What Pharma Marketers Need to Know About Ad Verification

December 2013

Communications Media Inc.

WHITEPAPER

Fraudulent advertising behaviors are becoming more prevalent, costing advertisers millions of dollars a month in wasted ad impressions and clicks. This trend has been on the rise over the last several years. comScore recently reported that 36% of ad traffic is non-human traffic (NHT) which is a big jump up from only 6% in 2011. This being said, it is important to note that publishers, agencies, marketers, and media buyers monitoring their digital campaigns have options for identifying and minimizing instances of high-risk impressions through the use of ad verification services. Ad verification services originated with the need to protect brands from inappropriate placements, and are now extending to ensure quality impressions as well.

What is Ad Verification?

Ad verification is designed to ensure that every ad impression is a quality impression, every impression is compliant and is served and displayed as intended and purchased. Ad verification is a service that offers technology to ensure that ads appear on planned sites and reach the targeted audience. Publishers, agencies and marketers use ad verification technology to validate the delivery of display ads and ensure brand safety.

Types of Digital Media Discrepancies and Impression Fraud Activity

There are four primary areas that verification companies serve: Geotargeting, Placement, Viewability and Fraudlent activity. We will define these below, examining some of the most commonly known impression discrepancies that are of concern to digital marketers.

> "36% of ad traffic is non-human which is a big jump up from only 6% in 2011."
>
> comScore

Outside of Geographic Areas; also known as "Geotargeting"

Geotargeting refers to the serving (or non-serving) of ads to users in specific geographic locations, this can be outside of national and international targeting or outside of designated regions detailed in the media plan. Mapping users' IP addresses is the most widely used method to assign geographic location to users. This is one of the most common and basic impression discrepancies that ad verification technologies identify.

In our pharmaceutical space it is important on most campaigns to ensure that ad impressions run only within the United States, so we employ ad verification technology to monitor, catch, and block impressions from being served to IP address locations registered outside the United States (OUS Impressions). It is expected to see less than 1% of ad impressions delivered to OUS IP addresses. This is also measurable via an ad-server.

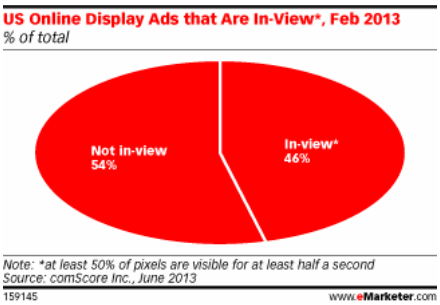
Placement Verification

Placement verification covers a variety of concerns to marketers. Ensuring one's ads are placed amongst relevant content, not within inappropriate content; confirming there is appropriate competitive ad separation, ads run as frequently as defined: only one ad per page or multiple ads per page if a roadblock, and if the frequency capping as requested; and ads are viewable by the user.

- **White List/ Black List:** White and Black lists are sites and/or domains you can provide to an ad verification supplier to ensure you are running on the sites on which you contracted. A White list being those sites on which you only want to appear, and a Black list being a set of websites upon which your ads should never appear.
- **Content or Keyword Verification:** Keyword verification is used in specific campaigns looking to ensure ultimate brand safety based upon the content or specific inappropriate keywords found within the content of the websites/pages that the impression is being served. This tracking is especially important in the pharmaceutical space where there are many restrictions about where and near what an ad can be featured and where failure to have this level of protection can result in costly fines for the pharmaceutical brand/company. Many ad verification suppliers, and some ad servers, will also create content categories upon which you can request your ad not be served. Examples of such categories include Adult Material, Suggestive, Disaster, Copyright Infringement, Weapons, Violence, and Hate/Profanity. By blocking one's ad in areas deemed unsafe, brands are assured that their ads will not run near unapproved or undesirable content.
- **Competitive Ad Separation:** In instances when a brand's contract specifies that it cannot appear on the same page or section as its competitor, ad verification can be used to help prevent or block the creative from serving when a known competitor is on the same page.

