performance metrics, or worse, deplete budgets for which marketing organisations often fight so hard.

It's critical to protect campaigns from invalid traffic, whether it's a known spider providing a useful service or a nefarious ad fraud criminal network impacting publishers, advertisers, and consumers. Thwarting criminal enterprises that benefit from the anonymity of the web and the complexity of our digital ad ecosystem is imperative.

This means that fraud detection and prevention tools must be even more sophisticated, focusing on three key tenets: coverage, speed and accuracy. Furthermore, these tools need to be applied across all media, platforms, devices and fraud types.

Section 4. Ad Fraud Detection Methods

As the industry develops advanced technologies to detect hazardous activity, fraudsters continue to learn how to better replicate user behaviour.

Attempts to tackle ad fraud issues have made progress on the industry level, particularly with the Trustworthy Accountability Group's (TAG) Certified Against Fraud initiative. The guidelines strongly recommend publishers to adopt the ads.txt specification and independent validation requirements. This increases transparency and the ability to reduce ad fraud. In fact, when all components within the ad purchasing cycle are TAG compliant, invalid traffic (IVT) rates for display are 94% lower than the industry average. While positive, such programmes don't resolve the challenge of establishing whether entities are reputable or not, or prevent the continued growth of ad fraud operations: now large enough to gain the FBI's attention.

What's needed is a greater understanding of how best to measure ad fraud across multiple media platforms so that resources can be directed to address the real problem.

4.1 The Importance of Rapid Detection

When detecting fraud, it is extremely important to rapidly identify newly infected devices, since a significant portion of the fraudulent traffic they would generate (as bots and/or hijacked devices) occur within the first 48 hours after the device has been infected.

To facilitate rapid detection, verification providers often use machine-learning models that are fed a verified set of known fraudulent patterns curated by a team of data scientists that are used to "train" their models. The automated models then assess risk for every device, impression and app/site observed online to rapidly identify new infections.

Using this AI-based approach, data scientists can flag new device-signatures per day, with high levels of accuracy and industry-leading low levels of false positives. This approach complements a purely deterministic methodology to identify instances of fraud, resulting in a robust and comprehensive solution — and a definitive "Yes/No" output to fraud identification.

4.2 The Stages of Ad Fraud Prevention

Stage one of improving ad fraud protection is **defining where current methods fall short.** Take exclusion listing. On the surface, this seems like an efficient approach: sites with fraudulent history are added to a list of no-go areas, and advertisers stay safe through avoidance. But it has limitations. Not only are lists updated infrequently — for example, rogue publishers can reappear under a new URL — but they also restrict scale. Even premium sites can fall victim to ad fraud, and removing them as a supply channel can mean cutting off valuable inventory, as well as impact funding for quality content. Moreover, exclusion lists don't actually determine if ad fraud is present: they only show sites it has affected in the past.

Stage two is **recognising which techniques should be applied.** At a basic level there is robust vetting — checking that trading partners have the TAG or media ratings council (MRC) anti-fraud seal of approval — and adjusting key performance indicators (KPIs) to minimise risk. For example, replacing metrics that are easy to fake, such as high clicks at low cost, for KPIs linked to specific business goals, including sales and possibly other types of conversions.

4.3 Ad Detection Methodology by Fraud Type

For GIVT, identification is based on industry-wide supplied lists of known bots and spiders, known fraudulent sites, unknown browsers and known data centres.

For bot fraud, a deterministic approach to detection is both fast and accurate. Deterministic data improves business results by taking an empirical "Yes/No" approach based on granular data. This conclusively eliminates fraudulent inventory and maximises return on investment. In contrast, probabilistic data tracking infers the likelihood of an outcome based on observed past patterns, resulting in flawed data and suboptimal decisioning. This approach can only assign a probability that any given impression meets customer-specified quality standards. New bots generally live on average for 72 hours and produce the highest amount of fraudulent impressions within the first 24 hours. So speed, and a definitive understanding of what is and is not fraudulent, is critical.

For site fraud/IVT and app fraud/IVT, verification providers use automated algorithms to identify potentially fraudulent sites and apps. Data scientists analyse these sites and apps using a highly accurate, heuristic model with multiple empirical, technical and non-technical data points to determine whether any of the sites or apps have consistent evidence of significant amounts of non-human activity or alternative forms of impression manipulation.

