ANA | whiteops

May 2017

BOT BASELINE 2016-2017

FRAUD IN DIGITAL ADVERTISING

Table of Contents

Special thanks to the following ANA member company participants

About the Study

For the third year in a row, White Ops and ANA have partnered to measure bot fraud in the digital advertising ecosystem. In this latest study, 49 ANA member companies participated. Their digital advertising activity between October 2016 and January 2017 was analyzed, with the concentration of activity in November and December.

Measurements of fraud in the global marketplace are derived from White Ops's platform customers with calibration from ANA study participant data where needed for granularity and financial loss estimation.

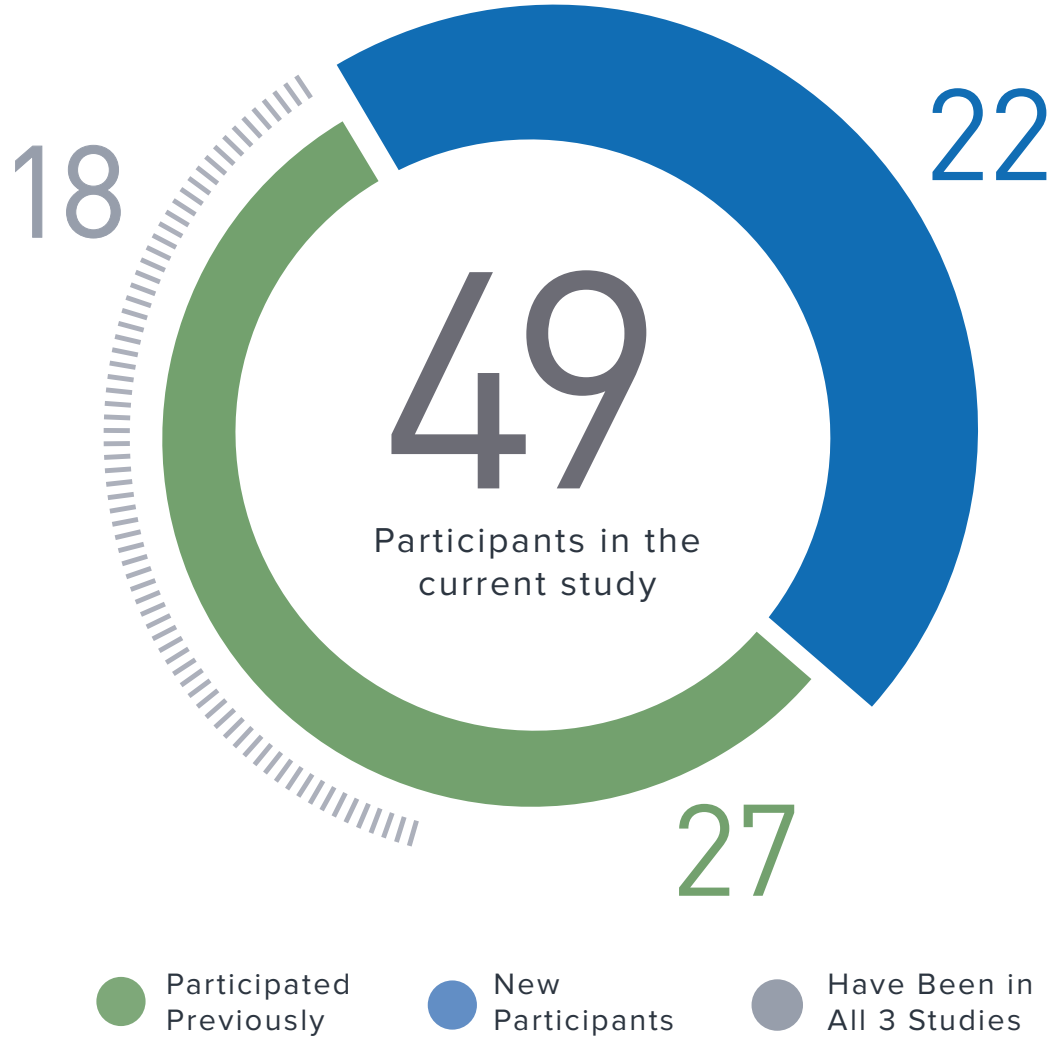
In this report we share:

- Baseline measurements of Sophisticated Invalid Traffic (SIVT), which does not include traffic which was blocked in a pre-bid fashion, social media, or direct marketing
- Practices related to the detection and prevention of digital advertising fraud
- Recommendations on best practices used by top performers to achieve impressive results

Number of Participants

Of the 49 participants in the current study, 27 participated previously (including 18 which have been in all three studies) and 22 participated for the first time.

Our study examines brand advertising by brand advertisers. It does not include search buys, pay-per-click (PPC) buys, or paid social media campaigns.



