2018-2019

Bot Baseline

Fraud in Digital Advertising
Executive Summary

May 2019

About the Study

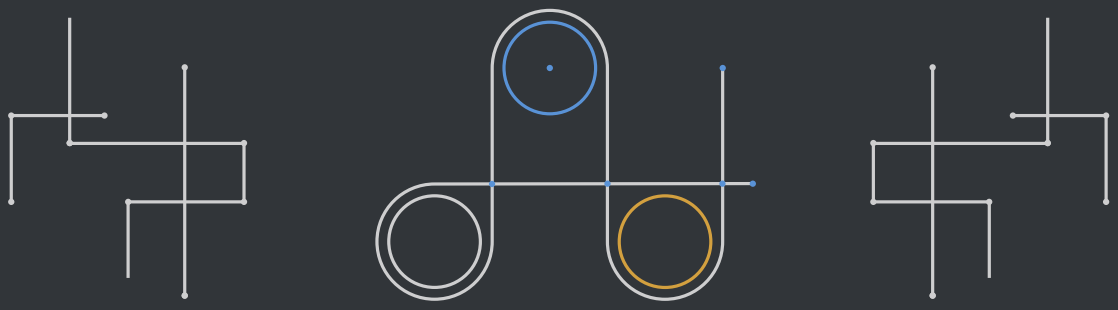
For the fourth time, White Ops and the ANA have partnered to measure bot fraud in the digital advertising ecosystem. Previous studies measured bot fraud in the digital advertising ecosystem in August/September 2014, August/September 2015, and November/December 2016.

In the latest study, 50 ANA member companies participated. White Ops worked with brand advertisers and their agencies to analyze digital advertising activity data between August 1, 2018 and September 30, 2018.

Measurements of fraud found in the global marketplace are derived from White Ops' ANA study participant data.

In this year's Bot Baseline, we share:

- **Baseline measurements of Sophisticated Invalid Traffic (SIVT),[2] excluding SIVT that was thwarted or otherwise not paid for.**
- **Initial metrics of the measurability and auditability of all the digital media paid for by study participants, illustrating the uphill battle toward full transparency.**
- **Practices related to the detection and prevention of digital ad fraud.**
- **Recommendations on best practices that will help advertisers protect budgets by ensuring their advertising dollars are not stolen by fraudsters.**

