Brand Safety and Combating Digital Advertising Fraud

Learn How Marketron Protects Digital Advertising from Click Fraud

Marketron

Digital Ad Fraud Is Serious but Avoidable

Digital ad fraud is a concern for every seller and every advertiser. While it is prevalent globally, there are many ways that third-party digital platforms combat it. With our third-party digital advertising platforms, we're aligning with the best practices, technology and tactics to eliminate most ad fraud.

That includes four core components — technology and security, verification, transparency, and industry guidelines. With the combined capabilities of all these tactics, you can be confident in addressing ad fraud concerns with advertisers.

In this white paper, we provide information on brand safety and minimizing fraud to enhance your digital advertising literacy and explain it to your advertisers.

What you'll learn:

- What ad fraud is
- Types of ad fraud
- Ad fraud statistics
- Brand safety vs. brand suitability
- How Marketron monitors and prevents ad fraud with a four-pronged approach

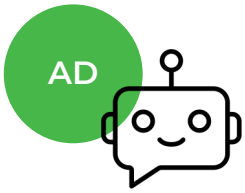
Marketron

What Is Ad Fraud?

Ad fraud happens when advertisers pay for clicks and impressions that never occurred or are not legitimate. It's an attempt to defraud digital advertising networks for financial gain. Such activities can be carried out by bots (machines and algorithms) and humans.

What Is Click Fraud?

Click fraud occurs when a person or bot pretends to be a legitimate user and clicks a digital ad. The goal of perpetrators is to "trick" platforms into thinking real users are engaging with the ad.



How Click Fraud Occurs

Typically, click fraud happens on a large scale with multiple clicks on links. Click fraudsters often program bots to automate the process. A bot may only be a "clicker" but could also replicate interactions like mouse movement, random pauses or other actions real users would take.

Scammers install bots on multiple devices with different IP addresses to avoid identification as suspicious. This is referred to as a botnet.

Bots aren't always the culprits. There are groups of people that do this too; this is called a click farm. Fraudsters may take this approach because of the human factor, which means less scrutiny by networks.

Click injection is another type of click fraud. Malware ends up on a user's device. It then generates clicks on digital ads to falsely inflate the spending on those ads.

Key Takeaway:

Ad and click fraud are part of the digital advertising ecosystem. The numbers around its prevalence and costs are shocking. However, this isn't a new problem. It's been around for decades, and the digital advertising community elevates its prevention capabilities constantly.

Types of Invalid Traffic

All these fraudulent clicks fall into categories of invalid traffic. Invalid traffic (IVT) is any traffic that is bot created. Not all IVT is bad; some bots are "good" bots, such as search engine crawlers.

The Media Rating Council (MRC) describes IVT as "traffic that does not meet certain ad serving quality or completeness criteria, or otherwise does not represent legitimate ad traffic that could be included in measurement counts."

There are two types of IVT.

General Invalid Traffic (GIVT)

This category includes traffic that doesn't meet a parameter threshold. It comprises bots, search engine crawlers and traffic from known data center IP addresses that generate non-human traffic. It can also be activity-based filtration using campaign or application data (and its transaction parameters) and browsers that prefetch or prerender pages for user convenience.

Sophisticated Invalid Traffic (SIVT)

SIVT is more complex than GIVT. It uses fraudulent or malignant bots and scripts to commit various illegal activities. It can often be more difficult to detect and requires more detection tools.

SIVT may include adware, which is software that displays unwanted advertisements on your computer to generate revenue. Additionally, SIVT may be the result of cookie stuffing. Cookie stuffing is the act of inserting, deleting or misattributing cookies to manipulate or falsify prior activity of users. The motivation behind this is to generate fraudulent affiliate income for the cookie stuffer.

Other Types of Ad Fraud

Domain Spoofing

Domain spoofing is the practice of disguising a website as one that's legitimate for ad serving. A cybercriminal would spoof a domain to trick advertisers into paying more for ad placement on the spoofed website than they should.

Ad Stacking

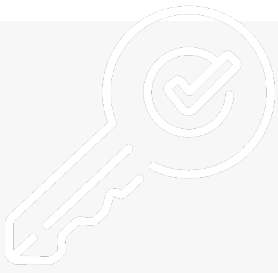
In this scenario, ads stack on top of each other. The audience only sees the ad on the top. Those stacked underneath still get the impressions or views even though they are not visible.