01

Topline Findings

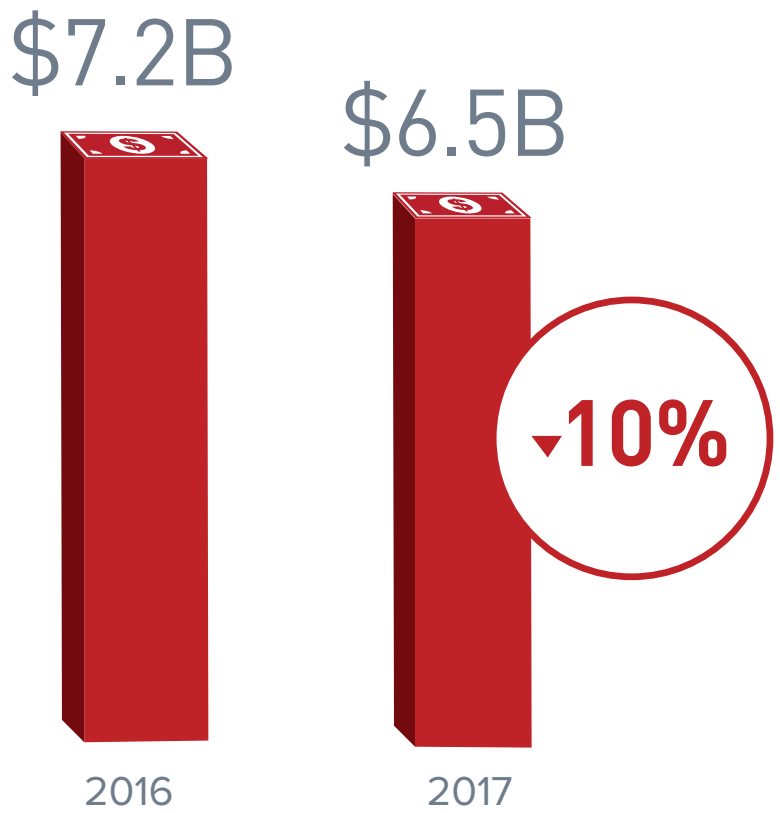
Topline Findings

The industry is adapting well to the fluid fraud landscape. The two top findings from our research:

Overall economic losses due to digital ad fraud have been reduced.

Fraud losses for 2017 are estimated to be $6.5 billion globally, down 10 percent from the $7.2 billion reported in last year's study. That 10 percent decline in global dollar losses is even more impressive considering that digital advertising spending is expected to increase by 10 percent in 2017[1].

Total Projected Fraud Losses ($B)



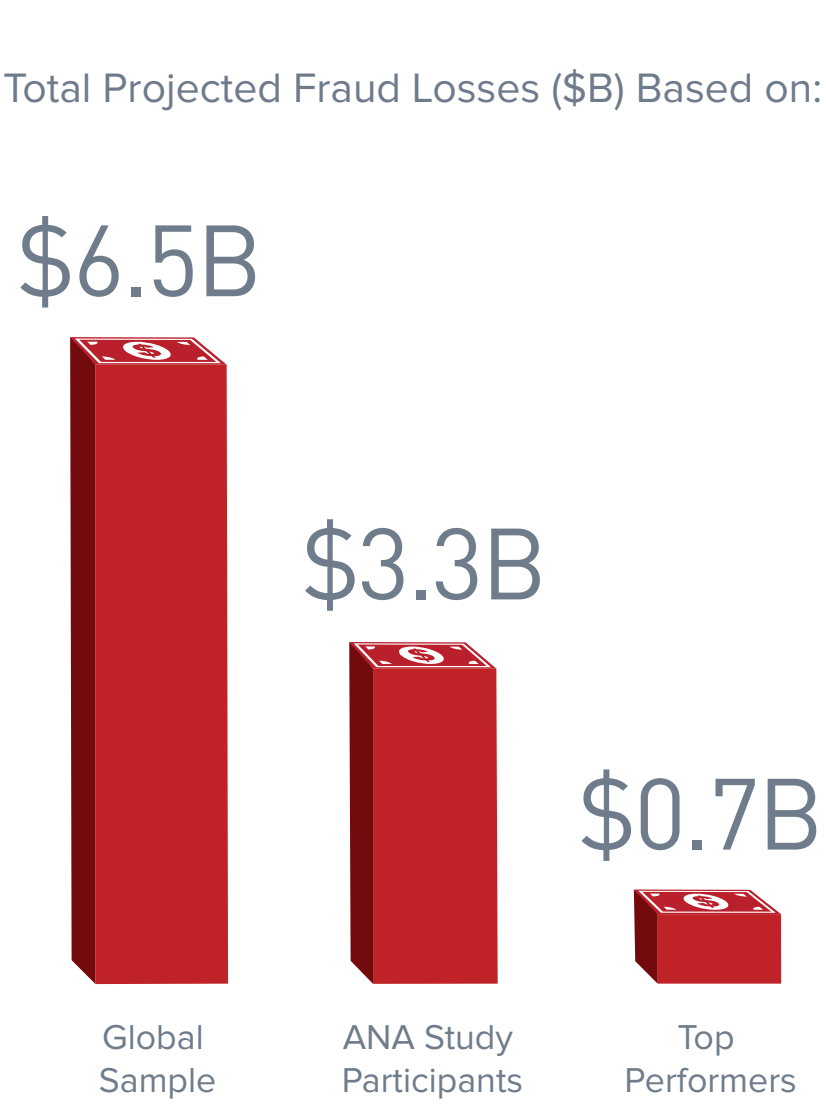
[1] PricewaterhouseCoopers: *Global Entertainment and Media Outlook* 2016–2020.