- **Frequency of Display (Ad Placement):** There are numerous placement specifications a brand could contract for that some ad verification companies can help ensure are met. Below are a selection of ad placements which may be verifiable:
    - Above/Below the fold placement: Reports on whether the ad appears above or below the fold.
    - Double-Serving: Occurs when there is more than one impression on a single page from the same brand. For example a 300x250 and 728x90 of the same creative appear at the same time.
    - Road Blocks: Occurs when a brand reserves multiple ad units, typically within a page or section. An infraction would occur if only a portion of those placements are executed.
    - 100% Share of Voice: In cases where a brand contracts to appear on 100% of a specific page or section of a site and another brand's ad appears within the contracted area.
    - Section/Channel targeting: A brand contracts to run within a specific a section of the site and ads are served outside of that section.
    - Frequency capping: A specific number of impressions are contracted to appear per user across a specific time frame, and the ad delivery exceeds the cap which was contracted.

The IAB guidelines define an ad as being "In-View" if at least 50% of the ad is visible for at least one second, however, in ad servers, an impression counts the same whether it's viewed for 30 seconds by the user or never seen at all. Data from comScore indicated that less than half of US display ad impressions delivered between May 2013 and February 2013 were "in-view."



> "The IAB guidelines define an ad as being 'in view' if at least 50% of the ad is visible for at least one second."
>
> ***IAB***

- **Viewable Impressions (also known as Viewability):** Another area of quality assurance that media use ad verification for is viewability. Viewability is defined by whether the ad was contained in the viewable space of the browser window based on pre-established criteria such as the percent of ad pixels and length of time the ad is in the viewable space of the browser.

Now, with ad verification, advertisers have the ability to calculate real reach numbers based on actual viewing, to measure which buys are providing the most value.

To track viewability, verification suppliers use ad tags that have the capability to look outside of the iframe to assess where the ad is on the page, and how long the user was active on the browser page, therefore determine viewability. Though this provides a point of reference, it is not a complete measure because viewability can also be determined by measuring whether or not the intended audience viewed the ad impression. Just because your ad doesn't load "above the fold" doesn't mean that it's not a viewable impression. For example if the content which your intended audience is most interested in is at the bottom of a page then it might be more impactful for your ad to fire below the fold where the audience is spending more quality time reading the content and the surrounding ads.

Fraudulent Activity

Millions of dollars are being lost by advertisers every day due to the growing problem of fraudulent digital activity. Impressions are being served that are never seen by the intended end user and clicks are registering and being paid for that do not result in site visits or anticipated actions. In addition, the time and money it costs to identify fraudulent activity and attempt to eliminate it is costing clients and publishers alike. As the proliferation of fraudulent activity continues, ad verification suppliers are devising automated ways to identify and report on suspicious activity.

- **Human or Non-Human Impression Fraud:**

Fraudulent click traffic and ad impression is an issue that has been plaguing the digital community since 2012. It can take multiple forms as outlined below.

  - Bot Generation: Botnet, one example of fraudulent activity, is defined as artificial traffic generated from thousands of infected zombie PCs attempting to, among other things, generate fraudulent advertising revenue through click fraud and impression fraud. A specific Botnet virus, dubbed "Chameleon," was reported to have infected approximately 120,000 PCs since 2012. The botnet fakes around 9 billion ad impressions per month leading to costly wasted impressions if undetected. Chameleon is also able to deceive systems that try to identify it, making it difficult both detect and address the fraud.
  - AdWare: Toolbars and advertising software that automatically inject unwanted ads into the page, shifting and obscuring the publisher's content, and replacing ads already bought. Almost all commercial antivirus software is able to detect adware.
  - Impression Laundering: Cases in which ads appear to display on legitimate sites, but through a complex number of re-directs are 'laundered' on to sites with high user traffic but low brand interest (i.e. adult content, illegal downloads).

- **Hidden Ads:** Hiding online ads, also known as ad stuffing, is a common technique used by nefarious actors to increase served impression counts by serving them in conditions under which they are not visible to the user. Sites participating in this type of fraud utilize many methods of ad serving manipulation including placing the ads in tiny iframes (1 pixel wide and tall), creating off-page HTML elements in which to serve ads, or stacking ad creative behind content or other advertisements.

