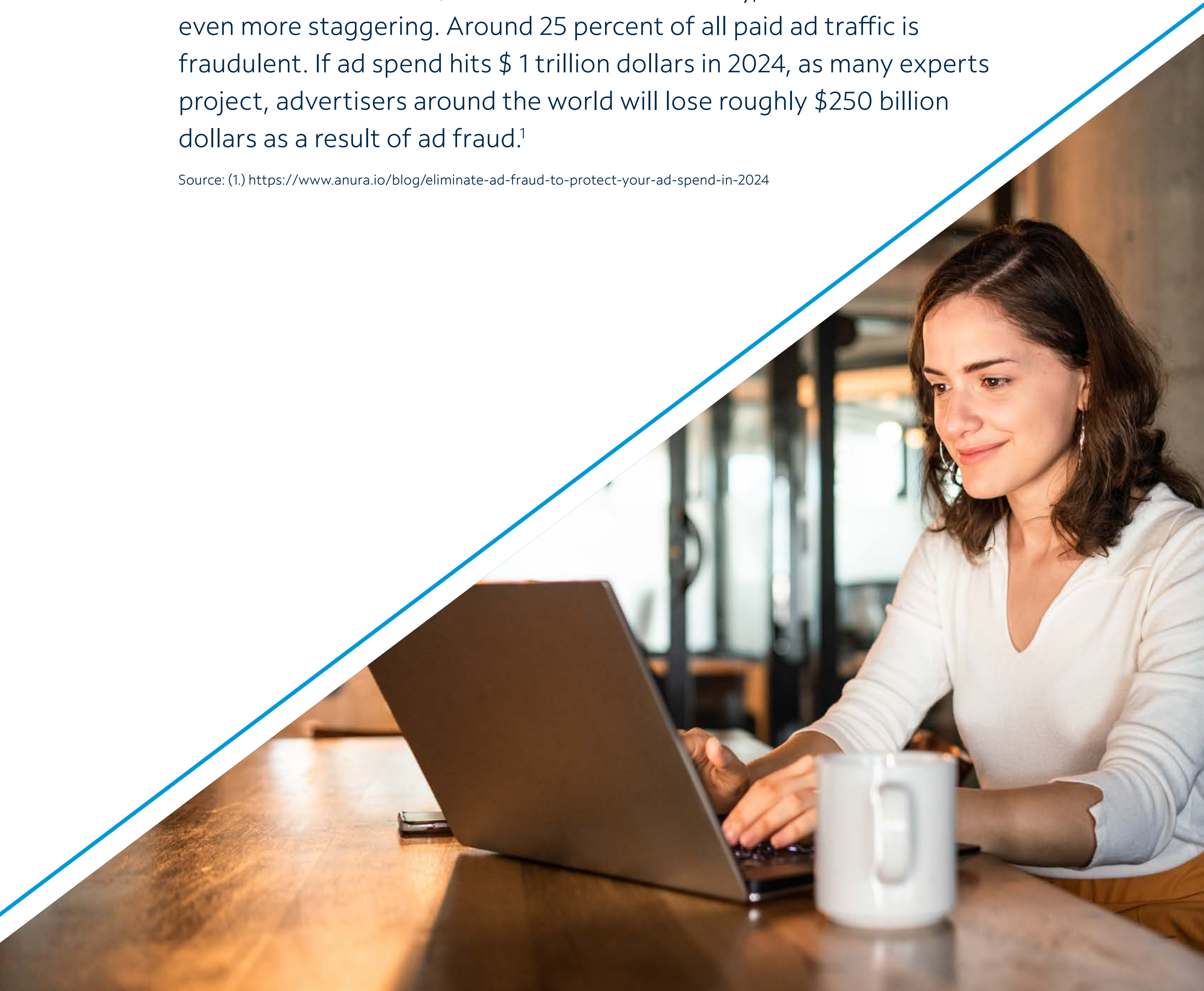
Spectrum REACH®

Brand Safety Guide

How to Prevent Ad Fraud and Protect Your Ad Spend

With nearly $264 billion in digital spend in the U.S. alone, advertisers are set to lose almost $66 billion in 2023. Globally, the numbers are even more staggering. Around 25 percent of all paid ad traffic is fraudulent. If ad spend hits $ 1 trillion dollars in 2024, as many experts project, advertisers around the world will lose roughly $250 billion dollars as a result of ad fraud.[1]

Source: (1.) https://www.anura.io/blog/eliminate-ad-fraud-to-protect-your-ad-spend-in-2024



How can you prevent ad fraud?

Spectrum Reach, the advertising sales division of Charter Communications, Inc., is at the forefront of the advertising industry-wide initiative to combat ad fraud. Ad Fraud is criminal activity that prevents digital and CTV ads from being seen by their intended customers, or even by any humans at all, and results in wasted or stolen advertising dollars.

It is important for advertisers not to rely alone on a publisher's guarantee of premium inventory, but to demand independent third party verification of all inventory from trusted Media Rating Council accredited partners. This way, marketers can better protect their media investment against fraud and malware, and make sure their ads were seen by their intended audiences.

Spectrum Reach can help you prevent ad fraud and protect your advertising investment by ensuring a premium environment across all screens. By adhering to these three practices, we ensure you are getting the highest quality, fraud-free streaming TV and online inventory:

1. **Premium Ad Placements:** Spectrum Reach operates a premium pool of inventory consisting of owned and operated properties, in addition to direct deals, carriage agreements, and partner relationships. This ensures no inventory is being aggregated blindly from indirect marketplaces or open exchanges.