Gains among the 49 ANA member study participants were even more encouraging

It should be recognized that the ANA member participants no longer reflect the overall market (as they did in the first two White Ops/ANA studies). The 49 participants in this year's study have learned strategies and tactics to help fight fraud. Extrapolating the results of the 49 ANA member study participants to the overall market would result in overall fraud losses for 2017 of just $3.3 billion globally — about half that of the $6.5 billion projection noted above.

Furthermore, the very best ANA member performers — those study participants in the top quintile (20 percent) of performance — have shown even more dramatic positive outcomes. Extrapolated globally, those top performers would project **only $700 million lost globally to fraud in 2017.**

Therefore, a headline of this new research might be "The War on Digital Ad Fraud Is Winnable!" for those who pay attention and set proper controls.



02

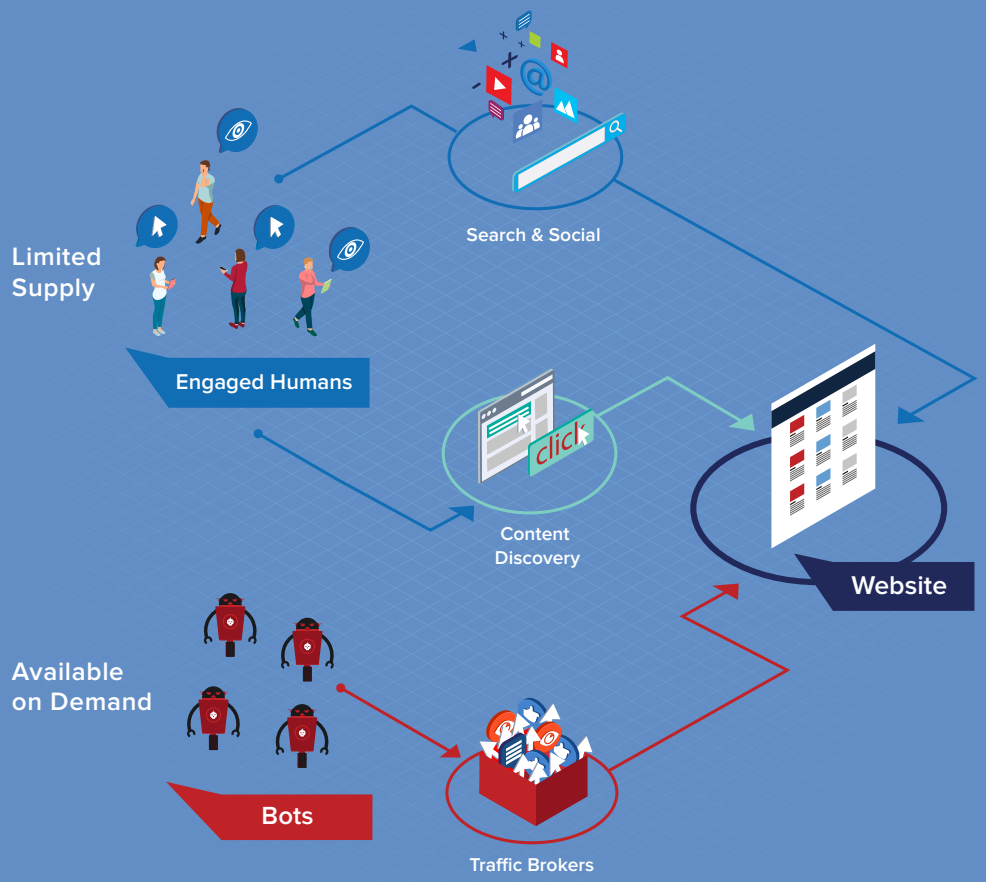
The Battle Continues: Gaining Ground in Some Areas, Losing in Others

> Levels of fraud are not constant throughout the year. Fraud is invited whenever and wherever digital advertising demand outstrips supply.

Traffic sourcing is still the top way bots make money.

Paid traffic acquisition, aka traffic sourcing, is an ordinary part of promoting a site to reach a larger audience. It is not inherently bad. But not all sources of traffic are equal. When a real website has a big bot audience, the bots are showing up because they were paid for. Behind every big bot problem, someone is paying a traffic source. We observed 3.6 times as much fraud coming from sourced than non-sourced traffic.

Publishers paying handsomely for legitimate search traffic are competing against publishers paying much less for bot traffic, and the tools used by most marketers cannot tell the difference. Botty traffic vendors may defeat detection, but they never have a credible explanation for why they are able to deliver high volumes of visitors. When a publisher finds a source of traffic for $0.01 per visit that gets scored as viewable and "high quality," some might call that a gold mine. We would call it a gap in bot detection.

