FAQ

UNDERSTANDING DIGITAL AD FRAUD

Q. WHAT IS AD FRAUD?

A. For many advertisers, a large percentage of the potential digital market that they pay for is an illusion. This imaginary potential business is created by cybercriminals who are defrauding digital marketers out of billions of media dollars by selling the prospect of promotion with potential customers. Ad fraud is the most pervasive cybercrime by far, costing advertisers and estimated $7.2B annually.* Because digital ad fraud is so lucrative, it attracts the most sophisticated and smartest cybercriminals. The payoff from digital ad fraud is a strong incentive for those criminals to spread malware to every possible Internet-connected device.

Q. WHO IS THE ADVERSARY?

A. One type of adversary are the **black hat hackers** who pose as legitimate publishers. These cybercriminals build systems of **cash-out sites** -- sophisticated, counterfeit sites that host ads that will never be seen by a human. Botnet operators drive billions of bots a day to "view" ads on cash-out sites. The second type of adversary are **reseller-profiteers** who pose as legitimate digital media companies. These **bot traffic resellers** arbitrage page view traffic from botnets and sell **fake digital marketing events** to defraud advertisers. Both the cybercriminals creating and controlling the fake events and their traffic re-sellers are motivated by profits. They refine and multiply their attacks to maximize payouts.

Q. HOW DOES A CYBERCRIMINAL COMMIT AD FRAUD?

A. Bot fraud traffickers sell fake digital marketing events by setting up cash-out sites with fake content and building ad fraud bots. The ad fraud bots run on **botnets** -- networks of hacked devices -- to visit the fake sites. Black hat hackers also hack internet-connected devices to drive **stolen digital marketing events** such as **ad injection** – showing ads in hacked computers -- which was seen at 6% of total volume for one publisher in 2015 White Ops and ANA Bot Baseline Study). These profiteers also copy / steal content from publishers and use misdirection to serve ads to real consumers on cloned web sites that display stolen content.

Q. WHAT IS BEING STOLEN?

A. Marketers purchase ad placements on web sites, but many of these placements are offered by ad fraud traffickers on fake sites using fake users. Between 3% and 33% of marketers' digital ad budgets* are being stolen through the accidental purchase of digital ads on fake sites using fictitious users. Because marketers do not even know that they are being defrauded, attribution modeling, partner choices, and channel allocation based partially on fabricated success metrics are all affected.

*Source: *2015 White Ops and ANA Bot Baseline Study*

Q. DON'T WEB ANALYTICS IDENTIFY DIGITAL AD FRAUD?

A. Ad fraud bots can fake any digital audience characteristics that are targetable. This includes anything stored in a browser's cookie. Web analytics show details of the interaction between the audience and the page or the ad. When the viewer is a bot, the engagement details being shown in KPI reporting are meaningless.

Q. WHAT TYPES OF DIGITAL MEDIA ARE AT RISK FOR AD FRAUD?

A. All media is at risk to ad fraud -- even media directly purchased from premium publishers. Ad fraud is most rampant within video advertising, as that media is more expensive and has greater returns for fraudsters (In 2015, Video media campaigns with $15-or-greater CPM had 2.73 times more bots than campaigns with less than $15 CPM)*. Similarly, as advertisers will pay more for highly targeted campaigns or for specific KPIs, ad fraud bots have become sophisticated enough to mimic all of these characteristics and actions. This includes viewability, video completions, qualified registrations, and any actions stored in a browser's cookie.

Q. HOW DOES AD FRAUD AFFECT AGENCIES?

A. Brands are becoming better versed in digital media and more involved in their media strategies and partnerships. It is imperative for agencies to maintain transparency and create trust in their media buys. When agencies are aware of fraud and help clients avoid succumbing to fraudulent ad traffic, they win confidence from clients, bolster sales, and improve their competitive position in the marketplace.

Q. HOW DOES AD FRAUD AFFECT PUBLISHERS?

A. Advertisers lose trust in publishers that source external traffic to meet sold impression quantities or use audience extension programs that reduce quality. With transparency being top-of-mind in our industry, verified-human engagement is vital for publishers to demonstrate sustained inventory quality and continue to win advertiser budgets.

Q. HOW DOES AD FRAUD AFFECT AD TECH PLATFORMS, EXCHANGES, AND OTHER BUY-SIDE AND SELL-SIDE PLATFORMS?

A. Just as the programmatic supply aids automation and sophisticated audience-buying for authentic media impressions, programmatic targeting technologies unknowingly facilitate a massive black market for fraudulent ad traffic. As marketers and agencies become more aware of their stolen budgets, they will shift away from partners that are not actively combating and eradicating this fraud.

Q. HOW DOES AD FRAUD AFFECT CONSUMERS?

A. All of us are targetable consumers. Ad fraud encourages malicious hacker activity on our Internet-connected devices – meaning hackers are actively trying and succeeding at entering our homes and workplaces. Not only does this slow load times and denigrate user experiences, it puts our data at risk. Protecting against ad fraud is a first step in reducing the economic benefits of hacking into consumer devices and networks at scale.

*Source: *2015 White Ops and ANA Bot Baseline Study*