3 Truths That Help Confront the Digital Ad Fraud Crisis

Alliance for Audited Media

TRANSACT WITH TRUST

Digital advertising fraud truly is a huge industry problem. Fraud estimates range from $6 billion to $42 billion annually, and the current supply chain structure makes it easy and attractive to commit ad fraud with little chance of retribution. Marketers, agencies, publishers and technology suppliers are frustrated. Trust is at an all-time low. The industry is nearing crisis stage as marketers are seriously questioning, rethinking and redoing their digital investments.

Ad fraud is a confusing topic because it is technically complicated and certain underlying issues have not been openly discussed. As an independent auditor, the Alliance for Audited Media sees the underbelly of the media supply chain where little transparency exists. This paper addresses key issues and illuminates **three truths to confront the ad fraud crisis:**

By looking deeper into each of these topics and the business of fraud—how the money is made and how it leaves the ecosystem—it's clear that ad fraud is conquerable. The war on fraud is winnable. Marketers can steer their budgets away from fraudulent sites to legitimate sites with verified human audiences, but the way marketers buy digital audiences must change. The entire supply chain needs to take steps to change how it operates. **The way the entire supply chain operates must change.**

Truth #1:
Ad Fraud Occurs on both Fake and Legitimate Websites

Ad fraud occurs in two primary places: **on fake and legitimate websites**.

Fake-Site Fraud

Marketers' ads are placed on fraudulent websites with content that is pirated, fake or non-existent, and displayed to bots.

This occurs when the fraudster creates a bogus website, plugs into programmatic exchanges, buys traffic for the site, sells and displays the ad impressions, and collects the money for doing so. The fraudster steals ad dollars that were supposed to go to real publishers—just like counterfeit handbags or watches take the dollars meant for legitimate brands.