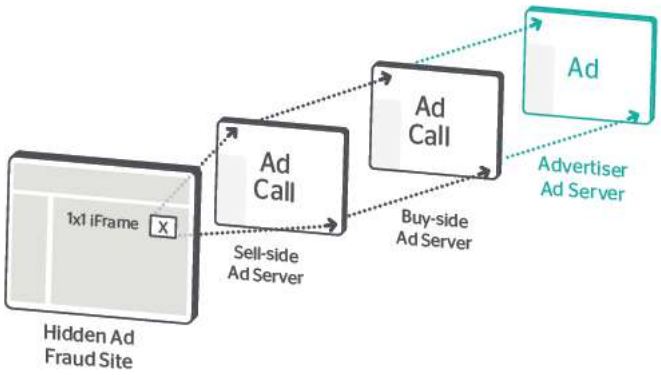


Figure 1 - Illustration of Hidden Ad Fraud

- **Invalid Clicks:** Invalid clicks on display ads are something we have dealt with over the past year and unfortunately the verification companies currently do not track. Click fraud occurs when a program automatically runs on a server clicking on ads on a particular site. It can also be caused by a person working for the publisher who clicks on the ads. The reason could be for crawling and scraping content, for quality assurance purposes, to artificially inflate click-through rates or other reasons. In such a scenario, while an advertiser does not necessarily lose much money, it makes the creative on that site appear to perform better than reality, and may be optimized toward.

Since this is an area that verification companies do not currently monitor, CMI/Compas will continue to track this in-house.

"With the volume and types of impression fraud on the rise it is increasingly important that media buyers are protecting their clients. "

Ad verification companies have been evolving their technical capabilities to help marketers better detect when impressions and clicks are being generated from fraudulent activities, but as technology advances, hackers also get smarter.

The Importance of Ad Verification as Part of All Digital Media Campaigns

With the volume and types of impression fraud on the rise it is increasingly important that media buyers are protecting their clients' investments by employing ad verification procedures and technology. These methods will help monitor, analyze, and take action when there are suspected or confirmed discrepancies. Ad verification will not only help advertisers save important budget dollars, but also keep publishers accountable to maintain transparent practices with regard to how they achieve and represent site traffic.

Now that we have outlined the various types of fraud, the impact it has on our industry and the ways in which we can protect our campaigns with ad verification services and technologies, it is now important to review the top tier ad verification companies that support pharmaceutical clients.

Next Steps for CMI/Compas Clients

Our supplier partnership and analytics teams have vetted the top three verification suppliers – DoubleVerify, Integral Ad Science (formerly AdSafe Media) and comScore's vCE (Validated Campaign Essentials). We have done a deep analysis of each supplier's offerings, the details of which we can share individually with clients. We will be choosing a partner soon.

With the large amount of advertising investment in online media, defrauders have a lot of incentive to continue, and if found, to devise other methodologies to avoid detection. In addition, defrauders in the online media space have networks for exchanging services and information, and among them are people who are extremely experienced and knowledgeable.

The challenge that verification suppliers are tasked with is a tough one. New types of fraud will emerge, existing forms of fraud (such as botnets) remain difficult to identify, and botnet operators are working on making non-human traffic appear more human. In short, defrauders will become prolific and better at evading detection. In such an environment, the verification companies will have to put the appropriate resources towards the development of their technologies and find the right talent to do this.

CMI/Compas will ensure that our clients have the best possible protection through both a partnership with an ad verification partner, and the continued advancement of our own internal technologies and detection services.

Communications Media Inc.

Compas Inc.

Analysts:

Nicole Woodland – De Van
SVP, Buying Services & Deliverables
Compas Inc.

Leanne Smith
Sr. Director, Insights & Analytics
Communications Media, Inc.

Shig Odani
Director, Insights & Analytics
Communications Media, Inc.