Bot Baseline:

FRAUD IN DIGITAL ADVERTISING

Key Findings Report

OVERVIEW

In 2014, White Ops and the Association of National Advertisers (ANA) partnered to release the Bot Baseline Study, considered by many to be the seminal report on advertising fraud. The 2014 study helped provide the industry with a better understanding of the impact of fraud on the online advertising ecosystem and provided a series of action steps to help stakeholders reduce fraud.

In 2015, White Ops and the ANA worked together again to repeat the study, this time with a larger group of participants: 49 advertisers versus 36 in 2014. These participants deployed White Ops detection tags on their digital advertising to measure bot fraud, or non-human traffic. Bots are automated entities capable of consuming any digital content, including text, video, images, audio, and other data. These agents may intentionally or unintentionally view ads, watch videos, listen to radio spots, fake viewability, and click on ads.

Data was collected over 61 days from August 1 to September 30, 2015 (the same period as 2014). Ten billion total impressions were examined across 1,300 campaigns. All participants received proprietary information on their buys. The aggregate data is reported here.

The 2015 study participants consisted of:

- 49 advertisers
- 28 returning participants and 21 new participants
- From 10 industries: auto, beer/spirits, CPG, financial services, health care, hospitality/travel, insurance, restaurant, retail, and technology

March 2016

SPECIAL THANKS TO THE FOLLOWING ANA MEMBER COMPANY PARTICIPANTS

ABInBev
Allstate
You're in good hands.
Bank of America
Bayer
Boehringer Ingelheim

CLOROX
COLGATE-PALMOLIVE
ConAgra Foods
Food you love
DELL
Denny's

Dr Pepper
Est. 1885
Expedia
Ford
GoDaddy

HAWAIIAN AIRLINES
HEINEKEN
HISCOX
THE HOME DEPOT
HONDA

hp
IBM
Johnson & Johnson
JPMorgan Chase & Co.
Kellogg's

Kimberly-Clark
La Quinta
Inns & Suites
Lilly
MARS
chocolate
north america
MasterCard

MillerCoors
Nestlé
NEW YORK LIFE
Pernod Ricard USA

Pfizer
PlayStation
PrestigeBrands
Prudential
State Farm

TACO BELL
TARGET
Tyson
Unilever
USAA

Walmart
Wendy's

Download the full report at www.ana.net/botfraudfindings2015

MAJOR FINDINGS

BOT PROFITS INCREASED IN 2015

a Financial Impact Averaged $10 Million per Participant, with $7.2 Billion Estimated Global Losses Expected in 2016

The annual financial impact of bot fraud ranged between $250,000 and $42 million for the 49 participating advertisers and averaged about $10 million per participant. The 2014 Bot Baseline Study estimated that advertisers would lose approximately $6.3 billion globally to bots in 2015. With the overall rate of fraud unchanged in our current study and estimating a 15 percent increase in global digital spending in 2016, losses due to bots could be approximately $7.2 billion globally in 2016.

b Bots Are Fooling Detection and Prevention Efforts

- Bots exploited users' cookies to appear as humans in general detection and prevention systems.
- Bots spoofed viewability, showing nearly the same viewable rates as humans. Bots fooled list-based prevention technologies in programmatic buys.
- Desktop bots impersonated mobile devices to consume mobile media.

c Bots Prey on Higher-Value Media

Media with higher CPMs (cost per thousand impressions) was more vulnerable to bots, as these segments provide a stronger economic incentive for botnet operators to commit fraud. Display media with CPMs over $10 had 39 percent higher bots than lower-CPM media. Video media with CPMs over $15 had 173 percent higher bots than lower-CPM media.

d More Focused Targeting Results in Increased Fraud

- The high demand/limited supply for targeting certain high-CPM market segments, such as high-income demographics or Hispanics, means rewards are greater for bot operators which can seemingly supply the needed audience impressions in those segments.
- Hispanic-targeted programmatic media had 70 percent greater bots than non-Hispanic.
- Hispanic-targeted direct buys had 20 percent greater bots than non-Hispanic.

MAJOR FINDINGS

BOT FRAUD RATES OVERALL SHOWED NO CHANGE IN 2015

a Overall Fraud Levels Ranged from 3 Percent to 37 Percent

In 2015, advertisers had a range of bot percentages varying from 3 to 37 percent, compared to 2 to 22 percent in 2014. But the overall rate of fraud was basically unchanged. Only about one-third of the advertisers which participated in both 2014 and 2015 experienced a decrease in their bot rates, suggesting that advertising fraud needs to continue to be a focus in 2016.

b Traffic Sourcing Remains Problematic

Sourcing traffic (any method by which publishers acquire more visitors through third parties) results in greater fraud. Sourced traffic had more than three times the bot percentage than the study average.

c Fraud Varies by Buy Type

- Direct buys had lower fraud. Programmatic buys had greater fraud. The high bot rates in programmatic video were expected given that video CPMs are significantly higher than other types of online media.
- Programmatic display ads had 14 percent more bots than the study average.
- Programmatic video ads had 73 percent more bots than the study average.
- Direct video ads, where measurable, were 59 percent less likely to have bots than the study average.
- Direct display ads were 14 percent less likely to have bots than the study average.

