ALM | LAW.COM

Risks and Ad Fraud Protection In Digital Advertising

By Cecily Uhlfelder and Robert DeWitte
September 6, 2024

What You Need to Know

- Fraud accounts for 22% of yearly digital advertising expenditures, resulting in losses of up to $84 billion for advertisers annually.
- Digital ad fraud involves deceptive practices where fraudulent actors exploit automated advertising systems to drain ad budgets, skew campaign metrics and diminish campaign effectiveness.
- Monitoring of a digital campaign's performance is extremely critical.

Credit: Murrstock/Adobe Stock

Fraud accounts for 22% of yearly digital advertising expenditures, according to Juniper Research, resulting in losses of up to $84 billion for advertisers annually. Notice programs in the settlement context are not immune from this danger. Class counsel has a fiduciary duty to protect the best interests of the class, therefore protecting notice programs and the effectiveness of a digital advertising campaign is critical. Further, the recent tidal wave of suspicious claim filing may be connected to advertising (ad) fraud as well. Counsel would be remiss to brush aside concerns over ad fraud in favor of cheap digital notice campaigns. This article explores various risks to digital advertising from pixel stuffing and ad stacking to domain spoofing and bots. It will also explore what should be done to ensure ad fraud protection and improve effectiveness.

The ever-evolving digital marketing landscape, coupled with the industry-wide adoption of programmatic advertising, poses a significant threat to the effectiveness and integrity of digital advertising campaigns. In contrast to historically traditional methods where actual real people negotiate prices and placements, programmatic advertising has largely taken over. This automated process of buying and selling digital online space — which takes a mere two hundred milliseconds to complete — involves the use of software and algorithms to manage real-time auctions, where marketers bid for ad space on websites, mobile apps and other digital platforms.

While revolutionizing the means of transacting digital advertising buying and selling, programmatic advertising (which currently comprises over 90% of U.S. digital display advertising) has greatly contributed to the current digital environment, now ripe with opportunities for ad fraud.

Digital ad fraud involves deceptive practices where fraudulent actors exploit automated advertising systems to drain ad budgets, skew campaign metrics and diminish campaign effectiveness. As the sophistication of ad fraud techniques increases, it is crucial to partner with trained marketing professionals who are vigilant in managing and protecting their campaigns.

Understanding Digital Ad Fraud

The bad news: digital ad fraud can take various forms, creating a persistent challenge. The most prevalent forms include fraudulent bot traffic, click fraud, ad stacking and impression fraud, domain spoofing and pixel stuffing.

- **Bot Traffic.** This refers to any non-human traffic to a website or app. A bot is a software application designed to perform automated, repetitive and pre-defined tasks over the internet. Different types of bots are designed to perform different types of tasks. "Good" bots, such as search engine crawlers, visit websites to discover content that is used to provide search engine query results. Site-monitoring bots monitor website functionality, providing automated alerts when a site is not functioning properly. In the context of digital advertising, "bad" bots are designed with the objective of generating fake impressions and clicks that are ultimately reported as legitimate interactions. Fraudulent bot traffic can skew analytics, reporting impressions and clicks as "delivered" or "served," but in reality, were served to and generated by a bot and not to a human.
- **Click Fraud.** This occurs when individuals or bots imitate legitimate user clicks on digital advertisements. The website or platform where the ad appears is tricked into thinking real users are interacting with the ad and registers the bot activity as a legitimate human interaction.
- **Ad Stacking and Impression Fraud.** These methods involve a form of mobile ad fraud involving the layering or "stacking" of multiple ads on top of each other in a single ad space. While only the top ad is visible, impressions and clicks are attributed (and charged) to all ads.
- **Domain Spoofing.** In the context of digital advertising, domain spoofing involves the buying and selling of ad space on fake, low-quality websites that are created using a URL that closely resembles, or even copies, the URL of a known and trusted legitimate website. A "spoofed" domain may have an extra letter (e., "gooogle.com" with three O's) or a different URL extension (*i.e.*, ".co" or ".org" instead of the more common ".com") and may even have text and images that mimic the legitimate site. Marketers using programmatic ad buying platforms believe they are buying impressions on a high-quality site, when in fact their ads are being served on less reputable or irrelevant sites. It is not uncommon to see these sites grow like mushrooms around settlement website URLs, hoping to harvest ad traffic.
- **Pixel Stuffing.** This describes the practice of placing digital ads within a 1×1 pixel area (roughly .02 inches) on a website. The ad is invisible to the human eye but is still reported (and charged) as a delivered ad.