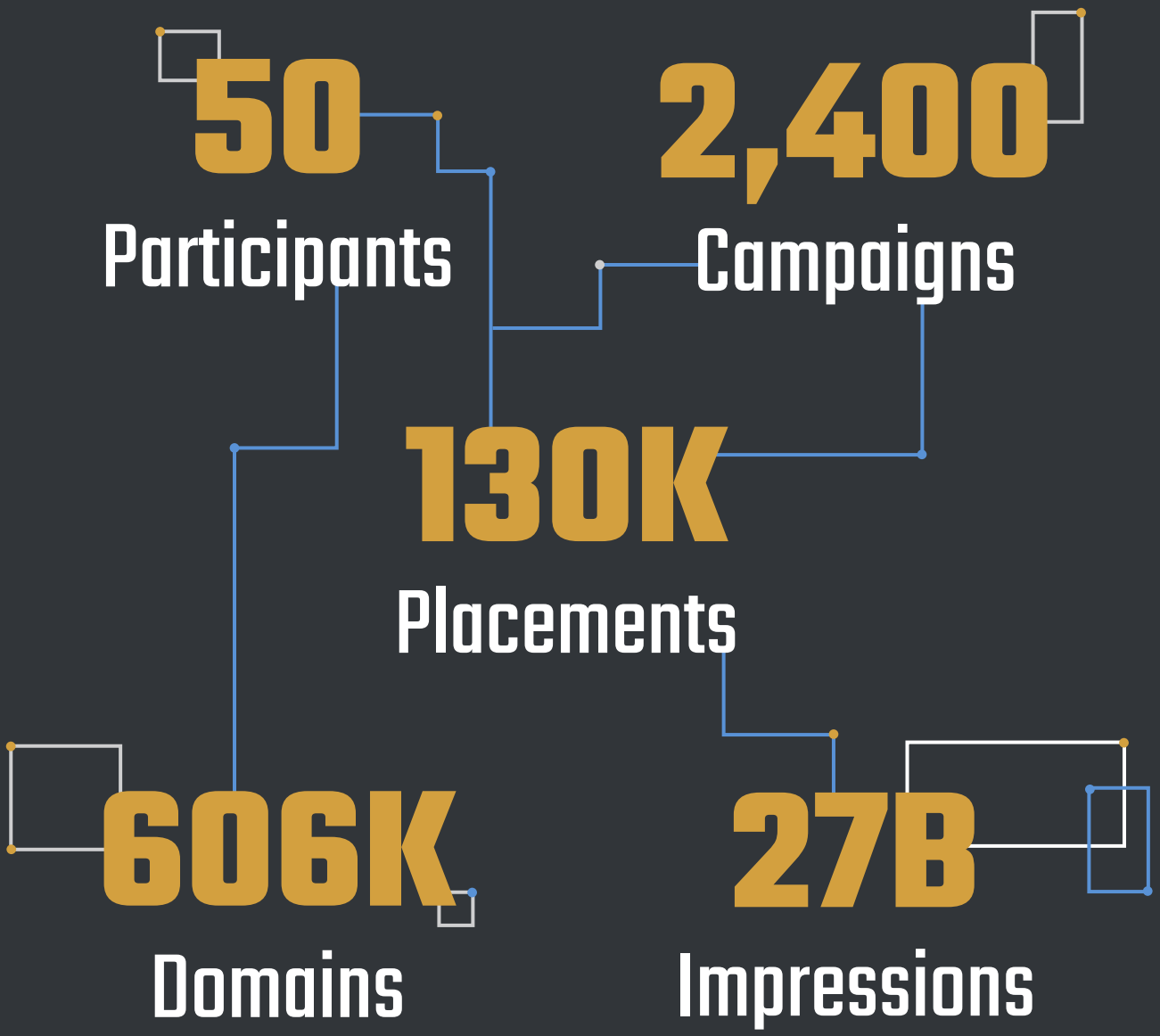


[2] General Invalid Traffic (GIVT) includes known non-human or fraudulent sources that can be identified with industry lists like the IAB Bots and Spiders List or parameter-based detection techniques. Sophisticated Invalid Traffic (SIVT) includes invalid traffic that is purpose-built to evade detection.

The Size and Scope of the Study

Of the 50 ANA member participants in the current study, 26 contributed data to previous Bot Baseline reports. Eleven have participated in all four studies, nine participated in three studies, and six participated in two studies; the remaining 24 participated for the first time.

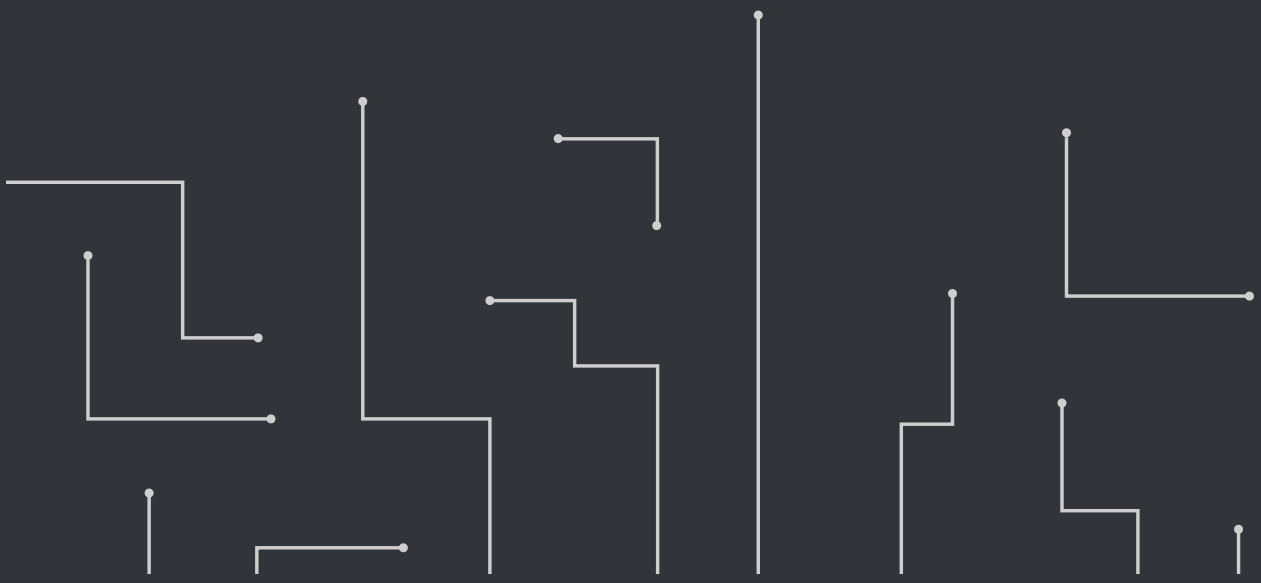
Our study examines advertising by brand marketers. It does not include search or paid social media campaign data.