In addition to automated review, data scientists also review publisher ownership records, privacy policies and other documentation to see if there are indicators that a publication is fraudulent. Following automated and manual reviews - if evidence of fraud is discovered - investigators assign the site fraud/IVT attribute to the site or app.

For adware/malware, such as hijacked devices (including mobile hijacked devices) or injected ads, verification providers use sophisticated real-time signal processing within the browser environment to identify injected adware/malware impressions at scale across their blocking and monitoring services. This is done by leveraging machine-learning technology, serving-chain and fraud analysis to isolate the signatures associated with malware/adware-served impressions.

For non-human data-centre traffic, providers will capture the IP address of the user to whom the ad was served and compare it with a list of data centres generating non-human traffic – which is created and maintained by third-party sources together with proprietary internal algorithms.

For fraud on CTV, verification providers work with buyers, sellers and the platforms inbetween to eliminate fraudulent traffic from the ecosystem. Once again, a team of data scientists is required to carefully evaluate and identify ad fraud in CTV. At any given time, this team may be monitoring hundreds of data points on every impression – analysing traffic patterns and leveraging human-tuned algorithms to identify anomalies across different devices and media types.

4.4 Selecting a Fraud Detection Vendor

As fraud techniques advance, the digital industry needs more **sophisticated fraud detection**. At a more advanced level, buyers and sellers must implement granular measurement that enables them to quickly isolate and prevent ad fraud. A layered approach to detection is vital and the most robust solutions to fight ad fraud are those that can combine rules-based methods that evaluate at the impression level, along with machine learning that can identify likely fraud patterns.

Rules-based methods:

- Catches obvious scenarios
- Requires manual work to capture all possible rules and exceptions to rules
- Human, biased, generalisation of the ecosystem
- Inflexible (cannot recognize risk beyond predetermined rules)

AI/Machine Learning techniques:

- Detects subtle patterns in data automatic detection
- Learns from data to adapt to the ecosystem
- Highly flexible (can adapt to subtle cases)

The most basic detections involve simple filtration of known spiders and bots as well as detecting traffic originating from a data centre. Your partner should always be researching suspicious activity and thinking about things like:

- Who could be profiting from this?
- Could this be a mistake in our detection or a messed-up integration?
- Who could tell us more about it?
- Do we have enough information to share with authorities?
- What is the best way to filter this as IVT?
- Can we catch it in more ways than one?
- What is the impact to our clients? What broader impact do we think is likely?

4.5 Top Tips to Prevent Ad Fraud in your Next Campaign

Optimised-against-fraud campaigns in Western Europe are 10 times less likely to be exposed to fraud than those lacking protection. The argument to put ad fraud prevention technology in place is quite simply, undeniable. Here are our top 10 tips to successfully prevent fraud in your next campaign:

1. Buy on a pre-vetted and fully transparent inclusion list of apps and domains, which is regularly updated.

2. Invest in quality content. It is usually a proxy for low fraud and low brand safety risk.

3. Continuously optimise your supply path and take the shortest route to the publisher.

4. Choose good partners who have a strong reputation for quality, who understand how critical good supply quality is for buyers.

5. Work with partners who value creating quality content and/or technical solutions.

6. Understand who your partners are: do they build content or innovative technology, or focus on monetising new technologies or opportunities without adding value to the ecosystem.

7. Vet your vendors and partners; ask how they measure for malicious bots and other forms of IVT.

8. Work with partners that help you limit the number of hops in your supply chain — every additional hop is another opportunity for IVT (or simple error).

9. Use verification and fraud solutions that can confirm ads were delivered to the desired sites, devices, and geographies.

10. Use fraud solutions that have been MRC accredited for both General and Sophisticated IVT. When choosing solutions pay attention in which environments they can operate, and which technologies they are interoperable with.

11. Measure fraud across all campaigns to understand anti-fraud performance.

12. Use industry standards for quality, and insist that your partners do too. ads.txt, app-ads.txt, sellers.json, and Supply Chain Object are major practices everyone should try to follow.

13. Offer and demand full transparency into inventory and traffic, including sourced traffic and audience extension.

14. Implement blocking technology or use anti-targeting technology like pre-bid filtering to avoid infected machines or pages with historically high fraud levels.