2. **Premium Certifications:** Spectrum Reach is a TAG Platinum Status partner, certified against fraud, malware, brand safety certified, and certified for transparency. These independent certifications are verified by MRC accredited vendors and an external audit to validate that our inventory and acquisition practices are best-in-class.

3. **Premium Verification:** Spectrum Reach partnered with Oracle Moat as our verification partner to validate that all of our inventory has been seen by real people and is held to the highest Key Performance Indicators. We monitor this on a daily basis to ensure ad placements are always delivered on premium content, and provide high performance results.

Understanding Ad Fraud

Ad fraud on streaming TV and online affects almost every advertiser in some way. At a time when many companies are facing budget constraints brought on by economic disruption, they want to make sure every dollar counts. By not properly measuring or verifying online or streaming TV inventory, advertisers are putting themselves at significantly higher risk of falling victim to sophisticated schemes and "spoofing" scams designed to generate fraudulent inventory/ad requests that lead to advertisers unknowingly paying for impressions that were never seen.

The landscape of ad fraud is shiftng as media consumption habits evolve and scammers follow trends in viewership. In recent years, the number of ways to access digital video content has expanded and marketers have allocated more dollars to CTV. In fact, of the more than $85 billion spent by U.S. advertisers across TV platforms last year, CTV accounted for 24 percent of total investment.[1]

Unlike online fraud, which is mainly due to bot activity, ad fraud in CTV does not usually affect viewing experience. However, CTV is vulnerable to both device and content-driven ad fraud. In the former, scammers use hardware, including computers, phones and other devices to counterfeit impressions.

In the latter, also called inventory misrepresentation or domain spoofing, scammers create a fake version of a company's domain, mobile app or CTV app, or buy low quality ad inventory and try to pass it off as legitimate premium inventory. Scammers trick buyers into thinking their ad is going to a premium website or app, when in fact it ends up in unsafe or low-quality environments.

In comparison to other digital platforms, ad fraud is much less likely to occur within the premium environment of CTV, but it's important for marketers to understand how to identify and safeguard against all forms of ad fraud, particularly when planning multiscreen campaigns.

How can advertisers detect ad fraud?

Detecting digital advertising fraud can be difficult. However, there are some warning signs that can help you spot ad fraud, such as:

- **High bounce rates for websites**
- **Reductions in ad spend ROI**
- **Traffic from unfamiliar sources or non-targeted geolocations**
- **Abandoned carts**
- **Sudden large increase in clicks without a proportional increase in conversion**

Source: (1.) eMarketer Insider Intelligence US. TV Ad Spending, March 2023
eMarketer Insider Intelligence US. TV Ad Spending, March 2023

Types of Ad Fraud Techniques

Bots

Short for robots, hackers create bots to surf the web, click on ads and play videos, which drives up traffic, resulting in more money paid out to the fraudsters. These bots are viruses that can be installed unknowingly on a computer. However, most people with infected computers are completely unaware.

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. Domain spoofing is also commonly used to mask unsafe sites.

Pixel Stuffing

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

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.

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.

Cookie Stuffing

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

User-Agent Spoofing

The web page "header" that provides a description of the browser 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.

3 Tips to prevent ad fraud and protect your ad spend.

PICK TRUSTWORTHY PARTNERS

Make sure the partners and publishers you work with have a good reputation in their industry – or, even better, that they are third-party validated for the high standards they have set by the Trustworthy Accountability Group (TAG). TAG Certified Against Fraud status is a designation for companies who have established industry best practices to protect their digital advertising operations from the corroding effects of fraud. TAG Certification differentiates between the companies that are truly committed to fighting cybercrime through high standards, industry collaboration, and threat sharing.

Spectrum Reach was the ***first local media sales organization to achieve TAG Platinum Status.***

VERIFY, VERIFY, VERIFY!

Use tools to verify ads or use a partner who uses third party verification on your behalf – like Oracle Moat. Do not allow the end vendor to also evaluate their own work. Use industry trusted third parties to audit performance and to help hold your advertising dollars to the highest standard. Investigate when the cost per thousands (CPMs) are too good to be true.

Spectrum Reach is committed to providing advertisers with access to the most diverse and premium pool of ad inventory available, with an emphasis on brand safety and supply standards. In order to deliver on this promise, Spectrum Reach partnered with Oracle Moat Analytics to closely monitor and optimize toward supply quality metrics, such as measurability, viewability, valid traffic, and brand safety. This close attention to detail gives advertisers confidence in the quality of inventory and associated performance metrics, all in a privacy compliant way.

DEMAND TRANSPARENCY

Quite simply, transparency over your marketing efforts means having oversight over exactly where and how your campaigns are served. Don't trust someone who offers new "ad tech," or who just says that they are high quality or have premium inventory. Demand transparency. Ask to understand how the technology works, what makes their inventory premium, where your ads are running, and who is seeing them. As the first publisher to achieve the "Certified for Transparency" seal from TAG, we are dedicated to upholding superior transparency standards, so advertisers can better assess brand safety and supply quality on their own.

This seal speaks to the gravity of our efforts to help our clients deliver ads to real people, not bots, in a brand-safe environment, now and in the future.

We put the power in your hands, and give you 24/7 access to our fully-transparent reporting dashboard so you can measure impressions, creative, by device, daypart, and geography, and we offer visibility into video completion rates, and to which websites and networks your message was delivered. Additionally, Spectrum Reach is 100% ads.txt compliant, meaning we utilize a filtered whitelist to ensure ads appear only on quality, brand safe websites and apps that have been vetted and verified as legitimate - so ads are delivered to humans, and not bots, in a fraud-free environment.

Confirming our promise to uphold the highest brand safety standards to protect our clients' advertising on Streaming TV and Online. CONTACT US to experience the Spectrum Reach difference.