Major Findings

For the First Time, More Fraud Will Be Stopped This Year than Will Succeed

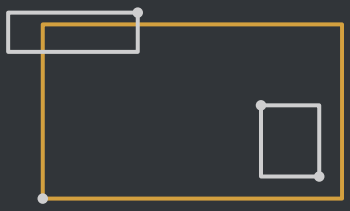
- Today, fraud attempts amount to 20 to 35 percent of all ad impressions throughout the year, but the fraud that gets through and gets paid for now is now much smaller.
- We project losses to fraud to reach **$5.8 billion globally**[3] in 2019. In our prior study, we projected losses of **$6.5 billion for 2017**. That 11 percent decline in two years is particularly impressive considering that digital ad spending increased by 25.4 percent between 2017 and 2019. A detailed breakdown by device and media type is below.
- For the first time, the majority of fraud attempts are getting stymied before they are paid for, by DSPs and SSPs filtering fraudulent bid requests, by clawbacks, or by other preventative measures. Absent those measures, losses to fraud would have grown to at least $14 billion annually.
- Fraud is an evolving threat. Fraud rates have been growing in new formats. Continued vigilance is needed. But there is no denying the structural gains the industry has made in this fight.



[3] Loss estimates are based strictly on digital spending in the categories included in the study: video, display, and other CPM formats for desktop and mobile devices.

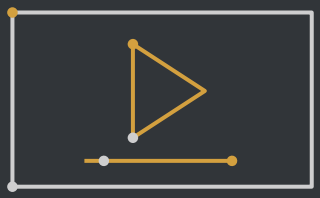
Projected Fraud Losses in 2019 by Category[4]

Desktop Study Sample Size: 13.6 Billion Impressions



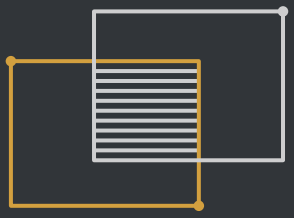
8% Display

down from 9% in 2017



14% Video[5]

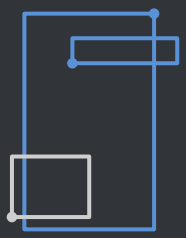
down from 22% in 2017



12% Other

Rich Media, Takeovers, etc.

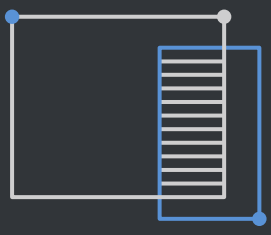
Mobile Study Sample Size: 13.5 Billion Impressions



3% Display

8% In-App Video

14% Web Video



7% Other

[4] Fraud rates exclude social media and search.

[5] As in prior years, video still shows more fraud.

