MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

March 24, 2025

The Honorable Andrew Ferguson
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Chairman Ferguson:

I am writing to express my continued concern about some companies within the digital advertising industry charging U.S. Government (USG) customers, and by extension American taxpayers, for services that they are not actually delivering to USG customers. Research indicates that certain ad verification companies are making apparently false and misleading claims about the capability of their products to avoid bots and ensure paid-for ad content reaches humans.

New research[1] from cybersecurity and digital forensics firm Adalytics shows that major advertisers – including non-profits and numerous US federal, state, and municipal government entities – have had their ads served to bots operating out of data centers rather than authentic human audiences. Dozens of major ad exchanges ("SSPs"), ad buying platforms ("DSPs"), and media agencies were seen serving these ads to easily identifiable[2] bots.

In 2016, Senator Schumer and I wrote to then-Chairwoman Edith Ramirez to express frustration with the growing phenomenon of digital advertising fraud ("ad fraud").[3] I voiced my concerns about bots plaguing the digital advertising space by creating fake consumer traffic, artificially driving up the cost of advertising in the same way human fraudsters can manipulate the price of a stock by creating artificial trading volume. In 2018, I wrote then-Chairman Joseph Simons to

[1] On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?, Adalytics (Mar., 2025), https://adalytics.io/blog/prebid-bot-filtration.
[2] HTTP Archive bot is on the IAB Bots and Spiders List. *See,* Interactive Advertising Bureau, *IAB/ABC International Spiders and Bots List*, IAB (2025), https://www.iab.com/guidelines/iab-abc-international-spiders-bots-list/ (last visited Mar 5, 2025).
[3] Sens. Warner & Schumer Call on FTC to Protect Consumers from Digital Ad Fraud, https://www.warner.senate.gov/public/index.cfm/2016/7/sens-warner-schumer-call-on-ftc-to-protect-consumers-from-digital-ad-fraud (last visited Mar 5, 2025).

emphasize the systemic nature of the state of digital advertising fraud, whereby major ecosystem stakeholders engage in willful blindness to fraudulent activity.[4]

Today, digital advertising fraud is estimated to comprise $84 Billion of the $700 Billion global digital advertising industry.[5] While ad fraud schemes have become more sophisticated during this time, the greatest cause for concern is in the industry's failure to take action on even the most basic forms of waste[6]. This new research highlights the role of ad verification companies Integral Ad Science (IAS), DoubleVerify, and HUMAN Security (f.k.a. "White Ops"), whose core offerings claim[7] to provide independent bot filtration and detection. Despite their advertising claims to target and deliver ad content to humans, data suggests that these ad verification vendors appear to be misclassifying bot traffic as human, and in turn delivering content from U.S. Government agencies, including ads from the U.S. Army, U.S. Navy, Healthcare.gov, Department of Homeland Security, United States Postal Service, and others, to bots. The failure to deliver these services as claimed would mean that the taxpayers are not getting what they have paid for.

The failures and misrepresentations of these verification vendors amount to far more than simple contradictions of their marketing puffery. As publishers and advertisers rely on these services' asserted ability to avoid bot traffic and deliver content to customers, these verification firms serve as cover for the systemic failure by key ecosystem stakeholders, potentially compromising a significant sector of the online ad market. Failure to meet the terms of contracts result in the misuse of taxpayer dollars, and undermine the efficacy of government public awareness and job recruitment campaigns.[8] These failures drive inflated ad costs and reduced effectiveness for thousands of small and midsize businesses and charities that rely on digital advertising to succeed, and these increased costs trickle down to consumers who end up paying more for basic goods and services.

The ad verification companies identified in the research offer "pre-bid targeting" services that are claimed to prevent advertisers from bidding on ad impressions that do not adhere to industry self-defined quality requirements, such as invalid traffic (e.g. bots).[9] However, evidence

---

[4] Warner Calls on FTC and Google to Address the Prevalence of Digital Ad Fraud, https://www.warner.senate.gov/public/index.cfm/2018/10/warner-calls-on-ftc-and-google-to-address-the-prevalence-of-digital-ad-fraud (last visited Mar 5, 2025).

[5] Quantifying the cost of ad fraud: 2023-2028, (2023), https://fraudblocker.com/ad-fraud-data-facts (last visited Mar 5, 2025).

[6] For avoidance of doubt, the "Invalid Traffic" bot detection failures discussed in the research do not constitute "advertising fraud" under industry definitions. Instead, this is considered to be a form of General Invalid Traffic ("GIVT"). *See* Media Rating Council, *Invalid Traffic Detection and Filtration Standards Addendum*, (2020); On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?, *supra* note 1.

[7] On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?, *supra* note 1.

[8] *See, e.g.* Ryan Barwick, *DOJ, NCIS Ask Ad Executives about Brand-Safety Companies*, Marketing Brew, https://www.marketingbrew.com/stories/2024/10/11/doj-ncis-brand-safety-google-integral-ad-science-doubleverify (last visited Mar 5, 2025). ("[O]fficials have also asked about how advertisers work with the ad verification companies Integral Ad Science and DoubleVerify, which sell services that claim to prevent ads from running against objectionable content, detect fraud, and measure digital ads").