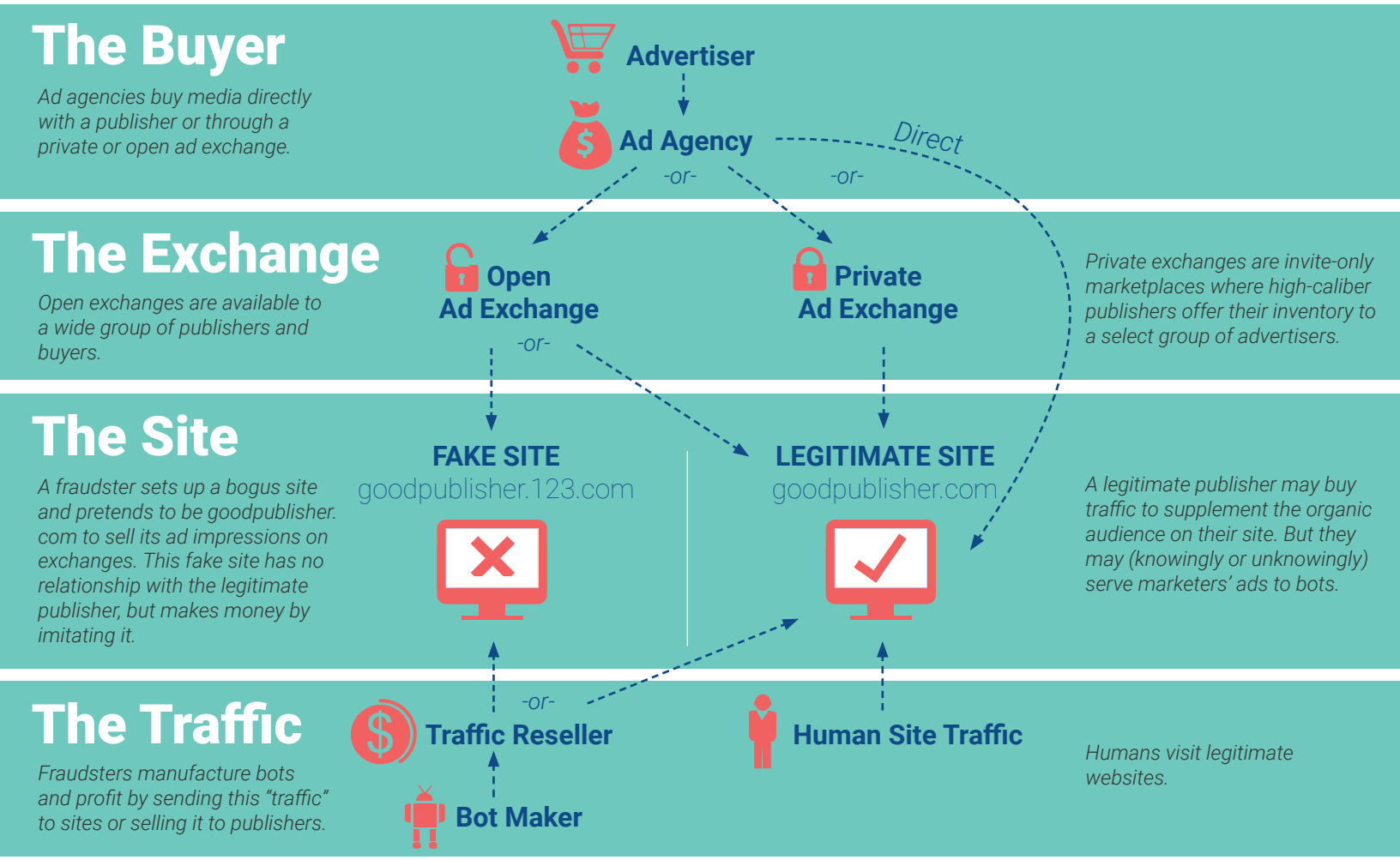
Legitimate-Site Fraud

Marketers' ads are placed on legitimate websites with real content and displayed to bots.

This occurs most often when a legitimate publisher's organic audience is supplemented with third-party traffic to fulfill demand. Often this is completed through the purchase of traffic that may appear to be human but is in fact illegitimate bot traffic. This practice of illegitimate traffic sourcing is explained in the next section.

Let's look at how it takes place...

How Digital Ad Fraud Takes Place



While this is a simple framework, the buy side of the programmatic market doesn't think or work this way today. Most automated buying is audience-based, and there is little transparency to distinguish legitimate from fake sites. Buyers are focused on reaching target consumers, no matter what site, and this is the root of the problem. Making the sites matter is one key step in minimizing fraud.

Fraudsters create bots to commit both fake- and legitimate-site fraud. But fraudsters do not covertly send their bots to legitimate publishing sites in substantial numbers because they don't make money that way. Instead, they make money by selling manufactured bots as "traffic" to publishers. Traffic sourcing is a common means for publishers to fulfill advertiser demand, but many publishers do not know the traffic they purchase is not human.

When an ad is displayed on a legitimate site, that publisher receives the revenue, not the fraudster that might send a bot in without the publisher knowing. This is important to understand as **legitimate site fraud occurs when a publisher, knowingly or unknowingly, introduces bots onto the site.**

Truth #2:
Illegitimate Traffic Sourcing is the Main Cause of Fraud

Traffic sourcing is any method by which digital media sellers acquire visitors through third parties. There are two main types: **legitimate marketing activity and illegitimate traffic sourcing.**

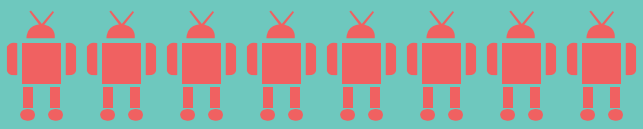
Legitimate marketing activity is when a publisher engages in audience acquisition methods that drive people to their site such as running sponsored posts on social media. This is a legitimate marketing tactic to bring more humans to the site.