Ad Injection

This fraud strategy involves criminals using browser extensions, plugins and malware to put ads where they shouldn't appear or replace legitimate ads on a page. If someone clicks on the ad, the fraudster gets the credit rather than the rightful website owner.

Pixel Stuffing

Pixel stuffing is similar to ad stacking. It works by shrinking images to a size the human eye can't detect. Although no one can see it, it's there, so impressions are still counted.



Key Takeaway:

Ad fraud is not just one tactic; it's many. That can make it more complex to detect. However, ad fraud prevention technology is just as advanced as cybercriminals' mechanisms.

Ad Fraud Statistics

Tracking how often ad fraud occurs and its impact is something the industry takes seriously. To defend against any issue, you have to quantify it. Here are some key statistics:

11%

of global ad traffic is invalid. Nearly one-third of that occurs in China.
(Source)

$65B

The global cost of digital ad fraud is $65 billion annually.
(Source)

38%

of fraudulent clicks are bot related.
(Source)

36%

of display ad clicks are fraudulent or invalid. The study attributes this rise to COVID-19, which increased consumer usage of e-commerce. This is a global number, with India and Australia having the highest occurrences. (Source)

17%

of all CTV impressions are fraudulent.
(Source)

11%

of search ad clicks are fraudulent or invalid.
(Source)

Click fraud by industry: Education, local trades and finance are the most impacted.
(Source)

Key Takeaway:

These statistics could make your customers hesitant about digital advertising. They may even quote these to you as reasons for objecting to digital advertising. Handle that objection by acknowledging that it's a global problem but not one without a solution!

Brand Safety vs. Brand Suitability

What Is Brand Safety?

Another key term in the advertising fraud landscape is brand safety. Brand safety describes a company being proactive and taking measures to protect its brand and minimize reputational risk when advertising online. It addresses two areas of risk:

- ROI issues like ad fraud in terms of cybercriminals planting malware or adware in advertising assets to defraud users
- Ad placement and context relating to digital ads running on pages where content is illegal, dangerous or offensive

The measures available to brands often center on the practices and reputation of the programmatic provider. Not all platforms have controls in place to prevent fraud and ensure ad placement occurs on suitable sites.

Ad buying is an automated process but not one without safeguards. Technology should engage the four pillars of technology and security, verification, transparency, and industry guidelines.

What Is Brand Suitability?

The second aspect of brand safety has to do with brand suitability. With brand suitability, you're not just preventing ads from running on inappropriate sites; you're also trying to better align ad placement to relevant sites. The goal is for ads to run adjacent to content that's suitable and appropriate for your brand.

Brand suitability is about where ads appear and incorporates factors like:

- Audience demographics
- Platform
- Location
- Content proximity

Brand suitability elevates brand safety to the next level.

Key Takeaway:

Your advertisers likely always ask, "Where will my ad run?" With this question, they may not be asking about brand suitability. If they do bring up these terms, here's how to explain ad serving:

- The targeting criteria (demographics, location, preferences and previous activity) define where ads are served. Relevance is determined by targeting.
- In the network we use, ads are only placed on legitimate, appropriate and validated websites.

How Does Marketron Monitor and Prevent Ad Fraud?

As you read, ad fraud is pervasive and can occur in many ways. No matter the channels they use or the budget they spend, no business is immune to ad fraud. What's important to know and explain to your customers is that the Marketron platform you use provides the most comprehensive safeguards to mitigate it.

There are four main areas to ensure high-quality delivery of digital ad products:

Technology and security	Verification	Transparency	Industry Guidelines

Technology and Security

In fighting ad fraud, technology and security are essential components.

The HUMAN Verification Engine

The HUMAN Verification Engine is a program with the sole objective of protecting the digital advertising ecosystem. It uses more than 2,500 signals and 350 algorithms to analyze and detect ad fraud, deploying a multilayered approach to detecting sophisticated bots. It verifies 15 trillion interactions weekly.

How It Works

SSP

An impression occurs on a digital advertising platform from a participating SSP (supply-side platform).

The platform identifies the campaign(s) configured to bid on that impression.

HUMAN

Before bidding, the platform passes the impression to HUMAN.

HUMAN scans traffic across all ad inventory from participating SSPs.

Bid

Blocked

HUMAN either identifies it as safe or fraudulent. If safe, the bid occurs. If not, the impression is blocked.

This entire process takes less than 2 milliseconds.

