choozle

REPORT

Combatting Ad Fraud in Digital Advertising

Introduction

Despite increasing concerns, the fight against ad fraud in digital advertising is seeing an upturn.

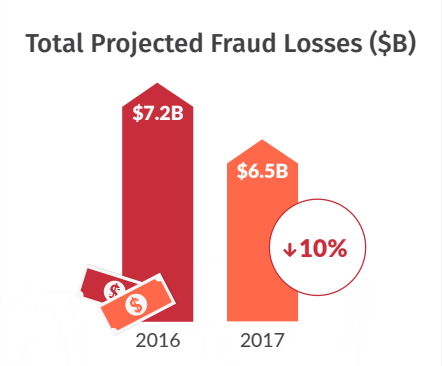
Imagine you bought a billboard on a busy highway, under the impression that it would be seen by 10,000 drivers a day. A week later, you find out that it's only seen by 8,500 drivers a day. Even worse, it was placed behind another billboard and on a quiet street with less traffic. Apply this example to the digital advertising space, and you have possible scenarios due to suspicious or fraudulent ads.

01 About Ad Fraud

Ad fraud is a term that many are familiar with, but few truly understand. In short, it is an umbrella term that refers to any illegitimate activity on an advertisement at the expense of the advertiser. As advertising budgets keep shifting to digital, fraudsters have found ways to game the system with the practice of fraudulently representing online advertisement impressions, clicks, conversion or data events.

In most cases, the cost of buying online ads is determined by one of two things: the number of clicks or the number of impressions. With ad fraud, the perpetrator uses backend schemes to generate fake clicks or impressions that offer no benefit to the advertiser. While these are the metrics most commonly associated with fraudulent activity, it's worth noting that ad fraud comes in many shapes and sizes and can affect a variety of different performance results.

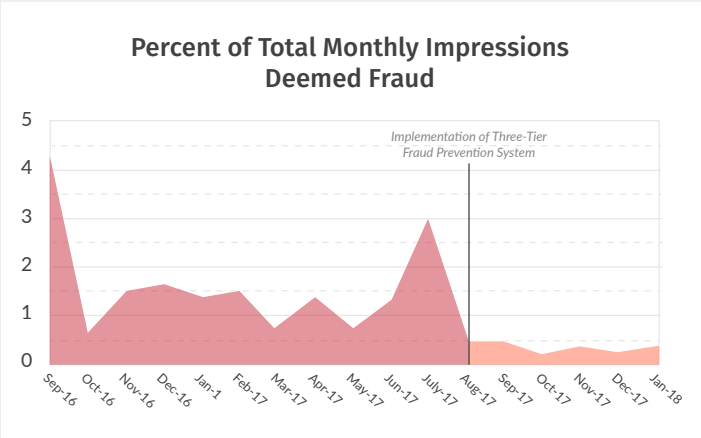
It's not all doom and gloom, though. In the ANA and White Ops' 2016–2017 "Bot Baseline" study, programmatic is no longer riskier than direct buys. **In fact, total projected fraud losses are down by 10 percent overall.**



Source: Bot Baseline 2016–2017 | Fraud in Digital Advertising

02 Choozle's Positioning

Choozle understands that ad fraud is a complex issue, and we're continually working to impove the way our platform deals with fraudulent traffic. Currently, we employ a three-tier fraud prevention system on all campaigns run on our platform. While some demand-side platforms (DSPs) employ tactics to identify and block suspicious IPs and inventory, Choozle's unique positioning in the market allows for a three-tiered fraud prevention system, which is unprecedented in the ad tech space. Within the first month of implementation, there was an estimated 84 percent reduction in month-over-month total impressions deemed suspicious or fraudulent.



Source: Choozle, 2018

03 Three-Tier Fraud Prevention System

The first line of defense comes from our buy-side partners. They track patterns and monitor activity across IPs, publishers, users, and supply vendors to help detect and prevent fraud. They continuously scan for signs of fraudulent traffic like high impression counts on a single page due to a bot reloading the page, domain spoofing, multiple impressions won on a single bid and bots mimicking human behavior. They place all of these traffic sources on a network-wide block list.

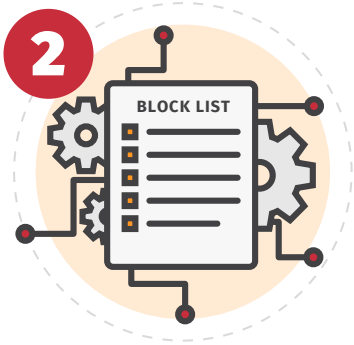
The second level of prevention consists of internal monitoring tools.
Choozle has two internal block lists to help further reduce suspicious sites and supply vendors. One is a continuously updated, internal pre-bid block list and the other is a list of historically low-viewable sites. We've created an automated system to scan network-wide performance data and identify any suspicious inventory as either red (actionable) or yellow (cautionary). Any site or application that comes back red is automatically added to our pre-bid block list and any inventory that comes back yellow is investigated manually. This block list allows us to quickly address and remove any site that is or could be affecting our clients.

The third and final layer of our system is at the user level. As a self-service platform, we heavily encourage our clients to build and use their own block and white lists to help reduce sites they are seeing low performance on or that they deem to be fraudulent. White Ops and the ANA estimates that $6.5 billion was lost to digital ad fraud globally last year. Not only does this hurt a company's bottom line, but it also makes it far more difficult to plan and allocate your marketing budget appropriately.

When comparing data from six months before implementation of the three-tier fraud prevention system to six months post-implementation, our platform-wide average conversion rate increased by nearly seven percent. While nearly 20 percent of total digital ad spend was wasted in 2016, our fraud prevention system has saved advertisers an estimated 1 percent of total ad spend in the past six months alone.

04 Action Items

The first step to avoiding ad fraud is **understanding it**. Take the time to learn about the various natures and what to look for in each. While most marketers attribute fraud to Clickbots such as Methbot which generates $3 to $5 million per day by targeting the video ad ecosystem, ad stacking, pixel stuffing, and domain spoofing are also prevalent contributors that shouldn't be overlooked.



Once you've learned about ad fraud, take that knowledge and use it to **analyze your campaign data and create comprehensive block lists**. The block lists should also be paired with a white list to create a solid foundation for safer ads. These lists should be consistently reviewed and refined over time.

Lastly, whenever possible, **optimize your campaigns for hard conversions** with clear intent such as discounts, contact form submissions, signups, etc. These types of campaigns will be much less prone to fraud.