$10	$7.2	39%	70%
Million average lost per participant	Billion estimated global losses in 2016	Higher bot rates in display media over $10 CPM	Higher bot rates in Hispanic-targeted programmatic media

RECOMMENDATIONS

Stakeholders in the advertising ecosystem are taking action to reduce ad fraud, but the leading edge of fresh botnet infections are holding the size of the problem steady and causing the bulk of monetary losses to advertisers.

In 2015, advertisers with the lowest impact from bot fraud:

- Used legal language that removed the impact of fraud during the billing stage, placing legal language in contracts that stated the commitment not to pay for fraudulent impressions
- Selected media partners that proactively reduce fraud
- Leveraged the watchdog effect by announcing anti-fraud policies to partners and encouraging them to provide the highest-validity media
- Created open dialogues with providers about traffic sourcing and carefully selected the providers with a commitment to providing valid impressions
- Combined technology with anti-fraud policies and strategies to reduce fraud at all levels

In 2016, all stakeholders can work to reduce ad fraud by combining the use of anti-fraud technologies with proactive policies and strategies that reduce the impact of fraud across all stages.

ACTION PLAN FOR ALL STAKEHOLDERS

a. Authorize and Approve Third-Party Traffic Validation Technology

To effectively combat bots in their media buys, advertisers, publishers, and agencies must be able to deploy monitoring tools. This study was not deployed across all participants' placements, partly due to agency and publisher policies, which did not permit the monitoring software in certain placements. All participants in the advertising ecosystem need to be able to set policy and procedures to enable advertisers to deploy fraud detection technologies in their ad buys.

b. Require Clarity from Vendors on How They Combat Fraud

Always ask the vendor how it measures for bots — whether it matches against a list (using general detection methods) or uses sophisticated bot detection method(s) as defined by MRC. When possible, use solutions that are proven to reduce fraud in targeted media and buy types.

c. Protect Against Fraud that Is in the Profit Window

When possible, use sophisticated bot detection to shrink the profit window for ad fraud. Use sophisticated fraud detection solutions to reveal the hard-to-find fraud that is still fresh and profitable for the botnet operators because it is not yet listed in general detection databases.

d. Use Sophisticated Fraud Detection to Block Bots in Programmatic Media

Protect programmatic media buys with sophisticated fraud detection as defined by MRC and avoid general blocking solutions that are not shown to significantly reduce fraud in programmatic buys.

e. Follow MRC Guidelines for Invalid Traffic Detection and Filtration

MRC recently issued a strong set of guidelines for invalid traffic detection and filtration. The ANA recommends all digital measurement organizations adopt these guidelines and that sophisticated fraud detection vendors seek MRC accreditation for their detection procedures.

f. Support the Trustworthy Accountability Group

The IAB, 4A's, and the ANA announced in November 2014 the creation of the Trustworthy Accountability Group (TAG), a joint marketing-media industry program designed to eradicate digital advertising fraud, malware, ad-supported piracy, and other deficiencies in the digital communications supply chain. In the past year TAG has made significant strides in developing solutions to thwart fraud in the advertising supply chain while gaining strong support from its industry leaders. TAG has developed an Anti-Fraud Working Group with a mission to improve trust, transparency, and accountability by developing tools, standards, and technologies that enable the elimination of fraud. In May 2015 TAG unveiled its Fraud Threat List, a shared database of domains that are known sources of non-human traffic. Shortly thereafter TAG launched the Data Center IP list, which identifies sources of non-human traffic based upon IP addresses. Support of TAG's initiatives is a crucial step in creating a transparent and legitimate digital advertising ecosystem. Every company across the ecosystem should register with TAG in order to ensure they are doing business with trusted partners.

ACTION PLAN FOR BUYERS

a. Be Aware and Involved

Advertisers must be aware of digital advertising fraud and take an active and vocal position in addressing the problem. Fraud hurts everyone in the digital communications supply chain, especially advertisers. Advertisers must therefore play an active role in generating positive change and should take responsibility for combating ad fraud.

b. Request Transparency for Sourced Traffic

Traffic sourcing correlates strongly to high bot percentages. It's recommended that buyers request transparency from publishers around traffic sourcing and build language into RFPs and IOs that requires publishers to identify all third-party sources of traffic. Furthermore, buyers should have the option of rejecting sourced traffic and running advertising only on a publisher's organic site traffic.

c. Request Transparency for Audience Extension Practices

Audience extension by publishers can introduce high bot percentages by extending content to providers that source traffic. It's recommended that buyers request transparency from publishers around audience extension and build language into RFPs and IOs that requires publishers to identify audience extension practices. Buyers should have the option of rejecting audience extension and running advertising only on a publisher's owned and operated site.