Ads.txt

The Interactive Advertising Bureau (IAB) Tech Lab developed ads.txt (Authorized Digital Sellers) to help ad buyers avoid illegitimate sellers who spoof domains. In a nutshell, it's an IAB-approved text file that works to prevent unauthorized inventory sales.

The Marketron demand-side platform (DSP) handles the process to validate the inventory purchased.

Why It Matters

Unauthorized reselling is problematic. Before ads.txt, there wasn't an effective way for buyers to know if SSPs (supply-side platforms) had the authority to sell the inventory. With a repository of authorized sellers, buyers can more easily determine which programmatic platforms have legitimate access to the inventory they seek.

Key Takeaway:

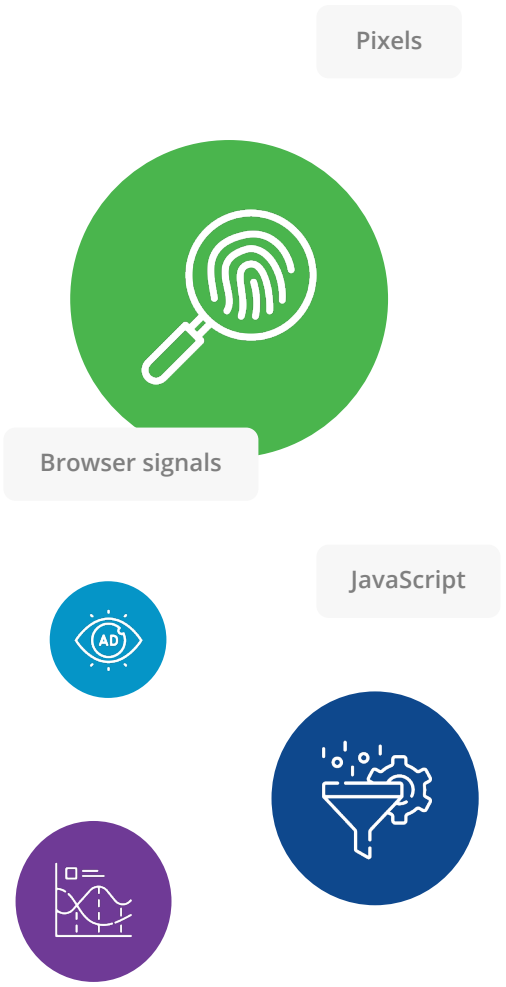
Those thwarting the attempts of cybercriminals used advanced technology and confirmation scripts to block fraudulent activity.