Examples of Activities to Drive Site Traffic

Legitimate Marketing Activities

- Posting articles on social media
- Buying sponsored social media posts
- Sending an email newsletter
- Running a contest

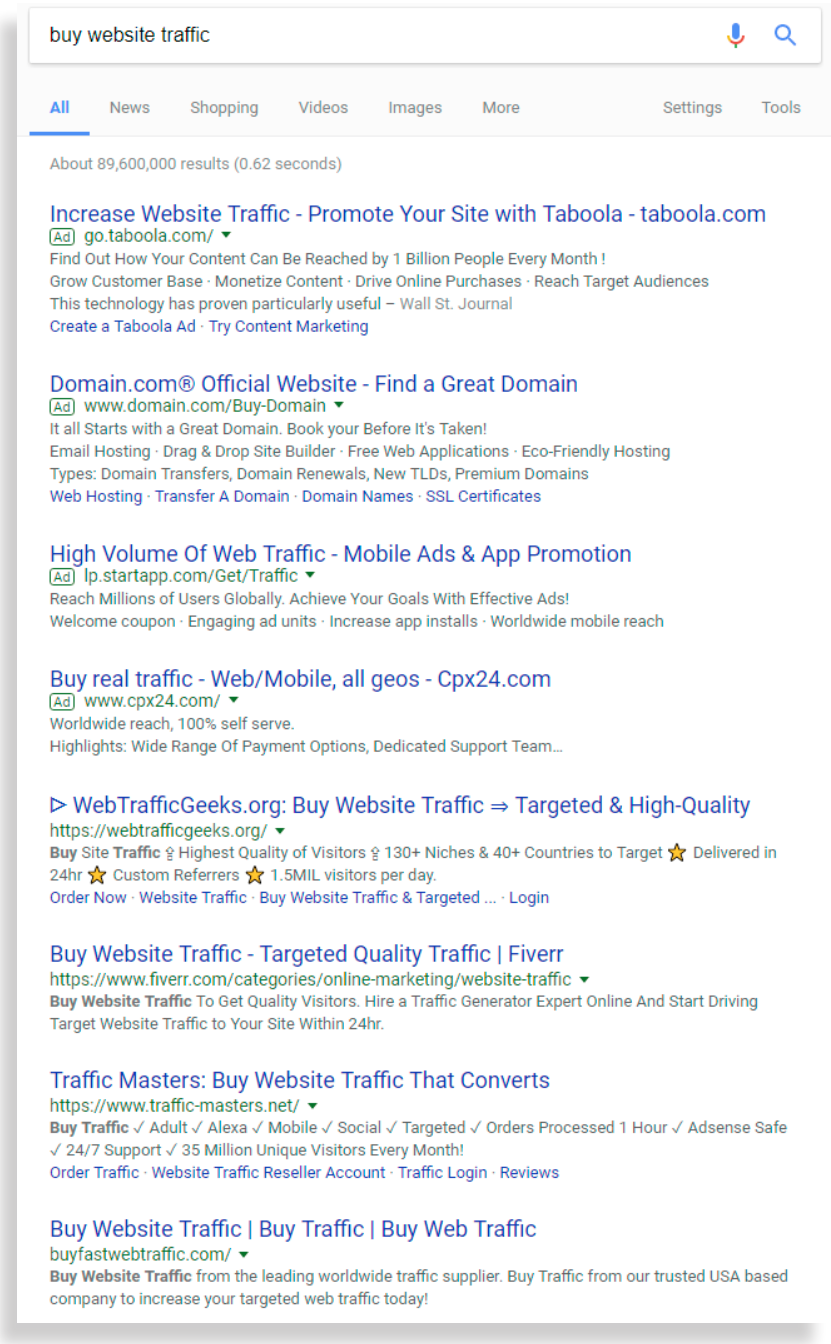
Illegitimate Traffic Sourcing



- Paying a traffic supplier for a fixed number of visits to a website, often at the end of the month or quarter to fulfill a campaign

Illegitimate traffic sourcing occurs when a publisher pays a traffic supplier for a fixed number of visits to their website. Publishers often buy traffic at the end of the month or quarter to "make its numbers." Traffic sellers often promise the publisher that the traffic is human and will pass through all ad fraud detection filters.

