The Ad Industry's Focus on Fraud Has Intensified

Author : eMarketer

Date : September 5, 2016

Ad fraud has expanded to include diverse and sophisticated methods of deception that now affect mobile and video

In spite of the great advances made in the fight against ad fraud, the practice is still costing US digital display advertisers billions of dollars, as explored in a new eMarketer report, "Ad Fraud in the US: How More Sophisticated Methods Are Hurting Mobile, Video and Performance Measurement" (eMarketer PRO customers only).

An April 2016 survey from MyersBizNet shows just how top of mind these topics are. Click fraud and bot traffic were some of the most-cited concerns about media planning and buying among US media agencies and **brand** marketers. Viewability—which marketers are finding is increasingly intertwined with fraud—was also of concern.

Despite the industry's time, attention and resources to combating display ad fraud, its effects are still pervasive. The "Bot Baseline: Fraud in **Digital Advertising"** study conducted by the Association of National Advertisers(ANA) and fraud detection firm White Ops found bot-based fraud levels worldwide relatively unchanged from 2014 to 2015. The study predicted this would cost advertisers $7.2 billion this year.

The IAB and fraud investigation and dispute services firm EY estimated that invalid traffic cost the US digital display advertising industry $4.6 billion in 2015—which included both the direct effect of fraudulent parties and the estimated $169 million spent to fight and address invalid traffic.

The firms projected that an additional $1.1 billion was lost to "malvertising"—which includes practices such as hijacking user browsers or illegally downloading viruses and software onto users' machines for the purpose of generating botnets and other deceptive tactics, including link hijacking (in which fraudsters replace a legitimate link with their own) and ad injection (illegitimate ads are inserted onto legitimate publishers' sites without their knowledge).

While such estimates offer insight into the full scope of fraud's impact, they are by no means foolproof, given that they are only generated based on the types of fraud these studies were able to detect and based on an extrapolation of a sample of impressions.

A separate ANA/White Ops survey found that CPMs greater than $10 had a 39% higher bot rate than lower-valued inventory. It also found programmatically traded media—particularly video—had the greatest propensity for bot fraud.

Programmatic inventory, specifically the kind sold in open marketplaces, often sees more ad fraud than direct-sold inventory. Unlike direct buyer-to-seller deals, open marketplaces still rely heavily on intermediaries, which makes it easier for fraudulent publishers and parties to insert themselves into the transaction chain. A Q1 2016 survey of US digital display ads examined byIntegral Ad Science found 8.3% of all impressions were fraudulent, compared with 2.4% of publisher-direct sold ads.

Still, advertisers buying direct should not be lulled into a false sense of security, particularly when buying from publishers that allow intermediaries into their fold via either sourced (i.e., paid) traffic, which is the use of a third party to drive traffic to a publisher's site, or audience extension products, which allow advertisers to target users cookied on one publisher across additional publishers within a specific partnership or network. In both scenarios, publishers seek to drive greater traffic for advertisers.

This article first appeared in www.emarketer.com