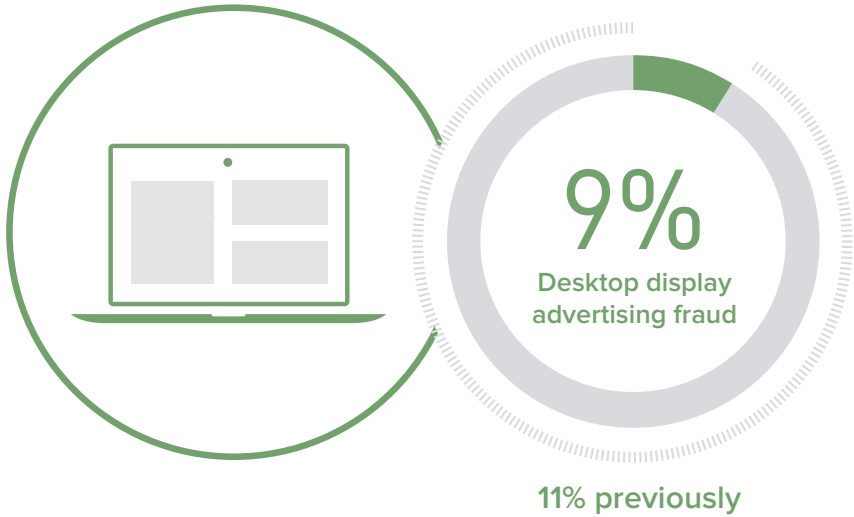


How Paid Traffic Acquisition — Traffic Sourcing — Works

There are many ways to source visitors to a website. Legitimate pay-per-click (PPC) search advertising, social media placements, and content discovery links bring new visitors at a high cost-per-visitor. Traffic brokers selling bot traffic claim to do the same thing, but provide arbitrarily large volumes of visitors in any kind of demographic at a much lower cost.

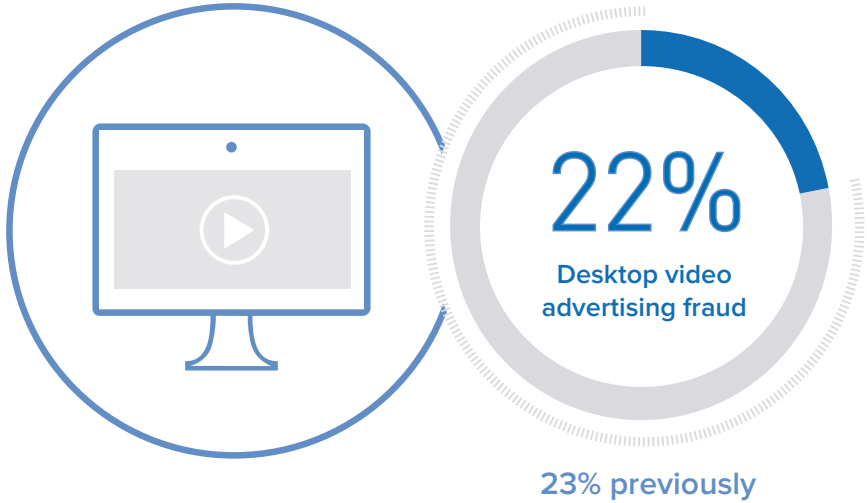
Fraud losses will amount to 9% of display spending.

This was a decline from the previous year, when fraud in desktop display advertising was 11 percent.



Fraud losses will amount to 22% of video spending.

This was comparable to the 23 percent fraud rate for desktop video in our last study. Desktop video remains a key target for fraudulent activity. The explosive growth there has created an insatiable demand for more inventory, and some publishers source traffic to meet demand. Furthermore, the higher CPMs of desktop video inventory create an opportunity for publishers to buy traffic at any price to show more desktop video ads.



Programmatic is no longer universally risky.

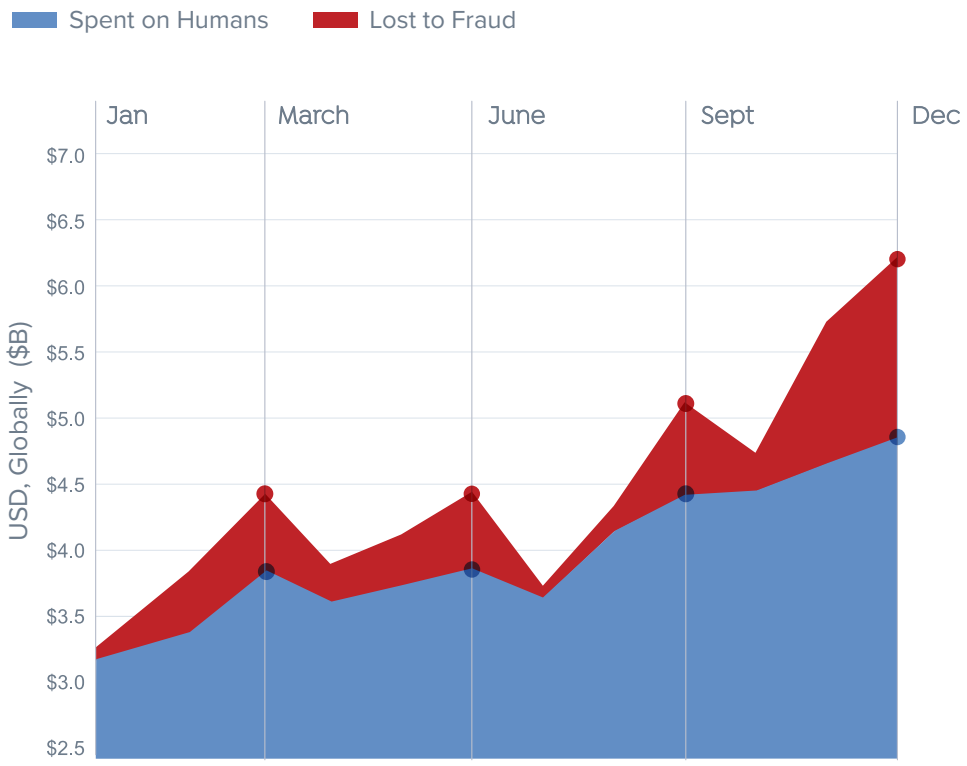
Past studies showed a consistently higher fraud risk in programmatic buying. That is no longer the case. Many study participants as a group observed comparable rates of fraud between programmatic buys and direct buys.