This type of traffic is likely robotic. Millions of people don't wait until the last day of the month to visit specific websites in specific quantities. The publisher might not know that this traffic is robotic because it may appear human in their fraud detection reports. It might also appear to be human traffic in the advertiser's fraud detection reports. And many marketers do not know that behavior is a common way for publishers to fulfill demand.



An example of a search for buying website traffic

The bots used in illegitimate traffic sourcing appear to be humans because fraudsters designed them to pass through ad fraud detection vendors' filters. A search for "buy website traffic" will return results for numerous suppliers selling traffic compliant with major fraud detection vendors. Publishers can purchase any flavor of traffic that works best.

Sometimes the traffic suppliers are overt and sometimes they are not. Sometimes publishers know what they are buying and sometimes they do not.

But the whole advertising economy relies on this practice today, and it is the main form of digital ad fraud as was outlined in the 2017 fraud study published by the ANA/White Ops.

Truth #3:

Ad Fraud Measurement Is Used to Transact but Does Not Minimize Ad Fraud

Ad fraud detection services are an important part of how the market transacts today because they add friction to combat the fraudsters. These services measure and filter non-human traffic. When these services are MRC-accredited, the market can have confidence that their processes and procedures adhere to industry standards for measurement services.

Multiple vendors with proprietary methods and technical measurement limitations compound the confusion surrounding ad fraud. To understand the limitations, consider the two techniques used to measure ad fraud today: **in-ad and on-page measurement.**

In-Ad versus On-Page Measurement

On-page measurement *assesses fraud on sites for publishers. A tag is placed on the page, which counts the impression as human or bot. This method sees the entire page actively to make the human vs. bot determination.*

In-ad measurement *assesses fraud in campaigns for media buyers. A tag is placed in the ad container, which counts the served impression as human or bot.*

Advertisers and agencies use ad fraud detection vendors to measure fraud in their campaigns. They use **in-ad measurement**, which means a tag (computer code) is placed in the ad container. As a user travels to a publisher's site, their browser executes the code and counts that ad exposure as a person or a bot.

There are two problems associated with in-ad measurement. The first problem is ad fraud detection vendors all have proprietary methods and calculate measurement differently. Running several fraud detection tags in the same ad will likely result in different measurements for each of them. The second problem is that in-ad measurement can only see what is happening within the ad container, not the other activity on the page. Because the ad is limited to a small area of the entire page, there are fewer data points that the tag can collect to determine whether the exposure was a human or bot.

Publishers also use fraud detection vendors to measure fraud on their sites and face the same issues of multiple vendors and methods. Publishers use **on-page measurement**, which is much different from in-ad measurement. The on-page method places a tag on the page where an ad is displayed allowing the tag to see the whole page. This method has a better chance of producing a more accurate measurement because it can detect more engagement on the entire page such as scrolling and clicking. This is the reason that an advertiser's in-ad measurements are normally at odds with a publisher's on-page measurements.

When you layer technical limitations of fraud measurement and proprietary methods from multiple vendors with the practice of purchasing bot traffic that is engineered to pass fraud detection, it is clear why there is frustration at all sides of the market. The measurements the industry relies on for transaction purposes deliver a false sense of security.

Illegitimate sourced bot traffic can pass through fraud detection and produce misleading metrics. The marketer pays the publisher for ads exposed to this traffic. The agency's and publisher's fraud metrics appear to be accurate. The marketer pays the agency. In this case, everyone in the system is making money at the expense of the marketer. But there's no return on investment for robotic exposures. Marketers are beginning to understand this and want to fix the system.

Marketers Demand a Fix

The Association of National Advertisers asked AAM to develop a **digital publisher audit** program to minimize digital ad fraud. Independent, third-party publisher auditing has minimized fraud in other forms of media and has the potential to transform the digital ad market.