Combating Digital Ad Fraud

The good news: there are several strategies that trained media professionals can employ to effectively prevent, detect and mitigate fraudulent activity in online advertising. Key tactics include the use of fraud detection, prevention and verification tools, leveraging allow and block lists, partnering with reputable ad networks and exchanges and regularly monitoring campaign traffic.

Implementing advanced fraud detection tools can reduce fraudulent activity and protect digital campaign integrity and effectiveness. In that regard, it is critical that notice providers utilize the leading platforms in ad fraud detection software. These platforms use sophisticated algorithms, machine learning techniques, and data analysis to identify patterns and anomalies indicative of fraudulent activity. Media professionals employ this software to monitor campaigns in real time and alert them of suspected fraudulent activity such as bot traffic and click fraud. In addition to identifying fraud, these software platforms provide verification of whether a digital ad was served to human traffic, displayed in the targeted location and to the targeted audience.

Allow and Block Lists

In the programmatic advertising environment, "allow" lists and "block" lists provide media professionals with

better control over their ad placements. Allow listing is a practice involving the selection of specific websites or app domains where ads are displayed. A strategy that leverages an allow list consisting of trusted, high-quality sites will greatly mitigate the risk of fraud that exists in cheaper and lower quality (including spoofed) sites. Block listing is, as the name implies, the practice of blocking specific websites and apps that are suspected to be fraudulent or subject to high fraudulent traffic.

Ad networks and ad exchanges are a fundamental part of the programmatic advertising ecosystem. An ad network is an online platform that allows publishers to sell their inventory to advertisers. A publisher typically connects to multiple ad networks. Publishers use ad networks to sell inventory that does not get directly sold to advertisers. For example, cnn.com is a publisher. CNN's website, Cnn.com, will work with the Google Display Network to sell remnant inventory on an auction bidding basis.

An ad exchange acts as an online marketplace where publishers, marketers and ad networks can buy and sell ad inventory using a technology called Real-Time Bidding (RTB). Exchanges sell inventory on an impression-by-impression basis where marketers bid against each other for a given ad space (i.e., cnn.com), to a given user (i.e., Men 25-54), on a given device (i.e., iPad), in a given ad position (i.e., politics).

Key Takeaways

It is essential to select a seasoned notice provider that partners with trusted ad networks and exchanges that employ robust fraud prevention measures. Reputable platforms will have stringent vetting processes and better controls to mitigate the risk of fraud.

Monitoring of a digital campaign's performance is extremely critical. In the machine automated world of programmatic advertising, there is a tendency to "set it and forget it" when it comes to digital campaigns. This approach imperils the ability to detect irregularities and discrepancies, further hampering the ability to limit click fraud, impression fraud and bot traffic.

Combating digital ad fraud requires partnering with an experienced legal notice provider that employs a comprehensive and proactive approach. Leveraging advanced technologies, staying vigilant, and keeping informed about evolving fraud practices and trends allows firms to protect their notice program's integrity and ensure their digital campaigns achieve genuine and effective results.

*****

Cecily Uhlfelder is the media director in Kroll's Notice Media Solutions practice. She has more than 20 years of legal notice advertising experience, developing and implementing integrated media strategies for cross-platform notice programs. Cecily has worked on national, local and international advertising campaigns covering a wide range of complex cases, including antitrust, environmental issues, consumer fraud, product defects, personal injury, bankruptcy and restructuring. **Robert DeWitte** is Managing Director and Head of Business Development for Kroll's Settlement Administration practice. He has more than a decade of experience in the administration of domestic and international complex class action and other matters, including class certification notice campaigns, mass settlements, consent agreements, government remediation plans and insurance rehabilitations. As head of business development, Rob is instrumental in guiding strategic initiatives and market responsiveness for our Settlement Administration practice.

This article appeared in Cybersecurity Law & Strategy, an ALM publication for privacy and security professionals, Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, Corporate Counsel, Internet and Tech Practitioners, In-House Counsel. Visit the website to learn more.