Contrary to last year, when programmatic buying was a strong risk factor for fraud, many programmatic platforms have instituted such sophisticated security controls against botty traffic sourcing that they have been able to outperform direct buys. This is thanks to the introduction of strong security measures that remove bad actors and discourage publishers from experimenting with risky traffic sources.

Seasonality demands continue to outweigh media supply, exacerbating fraud.

Due to a new study data collection period — a concentration in November/December versus August/September in prior studies — we observed fraud levels jumping at key holiday periods, specifically Black Friday and Cyber Monday. Fraud levels lowered and stayed more consistent for flat spenders for the remainder of the holiday season, while fraud levels for seasonal spenders continued spiking throughout the entire period. While spikes in fraud at the end of a quarter are not new information, this observation has huge implications for advertisers and how they manage spending across the year. Now armed with the knowledge that fraud moves in tune with seasonality, planning and buying in a manner countercyclical to industry norms may be a strategy to help minimize fraud.

Monthly Total Ad Spend ($B)



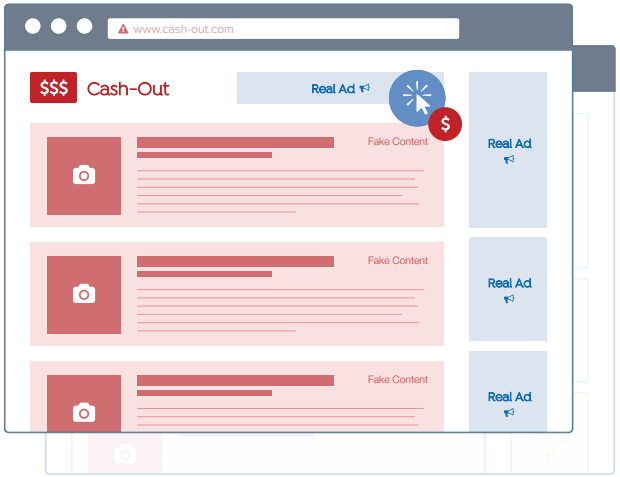
Fraud Levels Are Not Constant Throughout the Year

Digital ad fraud is not exempt from the laws of supply and demand. Economic modeling on Standard Media Index's Ad Market Tracker [2] data on total U.S. digital ad spending illustrates how fraud infiltrates the market whenever demand outstrips supply. This is especially prominent at the ends of quarters when publishers rush to fill their orders.

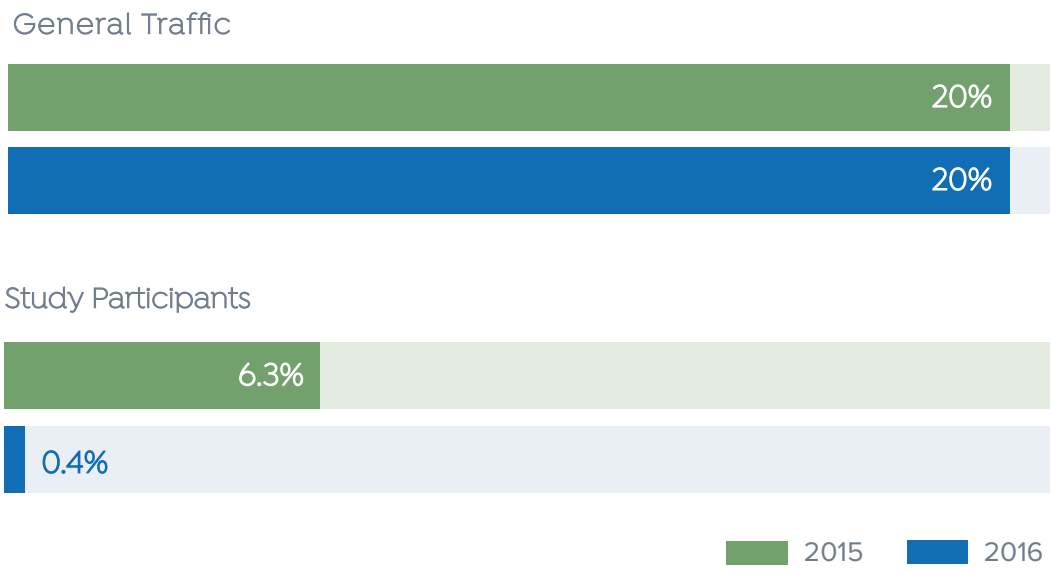
[2] Standard Media Index: SMI Ad Market Tracker http://www.standardmediaindex.com/Ad-Market-Tracker.html.

