Sizmek™

Fraud in Digital Advertising

What is 'Fraud' in Advertising?

Advertising fraud is typically done by creating fake ad traffic using content-scraping websites or other environments, launching ads outside of a user's view, or creating other fictitious mechanisms for delivering ads that are not seen by consumers.

Over a decade ago, the growth of search engine marketing and the lack of maturity in the space created an ideal environment for click fraud. The emergence of new ad formats and channels, like video or mobile, are today's new breeding grounds for fraud. With the rise of programmatic buying and, specifically, the nature of blind inventory available through RTB exchanges, advertising fraud has once again become the topic of the day due to the enormous volume of traffic.

Fraud is obviously a detriment to an advertiser's bottom line, with recent reports estimating that fraudulent practices comprise as much as one-third of all paid impressions. It should be noted that these numbers are often reported by companies offering fraud prevention solutions, and there has been some sensationalizing of the topic over the past year. That said, advertisers need better awareness of fraud methods, as well as ways they can be mitigated.

The good news is that we are here to help you understand what Fraud is, and how to best protect yourself, irrespective of solution provider.

Types of Advertising Fraud

Malicious Fraud:

Bots or Botnets

Bots are small programs usually hosted in unsuspecting users computers that can perform various activities on the internet. Groups of bots hosted on many computers are called Botnets.

Bots can do almost anything that a human can. They can click on links, generate web page traffic, and can even be segmented and targeted like any other user. Bots can be used to attack specific websites by overloading its servers to the point of failure. This is called a DOS or Denial of service attack, or bots can carry out a conversation with someone in a chat room. Bots are sophisticated programs.

Ghost Sites

The most widely reported type of fraud that currently takes place in online advertising is something referred to as Ghost Sites. These are real websites with real content, usually falsely produced or stolen from other legitimate websites. The sites' only purpose is to defraud advertisers. The site owners will create these sites and make them available through ad networks or exchanges that participate in Real

The emergence of new ad formats and channels, like video or mobile, are today's new breeding grounds for fraud.

Bots can do almost anything that a human can.

Time Bidding environments. They hire botnets to go to the site, which in turn generates ad impressions that enter the auction environment, and are then purchased by advertisers.

Purchased Traffic

Digital advertising fraud isn't only caused by ghost sites. Bot traffic exists on even the best websites. Monetizing content on the web can be difficult, and even name-brand publishers buy traffic to boost page views. They can sometimes get taken advantage of by someone promising legitimate web traffic but is really just producing bot traffic.

Given the number of bots traversing the internet (likely in the billions), some of them are going to land on legitimate sites generating false impressions, simply by following various links that they were programed to follow somewhere up-stream.

Free or ad-supported mobile app publishers face many of the same issues as digital media publishers: given the low cost of in-app media, they can be really difficult to monetize...and the margins can be slim. Given that dynamic, app publishers and ad networks need to drive extraordinarily cheap traffic back to their apps and their mobile web experiences. This often means buying traffic from resellers (who, in turn, buy that traffic from other resellers down the chain). The end result, again...bot traffic.

Ad Stacking

Ad stacking is a practice where multiple ads are stacked on top of one another, with only the top ad visible to the viewer. While only one ad is visible, the impression counts for each served ad, even the hidden ads underneath the stack.

This is another publisher/network specific trick to defraud advertisers.

Mobile SDK Overlap

Particularly prevalent in the mobile space, the stacking of Software Development Kits (SDK's) is another fraudulent practice. SDK's are sets of tools used to create applications. In a given mobile app, there may be different SDK's from the ad server, various ad networks as well as an ad format vendor – all tied together within the application. These SDK sets are not always designed to work together, which can lead to multiple ad impressions being delivered to the same spot – only one of which is seen. Sometimes, this happens by accident, but it's often purposeful activity.

iFrame/1x1 Pixels

iFrame stuffing, also referred to as pixel stuffing, takes place when a 1x1 pixel (invisible to the human eye) is placed on a site, sometimes through an ad unit. Unbeknownst to the user, these pixels can end up loading an entirely different website.

The site that loads out of view in a 1x1 iFrame often contains advertising – none of which is ever seen by a user.

While this method of fraud can be used to simulate false ad impressions, it's also often used in affiliate marketing scams, where the hidden site 'cookies' the visitor. The hidden site then gets to share the credit on any conversion or purchase with the site the viewer is actually visiting.