d. Understand the Programmatic Supply Chain and Require Inventory Transparency

The foundation of optimizing your media investment, including reducing bot fraud when using programmatic buys, is understanding the programmatic supply chain. Advertisers should ask about the role of each player in the process, know the partners of your partners, and then ask for inventory transparency to know where your programmatic advertising is running. You wouldn't "blindly" run your advertising in offline media such as television or print without knowing the specific networks or publications that carry your advertising. Why accept anything less in programmatic buying?

e. Include Language on Non-Human Traffic in Terms and Conditions

Insertion orders should include language that the company will only pay for non-bot impressions. Additional language should be added to your terms and conditions to address the issues discussed in this study. An illustration of one approach to the definition of fraudulent traffic and the safeguards that might be negotiated between advertisers and media companies is provided in the appendix of the full report (developed by Reed Smith, ANA's outside legal counsel). You should consult with your own counsel to develop specific provisions that best serve your company's individual interests (see Appendix B: Illustrative Terms and Conditions, on page 40 in the full report).

f. Use Third-Party Monitoring

Monitor all traffic with a consistent tool. We recommend relentless monitoring to get the best value out of your ad investment. Use monitoring and bot detection to reveal the bots in retargeting campaigns, weed bots out of audience metrics, and protect higher-value inventory that may have increased fraud exposure. Protect against ad fraud to be sure that bots are not being pushed into your media from other proactive stakeholders. Monitor your top-100 volume sites to prevent making payments to cash-out sites.

g. Use Frequently Updated Blacklists

For blacklists to be effective, they need to be updated at least daily, must be very specific (micro-blacklisting), and must accompany other defenses.

h. Announce Your Anti-Fraud Policy to All External Partners

In combination with covert, continuous monitoring practices, the watchdog effect will change behavior, reduce fraud, and encourage others to join the fight.

i. Equip Your Organization to Fight Ad Fraud: Budget for Security

Across many industries, the typical cost of security amounts to an overhead of 1 to 3 percent. In the credit card ecosystem, that security spending has lowered the losses due to fraud to just $0.08 per hundred dollars. Lowering bot fraud in advertising to those levels could potentially return many multiples of the security spending needed to achieve it.

j. Involve Procurement

Many ANA member companies have marketing procurement groups which should be a partner in the fight against bot fraud. The best marketing procurement organizations reduce waste and help improve marketing ROI by ensuring that every dollar is invested to deliver maximum growth and profitability. The fight against bot fraud can directly reduce waste and improve ROI, meeting procurement objectives.

k. Demand the Data

Ask suppliers for maximum visibility into bot levels in their inventory. Ask for third-party monitoring or certification of specific inventory to demonstrate that the inventory meets human impression requirements.

ACTION PLAN FOR PUBLISHERS, PLATFORMS, AND EXCHANGES

a. Continuously Monitor Sourced Traffic

Publishers should always monitor sourced traffic, know their sources, and maintain transparency about traffic sourcing. Publishers, platforms, and exchanges which are serious about reducing bot fraud should eliminate sources of traffic that are shown to have high bot percentages and monitor their vendors at all times.

b. Purge the Fraud; Increase Your Prices

Clean up the fraud in your supply. Once you can demonstrate higher value from higher valid impression percentages, the value of your media will increase.

c. Protect Yourself from Content Theft and Ad Injection

Use a service such as domain detection or bot detection to monitor for evidence of ad injection and for content scraping — from copying content from a site to in some cases monetizing the scraped content with ads on an unsanctioned site. A bot detection service can measure actual numbers of bots in high-bot traffic, allowing payment for the human audience while eliminating bots from the billing process.

d. Allow Third-Party Traffic Assessment Tools

Publishers can enable advertisers to improve the granularity of their traffic performance by authorizing third-party tracker measurement and third-party monitoring for characteristics such as viewability, engagement, and bot detection.

Bot Baseline:

FRAUD IN DIGITAL ADVERTISING

Key Findings Report

Download the full report at **www.ana.net/botfraudfindings2015**

ABOUT THE ANA

The ANA (Association of National Advertisers) provides leadership that advances marketing excellence and shapes the future of the industry. Founded in 1910, the ANA's membership includes nearly 700 companies with 10,000 brands that collectively spend over $250 billion in marketing and advertising. The ANA also includes the Business Marketing Association (BMA) and the Brand Activation Association (BAA), which operate as divisions of the ANA. The ANA advances the interests of marketers and promotes and protects the well-being of the marketing community.

ABOUT WHITE OPS

White Ops is the leading provider of cyber-security services for the detection and prevention of sophisticated bot and malware fraud. Unlike traditional approaches that employ statistical analysis, simple blacklisting, or static signatures, White Ops effectively combats criminal activity by actually differentiating between robotic and human interaction within online advertising and publishing, enterprise business networks, e-commerce transactions, financial systems, and more, allowing organizations to remove and prevent fraudulent traffic and activity. By working with customers to cut off sources of bad Internet traffic, White Ops makes bot and malware fraud unprofitable and unsustainable for the cyber-criminals—an economic strategy that will eventually eradicate this type of fraud.