Sites built specifically for bot fraud — "cash-out sites" — accounted for 20% of all domains.

Across the entire buying universe, sites with nothing but bot visitors make up about a fifth of all the world's websites. However, this year's study participants spent much less money on the long tail where these sites concentrate than their peers. They saw a stark decline (from 6.3 percent to 0.4 percent) in the total cash-out domains that appeared in their spending.



Percentage of Domains Identified as Cash-Out Sites



Mobile fraud is much lower than feared.

Overall, participants saw less than 2 percent fraud in app and mobile web display buys. This result stands in stark contrast to public estimates of outrageous levels of mobile fraud, which are largely based on volumes of suspicious traffic, not a dollar-weighted analysis of actual spending lost to fraud.

This surprising finding is driven by three factors limiting the growth of fraud in mobile. First, lower CPMs and a lower number of ad units on the mobile web decrease the profit margin for publishers buying traffic. Second, the growth of in-app fraud is limited by the install base of fraudulent apps; everyone, including fraudsters, has a hard time getting lots and lots of people to install their apps. Finally, while counterfeit inventory on programmatic platforms is a problem, especially when viewed as a percentage of all programmatic bid requests, on a dollar-weighted basis it is still a small problem, because it does not often achieve a very high price.

There are some notable exceptions that do not affect the typical brand advertiser, but may affect you. Mobile web video continues to be a notorious hotbed of fraud — how often, as a consumer, are you really seeing a video ad launched *by your browser?* — but was not purchased in much volume by study participants. Similarly, while not the focus of this study, pay-per-click and pay-per-install campaigns face high fraud risks for those marketers, but affect very little brand advertising spend.

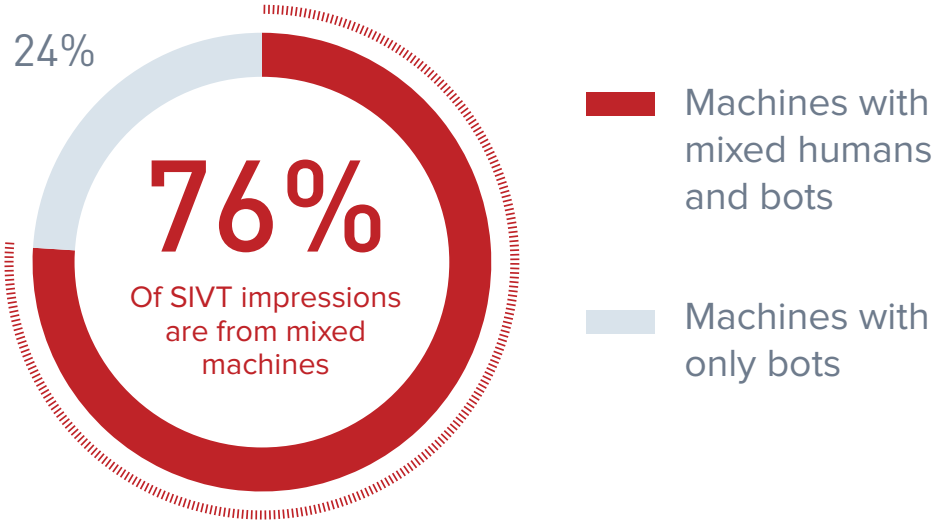
03

The Evasive Adversary: Why Ad Fraud Continues to Exist

Observed fraud made a substantial decline, but the battle is far from over. Bots continue to evade detection (despite 80 percent of participating brands deploying some form of countermeasure) and will net $6.5 billion globally in 2017. There are three reasons why fraud continues to exist at scale:

1. Bots are getting better at resembling humans.

Bots are exhibiting many behaviors that cause them to look more human, which have made them more deft at evading detection. For example, over 75 percent of the fraud observed in this year's study came from computers containing both a human and a bot on the same machine.



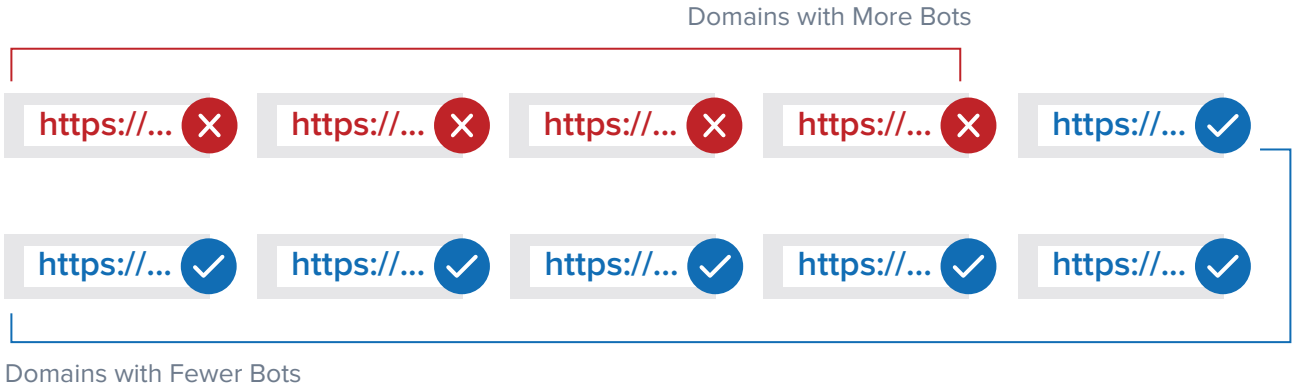
2. Bots game detection mechanisms.