AAM's digital publisher audit was developed to **minimize digital ad fraud**. **The program addresses fraud by differentiating good publishers** by ensuring that they are doing everything they can to serve marketers' ads only to humans.

This approach addresses the issues of both fake- and legitimate-site fraud. It allows marketers to stop advertising on fraudulent sites and invest with good publishers that are certified.

Publishers participate in a 90-day onboarding process. The publisher's processes, practices and procedures are documented, tested and verified. When the publisher completes their audit, the marketer has upfront, before-the-buy assurance that the publisher is delivering ads to people, not bots.

The audit process is continuous, which means the publisher's site is monitored 24 hours a day, 365 days a year to ensure consistent practices are followed. As part of the audit, the publisher must promptly remediate any issues.

What Makes AAM's Digital Publisher Audit Different?

AAM conducts an audit that is:

Independent

AAM is a tripartite not-for-profit that's owned by the industry to audit media.

Continuous

Monitoring a publisher's site consistently provides a high level of assurance.

Holistic

The audit includes a business process review that informs both quantity and quality verification.

AAM-audited publishers are prioritized throughout the media buying ecosystem through an expanded distribution network of ad exchanges, media buyers and whitelist service providers. A list of AAM-audited digital publishers will be integrated into buying systems so that marketers can specify these sites. Marketers will also use the audit to develop and prioritize the sites in their white lists. White list service providers will do the same.

Since the concept of digital publisher audits are new to the market, it is important to note how this audit is different than other initiatives. AAM is not an ad fraud detection service, and AAM does not produce new measurements. Fraud detection vendors are for-profit enterprises that exist to **measure fraud**. They are service providers, not independent audit companies.

AAM audits are part of a coordinated industry effort backed by the ANA to reduce ad fraud. The Trustworthy Accountability Group serves as an overall defense umbrella with compliance programs that span the ecosystem. The Media Rating Council (MRC) audits ad tech vendors to ensure that the measurement they provide meets industry standards. **AAM audits publishers** to certify that they are delivering human audiences to marketers. Together, we provide marketplace friction to combat fraud.

You Can Contribute to Fixing the Broken System

AAM digital publisher audits are a new paradigm in the market, requiring education on both the buy and sell sides. It addresses fraud with a time-tested model: separate the good publishers from the rest with independent audits to ensure that publishers follow best practices.

Marketers think it is time for the industry to stand up and do the right thing with independent publisher audits. Every industry professional—buyer or seller—has a responsibility to contribute to the fight against ad fraud.

Steps You Can Take to Fight Ad Fraud

Marketers must ask for media assurance to drive their marketing performance. We encourage marketers to take three steps to help build a quality digital media ecosystem through publisher audits:

- Decide which sites you want audited.
- Communicate with your agency and publisher partners that you plan to invest in audited media and make it a condition of your contracts.
- Activate by using the AAM-audited digital publisher list to plan your media investments, build white lists and buy directly or through exchanges.

Publishers can take steps to help build a quality media ecosystem and stand out to buyers.

- Commit to an audit. The simple act of agreeing to an audit can separate a publisher from millions of other sites.
- Participate in the process. AAM helps publishers through the audit preparation, including the information needed for the business process review and site tagging process.
- Stand out as a quality publisher. AAM-audited domains are differentiated in direct buys, white list services and the OpenRTB ecosystem.

Independent third-party audits will go a long way toward minimizing fraud. Marketers are beginning to vote with their dollars. Publishers who prove their quality with AAM digital publisher audits will be rewarded.

The **Alliance for Audited Media** (AAM) is a not-for- profit, tripartite media assurance organization. It has conducted media audits for over 100 years, including digital audits for 25 years. Owned by all sides of the media industry—advertisers, agencies and publishers—its mission is to help buyers buy and sellers sell in a trusting environment.

To learn more about AAM digital publisher audits, visit auditedmedia.com.