How the Industry Has Made Gains Against Fraud

- Anti-fraud measures have made traffic sourcing more difficult and expensive.
- Thanks to traffic sourcing transparency efforts led by the Trustworthy Accountability Group (TAG), traffic vendors have gone further underground, reducing "retail" bot buying on the open web.
- Ads.txt has reduced domain spoofing.[6] Additionally, TAG requires publishers to have completed ads.txt files if they want to be Certified Against Fraud.
- Far more dollars are now being spent through programmatic platforms with built-in fraud prevention measures.
- Arrests, like those of the alleged masterminds behind the 3ve and Methbot operations, have brought real consequences to botnets operating overseas.

The Best Buyers Are Doing Better than Ever

- In our first study in 2014, fraud affected everyone, those with straightforward media plans and very sophisticated ones alike.
- This year, every buyer in the study knew about fraud risk; 90 percent had MRC-accredited fraud verification measures in place to deal with this risk.
- Performance was loosely correlated with study participation; long-time participants performed better than they did in previous years.
- For the top quintile of buyers, fraud was nearly nonexistent. However, discrepancies between ad server impressions numbers and verification impressions numbers were present for even the most sophisticated buyers.

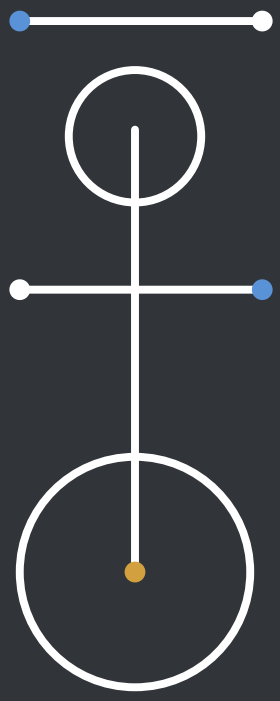
[6] Ads.txt, created by the IAB, stands for Authorized Digital Sellers. The mission of ads.txt is to increase transparency in the programmatic advertising ecosystem. It is a simple, flexible, and secure method that publishers and distributors can use to publicly declare the companies they authorize to sell their digital inventory.

It's Still Too Hard to Know What You're Buying

- The ability to hold all ad spending to the same high level of validatability should be one of marketers' top concerns in 2019. The time has come for marketers to stop tolerating — and stop paying for — outdated media formats like VAST 2 that cannot support the highest levels of third-party validation.
- By selling media under conditions that do not support high third-party validation, even trustworthy media companies are essentially part of the problem, since the vast sea of good but low-transparency inventory provides cover for the fake inventory sold under the same formats.
- Fraud detection and prevention are only as good as their implementation. Low Invalid Traffic (IVT)[7] measurements do not provide a full picture when half of a media plan is highly validatable with accredited third-party, dynamic JavaScript verification, but the rest is covered by a mix of half-measures like 1x1 pixels, list-based protections, and limited, static integrations.

Case Study: Trading Desk Video

One CPG participant purchased 44 million video impressions from an agency trading desk. Of the 44 million impressions, only 48 percent were validatable at the highest standard, with a dynamic fraud test served via JavaScript.



[7] Invalid Traffic is often referred to as Non-Human Traffic (NHT). It is the total of General Invalid Traffic (GIVT) and Sophisticated Invalid Traffic (SIVT).

For the fourth year running, White Ops and the Association of National Advertisers (ANA) have teamed up to produce the industry benchmark on ad fraud.

In this year's report, 50 ANA member companies participated in the study, enabling White Ops to track sophisticated invalid traffic (SIVT) across 130,000 ad placements and 27 billion ad impressions over the course of two months.

In the full report, we share:

1. **Measurements of SIVT among some of the biggest brands on the planet.**
2. **The first coverage analysis of its kind, taking into consideration third-party ad server impressions as compared to fraud verification metrics.**
3. **The good news, the bad news, and where ad fraud is going next.**
4. **Steps your organization can take to reduce ad fraud today.**

To download the full report, visit www.whiteops.com/botbaseline2019

Bot Baseline 2018-2019

www.ana.net | info.ana.net | www.whiteops.com | info@whiteops.com