The fraud prevention process is often thought of as a "one-way" street: the bot executes and the fraud detection detects the bot. However, the reality couldn't be more different. Publishers buy and traffic brokers sell bot traffic that doesn't get caught. Publishers and networks that buy traffic use feedback loops with verification companies and advertisers, and adjust their sources accordingly.

3. A false sense of security enables fraud to thrive.

If fraud happened only in the places people expect, those places would be cheap and the total losses small. A great example of this is the fraud we observed in private marketplaces, traditionally thought of as very clean, protected, premium sources of fraud-free inventory. But when spending surges, botty traffic sourcing is just as pervasive in private marketplaces as elsewhere. Unless a private marketplace is specifically engineered to be immune to publishers buying evasive bot traffic, it will have just as much of a bot problem as any other kind of buy. In fact, looking at all the domains that buy bot traffic and sell via PMPs, 40 percent of the time we actually observed *higher* bot levels on their PMP deals than their non-PMP deals.

PMP Buyers Beware: 40% of Domains Had More Fraud on Private Buys than Outside PMPs



But the 49 ANA participants were able to make even more substantive headway against the increasing sophistication of fraud. As detailed in the following section, ANA participants leveraged fraud reduction strategies that drove down the incidence of fraud by almost 50 percent. And the top performers did even better.

04

The War on Digital Ad Fraud Is Winnable: Top Performer Best Practices

Top performers (those study participants in the top quintile of performance) observed the smallest desktop display or desktop video SIVT percentage over the entire measurement period among this year's 49 participants. Seventy percent of those top performers returned from previous studies. In fact, we would project only $700 million globally in overall 2017 fraud losses had the entire industry performed as well as these top study performers. Top performers demonstrate that sustained fraud levels on desktop under 2 percent is a reasonable, achievable goal, and our recommended action steps are drawn from what these participants have put into practice.

$700MM

Projected 2017 fraud losses had the entire industry performed as well as top study performers

LESS THAN **2%**

Sustained fraud levels on desktop is reasonable and achievable

Pre-Campaign Checklist

The planning period of a campaign provides not only insight into a partner's capabilities but also grounds to shape the relationship and activity. We encourage buyers to set a new standard for partnerships that revolves around transparency of activity, data collection and tracking, and setting campaigns up for success. These are the actions we recommend before signing any paperwork:

Pre-Campaign Checklist

Demand transparency from all vendors.

Fraud tends to thrive in areas of opacity. Seek out specifics about pricing, traffic sourcing, and the extent of audiences being delivered via owned and operated domains vs. audience extension[3]. Buyers need to demand this transparency, and if it's not offered, reconsider the relationship.

Demand transparency about traffic sources.

While there are plenty of legitimate third-party sources of traffic — for instance, paid search — traffic sourcing is the most common way in which bot masters make money, by selling visits to publishers. Bot masters sell visitors on a cost-per-click basis. Advertisers must be aware of sourced traffic and work with their media agency to clearly understand its use in the media schedule. Buyers should demand transparency from publishers about traffic sources and build language into RFPs and insertion orders that requires publishers to identify all third-party sources of traffic. An illustration of one approach, developed by Reed Smith, the ANA's outside legal counsel, is:

> "Media Company shall disclose to Advertiser and Agency in writing (and update on an ongoing basis) its practices for sourcing third-party traffic."

You should consult with your own counsel to develop specific provisions that best serve your company's individual interests.

[3] Audience extension: Behavioral targeting reaching a publisher's audience beyond its own site and on other sites that belong to the same ad network.

Pre-Campaign Checklist

Demand 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 demand transparency from publishers around audience extension and build language into RFPs and insertion orders 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.

Implement proper tracking to collect the data needed to make correct decisions.

Advocate for independent, robust third-party SIVT measurement of all your supply and publisher partners. This means enforcing the latest video standards with publishers to ensure third-party tag execution — either VAST 4.0[4] or VPAID[5] player support.

Also, asking for JavaScript execution with third-party measurement providers to directly measure SIVT exposure versus 1x1s[6] will allow you to collect more data. This allows you to more accurately determine fraudulent activity and make better decisions.

[4] VAST: Video Ad Serving Template, the universal specification developed by the IAB for serving video ads.
[5] VPAID: Video Player Ad-Serving Interface Definition, used in establishing a common interface between the video ad and video player.
[6] 1x1: Pixel-based tracking that is limited with data collection.

Pre-Campaign Checklist

Include language on non-human traffic in your terms and conditions.

Insertion orders should include language that the company will only pay for non-bot impressions and not IVT or SIVT. 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 by the ANA** (developed by Reed Smith, the ANA's outside legal counsel). You should consult with your own counsel to develop specific provisions that best serve your company's individual interests.