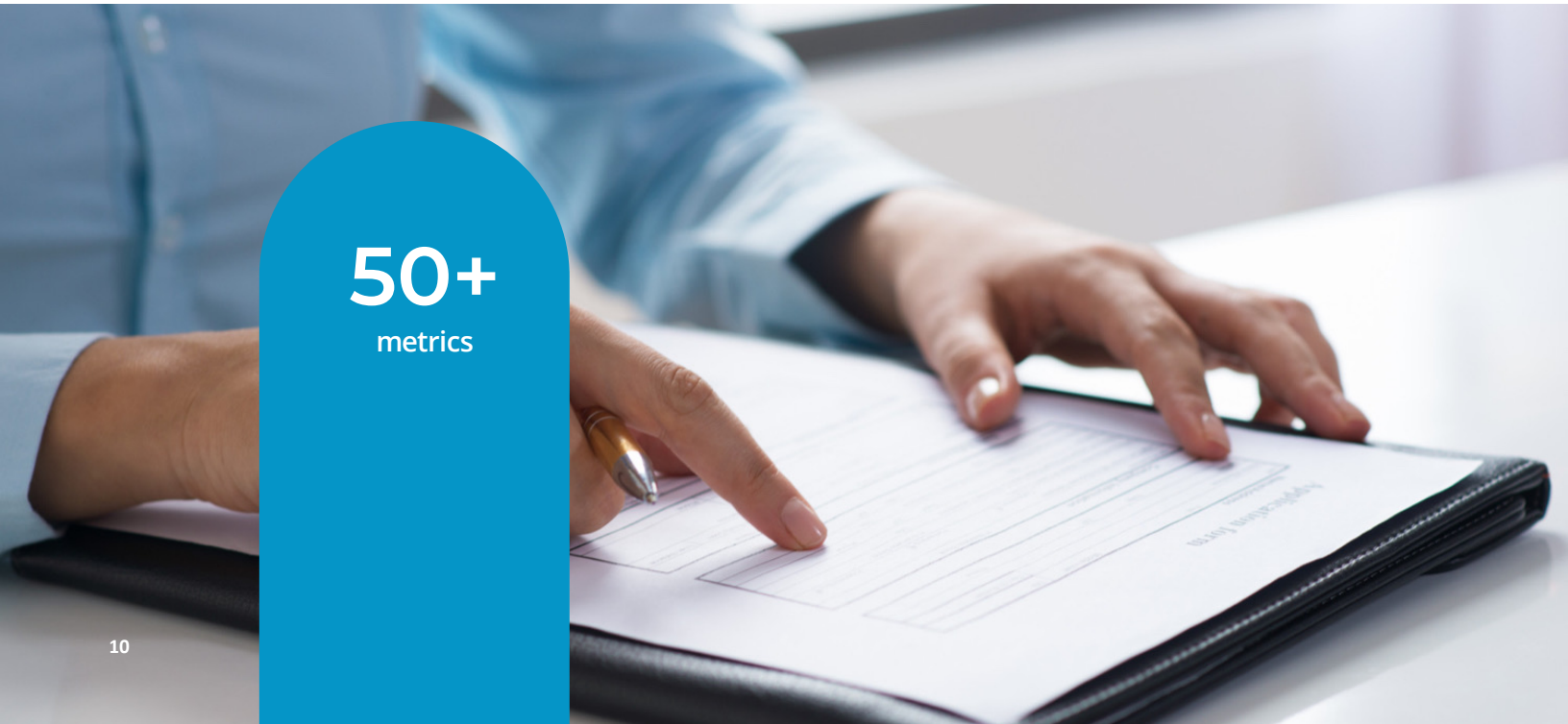
Third-Party Verification Providers

Our solutions incorporate MRC-accredited third-party verification providers. These verification engines are non-biased and must pass rigorous testing to earn accreditation. They use a range of sophisticated mechanisms to detect invalid traffic. The process includes a variety of behind-the-scenes tools, including pixels, JavaScript and browser signals to:

- Count ad impressions
- Detect, measure and filter invalid traffic
- Measure attention
- Determine the context of the content on the pages where ads appear, ensuring they meet advertiser objectives regarding viewability, brand safety and site quality

These fall in line with MRC guidelines, which include more than 50 metrics.





Site Transparency

Site transparency is another component of negating fraud and supporting brand safety. It's key to understanding supply quality. We offer 100% transparency for all users.

A central part of site transparency is whitelisting and blacklisting at the site level. A whitelist would include appropriate websites that align with your advertiser's requirements. Those could include content, price, location or other factors.

A blacklist includes websites in specific categories of sensitive subjects. That can include adult content or the exclusion of sites for kids to remain compliant with the Children's Online Privacy Protection Act (COPPA).

A site can also land on the blacklist if third-party verification platforms find irregularities regarding impressions versus site visits. If a site's data looks inconsistent, it's a sign that there could be fraud concerns. In that case, the verification platform blacklists those sites.

You can set blacklists and whitelists at the advertiser level or globally across your platform.

Key Takeaway:

Blacklisting and whitelisting protect against fraud and ensure brand safety. Explaining this can be key to answering additional questions about where ads are served.

Industry Guidelines

Our platforms maintain compliance with industry-leading organizations such as the Trustworthy Accountability Group (TAG). The organization is a global initiative fighting to end criminal activity and improve trust and transparency in digital advertising. The group has more than 700 members representing global brands, agencies, publishers and ad technology providers.

One of TAG's capabilities is its Certified Against Fraud Program, started in 2016 to combat invalid traffic. In its 2019 benchmark study, the use of TAG-certified distribution channels reduced the IVT rate to 1.41% across more than 210 billion impressions. As a result, fraud fell by 88%. Marketron is a member of the TAG Registry under

MBS Co LLC.

In addition, we follow the general best practices of fraud prevention, including the responsible use of consumer data and allowing any user to opt out of cookie-based targeting.

Making Every Impression and Click Count

Marketron has a strong commitment to eliminating ad fraud, leveraging multiple tools and protocols to mitigate its impact. With our investment in the four components of technology and security, verification, transparency, and industry guidelines, your advertisers will realize significant benefits from this multifaceted approach.

As technology matures and the industry changes, we'll continue to stay proactive in our approach to fraud.

If you have additional questions about our anti-fraud framework, contact our digital advertising experts.

Learn more at marketron.com

hello@marketron.com | 800-476-7226

Marketron