Sub-standard placements:

Video

A large number of sites feature 'auto-play' videos, which do not require a viewer to actually click on the video for it to play. Because a video impression is only counted when video playback begins, the advertiser ends up being charged for the video ad regardless of the user actually seeing the ad or not.

Additionally, these ads are often featured 'below-the-fold', which means they were less likely to be viewed. Worse still, these videos are often muted by default, giving the site visitor no indication of their existence.

This is not purely fraudulent (just not ideal for the advertiser), however if this website is then launched in a 1x1 pixel as mentioned above, you now see how a video ad as well as any other ad on the page was taken advantage of via fraud.

Mobile

Advertisers using in-app placements also face the challenge of quantifying the true value of those impressions and conversions.. So-called "incentivized media" may perform well, but often only because people are viewing ads to gain an app-related reward, and not because they're interested in the content.

Even mobile web comes with challenges that must be considered. The fact that mobile is relatively new means that many of the moving parts for delivering digital ads don't always work well together, meaning ads don't always appear as intended. Engagement-focused formats, like rich media, often are designed in Flash. Flash ads, however, do not work on iOS, and must be written in HTML5 to function properly on those devices... but not all mobile publishers support this format.

Auto-initiated video ads are often muted by default, giving the site visitor no indication of their existence.

Fraud Solutions from Sizmek

How to tackle the ghosts, bots and bad placements

The Sizmek MDX platform removes suspected fraudulent traffic based on known bots, and suspicious activity of both clicks and impressions. We strip this out of our reporting so that advertisers are never paying for this type of inventory.

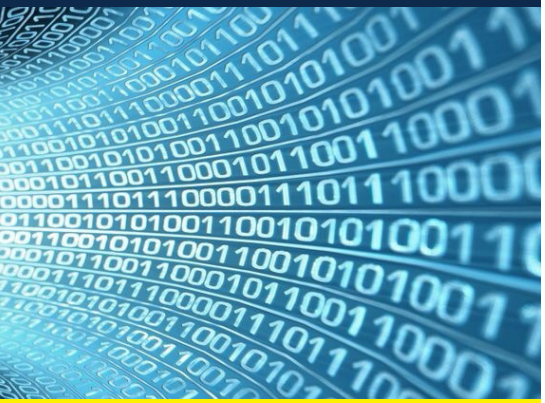
For the tough stuff, we also have a number of products that help advertisers mitigate their exposure to fraud and sub-standard placements. We also support solutions for both direct and RTB buying environments.

The Sizmek MDX platform removes suspected fraudulent traffic.

Sizmek Video Verification

Find out what's really going on with an ad. Sizmek's Video Verification solution provides advertisers with metrics that determine the player position per site, the size of the player, whether a video is auto-play or has user-initiated views, and it tracks whether the ad is placed on a video page. These metrics allow advertisers to approximate whether or not their ad had been seen as intended.

We know where our ads work, and that list is ever growing by the day.



Feel free to reach out to info@sizmek.com Our door is always open.

Sizmek Mobile Solution

Mobile is fairly new, and as a result is less mature when it comes to technology, specifically the technology that can help prevent fraud. This is more true in the networks and exchange world of mobile, then on publisher direct. As a result this is an area to be cautious about.

The first step to tackle fraud in the mobile channel? Be careful about where you buy inventory. Only work with reputable, top-of-the-range of publishers and be careful when working with networks or exchanges.

Our stellar certification process has been created to help advertisers eliminate their fear of ads not functioning properly in a mobile environment. With an ever-expanding list of certified publishers, we know where our ads work, and that list is ever growing by the day.

Even better, Sizmek's Verification, Viewability and Fraud detection tools work for the mobile web just as they do for desktop web.

Sizmek Ghost Sites and Non-Human Traffic Solution

We analyze the traffic patterns of sites for abnormal behavior (including in RTB environments) to flag suspiciously activity. We cross reference these patterns with a number of public and private data sources to help us identify pages that have been built and put up specifically to defraud advertisers.

Our identification of bots is both available in RTB as a filter through Peer39 by Sizmek, as well as a report in our verification products.

There are, and always will be, bad actors out there looking to defraud advertisers, and the best way to mitigate it is to work with trusted partners for inventory and technology, and stay educated.

Viewability measurement is also a way that advertisers can approach the subject, by ensuring ads are being actively viewed for specified periods of time; however viewability is a measure of performance, not a measure of traffic quality.

Similarly, while verification and brand safety involve additional campaign insights, these are measures of publisher inventory quality, not whether traffic to those sites is legitimate. Sizmek offers both viewability and verification solutions.