Look skeptically at narrow targeting and cheap reach.

In any situation where supply does not meet demand for a target audience, fraud will follow. Avoid too many actions that restrict potential supply (e.g., too many targeting parameters at once). Furthermore, fraud protection isn't free, so the lowest CPMs may not include sophisticated protection measures — even the simplest, cheapest bots go unnoticed.

Thus, focusing on only cost-efficient rates can be especially risky if it both restricts supply and removes protections. The top performers spent little on bargain inventory and thus were spared from this concentration of fraud.

Pre-Campaign Checklist

Set the correct metrics for success.

Recognize that viewability and fraud are not the same thing. They must be reviewed separately, and with best-in-class solutions. Media Rating Council (MRC) is the industry body that accredits third-party companies for their measurement processes. For SIVT detection/filtration, the current MRC-accredited list can be found **here.**

Encourage MRC-accredited third-party fraud detection on walled gardens.

The large digital media companies referred to as “walled gardens” are strongly encouraged to work with MRC-accredited third-party fraud detection companies to support SIVT detection. Marketers should be able to hold every publisher and platform accountable in a consistent and trustworthy way. While some large digital media companies have taken steps toward seeking MRC accreditation, others have not done so yet.

Active Engagement

Any successful digital media campaign requires monitoring, analyzing, and implementation of learnings. Fraud detection and prevention are no different in that sense. We encourage you to do the following not only on your own but with your various partners to review, understand, and ensure your digital media is being seen by your target audience: humans.

Active Engagement

Use audience anti-targeting to cut fraudulent audiences.

New computers are getting infected every day, and bots frequently refresh cookies. But regularly updating anti-targeting segments to exclude known botty IP addresses, User IDs, and Device IDs can be effective if refreshed frequently.

Use domain anti-targeting or exclusion lists to cut fraudulent domains.

Many websites — 20% of all the domains we saw — are dedicated to fraud. New domains are registered all the time for this purpose. But regularly updating domain exclusion lists to exclude known cash-out sites can be effective if refreshed frequently.

Use your DMP as a fraud-fighting tool.

If possible, stream log-level data directly from your data management platform (DMP) into your programmatic platforms to avoid serving ads to fraudulent user IDs and Device IDs. Regular or real-time updates are crucial: if traffic buyers can iterate through botty traffic sources until they find the one that you don't catch, they will.

Active Engagement

Engage partners when they're not meeting your goal.

Set a goal for fraud levels at the campaign start and engage with partners when their fraud levels do not reduce. Good partners are transparent and active partners.

Understand your activity.

Study placements, campaigns, tactics, publishers, and seasonality to identify trends you can apply to future campaigns to help you avoid fraud. Understand the types of fraud you encounter and where you can reach your human-concentrated audiences.

Disincentivize bad behavior.

Develop and communicate consequences for bad actors. Each brand has different needs and solutions, but should develop and communicate consequences for bad actors (domains, placements, partners, etc.) that consistently attract fraud. Some players will never steal from you. Some will always steal from you. The rest look at how you treat those two.

05

Embrace the Industry's Fraud-Fighting Resources

The fight against fraud is industry-wide. Be aware of the work other industry groups are doing and embrace it.

Register with the Trustworthy Accountability Group (TAG) and consider becoming TAG-certified.

TAG's products and services fight fraud, malware, and piracy while promoting a transparent digital supply chain.

Require all vendors that touch your digital media to be certified by TAG.

Working with only TAG-certified vendors ensures that every company which touches your digital media is using products that have been custom-designed to reduce fraud levels in the system.

At a minimum, ensure verification vendors are accredited by MRC.

Vendors that screen for fraud should be accredited by MRC and compliant with the most recent SIVT guidance released in 2017.

Demand AAM Quality Certification of publishers in your supply chain.

The AAM (Alliance for Audited Media) Quality Certification program is focused on minimizing digital advertising fraud by linking advertisers with Quality Certified publishers. The process verifies publishers' business processes, website analytics, and website audiences.

About the Study Partners

About the ANA

The ANA (Association of National Advertisers) makes a difference for individuals, brands, and the industry by advancing the interests of marketers and promoting and protecting the well-being of the marketing community. Founded in 1910, the ANA provides leadership that advances marketing excellence and shapes the future of the industry. The ANA's membership includes more than 1,000 companies with 15,000 brands that collectively spend or support more than $250 billion in marketing and advertising annually. The membership is comprised of more than 700 client-side marketers and nearly 300 associate members, which include leading agencies, law firms, suppliers, consultants, and vendors. Further enriching the ecosystem is the work of the nonprofit Advertising Educational Foundation (AEF), an ANA subsidiary, which has the mission of enhancing the understanding of advertising and marketing within the academic and marketing communities.

About White Ops

White Ops is the global leader in bot detection and human verification on the Internet. The company's mission is to defend the open Internet and make everyone more secure by disrupting the profit centers of cybercrime. White Ops works globally with companies and industry groups that are dedicated to preventing malicious activity in advertising. White Ops is headquartered in New York City. To learn more please visit www.whiteops.com.

BOT BASELINE 2016–2017

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