15. Put legal protection in place that guarantees fraud refund from your suppliers.

16. Where needed use exclusion lists. If it's too good to be true, it probably is. Focus less on low CPMs and more on hitting real KPIs tailored to your campaign goals.

5. Summary

As advertising budgets continue to shift to digital media, ad fraud remains one of the biggest hurdles that the Digital Advertising industry has to overcome. And it shows little to no sign of disappearing any time soon. However, thanks to the wide advances in verification tools and machine-learning technology capabilities, our industry is poised to tackle this ever growing monster.

Giving advertisers full confidence in their media investments is vital, and ad fraud prevention is crucial to achieving this goal. As such, this guide draws on some of the key considerations to help the Digital Advertising industry overcome the issues associated with ad fraud. It focuses on the importance of rapid detection and serves as a call to action to the industry to follow best practices to tackle ad fraud. By actively working together as an industry we are able to educate, and build solutions that limit the influence of fraud across all channels, formats and devices.

IAB Europe continues to work with its members to bring insight into key subjects, such as Ad Fraud, as we look to build a sustainable future for digital advertising together.

Testimonials

Publicis on the Importance of Ad Fraud Detection

"Publicis Media agrees with and supports the industry's best practices to prevent Ad Fraud, which mandate that marketers should work with at least one verification provider and TAG-accredited partners; take advantage of tools like ads.txt and app-ads.txt; and stay up-to-date on potential threats in new channels that may not be addressed yet by verification providers. A large part of what we do at Publicis Media is work with the larger industry to influence and drive change that better protects advertisers. Our commitment to industry collaboration, coupled with our Publicis Verified technology, helps ensure advertisers have the best possible protections against ad fraud."

Diana Romero, Manger, Digital Standards and Partnerships, Publicis Media Exchange

Integral Ad Science (IAS) on the Importance of the Guide to Tackle Ad Fraud

"The fight against ad fraud is ongoing and ever-changing. As fraudsters become more sophisticated, it is imperative that advertisers and publishers ramp up their fraud prevention technologies to stay one step ahead. Integral Ad Science welcomes collaborative, industry-wide efforts to combat ad fraud and is proud to be a part of this IAB industry guide, alongside key partners. The guide serves as a vital resource to understand the numerous forms of ad fraud, its challenges, and provides actionable solutions to the digital advertising community."

Nick Morley, Managing Director EMEA, Integral Ad Science (IAS)

Oracle Data Cloud on the Importance of Choosing the Right Partner to Tackle Ad Fraud

"Oracle Data Cloud is committed to both educating the industry through initiatives like this collaborative paper, and providing sophisticated ad fraud solutions to arm marketers against known and future threats. We're proud to work with IAB Europe on this piece, and hope it serves to jumpstart conversations around the various types of ad fraud, the solutions available today, and the importance of choosing the right partner to fight this battle."

Mark Kopera, Head of Product for Moat by Oracle Data Cloud

Contributors

IAB Europe would like to thank the following contributors who helped to author this Guide:

Nick Morley, Managing Director EMEA, Integral Ad Science (IAS)

Livia Shlesman, Sr. Marketing Manager, Integral Ad Science (IAS)

Roy Rosenfeld, SVP of Product, DoubleVerfiy

Mark Kopera, Head of Product for Moat Analytics, Oracle Data Cloud

Stevan Randjelovic, Director, Brand Safety and Digital Risk, Group M

Lisa Kalyuzhny, Senior Director, Advertising Solutions, Pubmatic

Maria Shcheglakova, Marketing Director, EMEA, Pubmatic

Tom Burns, Director, Digital Astandards and Partnerships, Publicis Media Exchange

Diana Romero, Manager, Digital Standards and Partnerships, Publicis Media Exchange

Krzysztof Madejski, IT Director of the Digitization of Gazeta Wyborcza, Agora S.A. on behalf of IAB Poland

Lauren Wakefield
Marketing & Industry Programmes Director
wakefield@iabeurope.eu

Helen Mussard
Marketing & Industry Strategy Director
mussard@iabeurope.eu

iab europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium

@iabeurope

/iab-europe

iabeurope.eu