[9] Interactive Advertising Bureau, *supra* note 2.

suggests that U.S. Government advertisers were charged by ad verification companies for ad verification services that do not perform as claimed.

Several of these ad verification firms, such as Human Security[10], claim publicly to perform real-time bot detection by evaluating every potential ad impression to avoid bidding on or serving ads to bots.[11] While such real-time detection would require the vendors to have access to the "User-Agent"[12] attribute during a real-time programmatic ad auction, it is unclear the extent to which DSPs actually supply this information to verification firms in real time.[13] In other words, if verification vendors do not have access to this data, they could not possibly complete the verification processes they claim to.

These vendors also offer tools to publishers. One such firm, Integral Ad Science ("IAS") offers "publisher optimization" technology which specifically claims to identify invalid traffic resulting from "known spiders and bots" and "originating from servers in data centers."[14] Despite IAS' alleged unique three-pillar approach "providing the most accurate detection and prevention," its technology appeared to label certain bots as legitimate human traffic 77% of the time.[15]

Where verification vendors market themselves as performing real-time bot detection to stop ads from serving to declared bots, promising comprehensive coverage, and yet fail to prevent ads from serving to bots even in instances where those bots are on an industry body bot list, we think there is reasonable grounds for the Commission to investigate if those claims constitute an unfair and deceptive trade practice under Section 5 of the Federal Trade Commission (FTC) Act.

---

[10] Google executives recently testified in the United States District Court for the Eastern District of Virginia about the company's partnership with HUMAN security, formerly known as White Ops, in combatting ad fraud. *See also, Testimony of Per Bjorke, Trial Update: September 24 – Google Says It's the Guardian of the Industry, but DOJ Says Not So Fast, U.S. V. GOOGLE ADS TRIAL TRACKER (Sept. 24, 2023), https://www.usvgoogleads.com/trial-updates/trial-update-september-24-google-says-its-the-guardian-of-the-industry-but-doj-says-not-so-fast.* Documents surfaced in the course of the trial demonstrate that Google believes HUMAN's capabilities to be more sophisticated than its peers; yet, HUMAN was among the ad verification firms that failed to prevent ads from serving to declared, easily-identifiable bots. *See* Google, *Display, Video Ads, Analytics and Apps*, 141 (2020), https://storage.courtlistener.com/recap/gov.uscourts.vaed.533508/gov.uscourts.vaed.533508.1132.2_1.pdf (last visited Mar 5, 2025). ("Our assessment is that WhileOps is significantly better than the other vendors in terms of anti ad-fraud technology and expertise.")

[11] *See, e.g.* The Trade Desk Partners with White Ops to Become First Advertising Platform to Block Fraudulent Impressions Before They Are Purchased, https://perma.cc/UBX5-JEK4 (last visited Mar 5, 2025).

[12] User-Agent, MDN (2025), https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent (last visited Mar 5, 2025).

[13] In relation to Senator Blackburn and Senator Blumenthal's inquiry regarding CSAM monetization, DoubleVerify recently stated that their measurement is predicated on historical ad impression volume instead of real-time scanning of the internet at scale. *See* DoubleVerify, *Statement on Adalytics Report*, (2025), https://doubleverify.com/statement-on-adalytics-report/ (last visited Mar 5, 2025).) This appears contradictory to previous claims of comprehensive coverage related to their brand safety products, cited in the Senators' inquiry, raising questions of whether there are similar false advertising claims applicable to their bot detection capabilities. *See, e.g.* Senator Blackburn and Senator Blumenthal letter to DoubleVerify CEO, Mark Zagorski, (2025).

[14] Fighting Invalid Traffic: A comprehensive guide to understand and mitigate invalid traffic on your sites., https://go.integralads.com/rs/469-VBI-606/images/IAS_Publisher_Fraud_Checklist_Guide_US.pdf (last visited Mar 5, 2025).).

[15] On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?, *supra* note 1.; IAS Ad Fraud Protection, https://go.integralads.com/rs/469-VBI-606/images/IAS_Fraud_Overview_One_Sheet_US.pdf (last visited Mar 5, 2025).

If ad verification vendors lack the technical capability or otherwise fail to meet their advertising claims about real-time detection, charging for those services creates a concrete harm to American businesses, US Government entities, taxpayers, and citizens at large, and warrants the FTC's urgent attention.

Accordingly, I request that you investigate this issue and provide a response to the following questions no later than April 28, 2025:

1. Did verification vendors such as Integral Ad Science ("IAS"), DoubleVerify ("DV"), and HUMAN Security, among others, claim in their marketing materials to be able to perform real-time bot filtering and have the capability to prevent ads from serving to declared bots, such as those on the IAB Bots & Spiders List?
2. Do these verification vendors receive access to the "User Agent" field in real-time programmatic ad auctions from demand side platforms like Google DV360 and the Trade Desk?
3. Can the verification vendors' pre-bid technology actually stop ads from serving to declared bots on the IAB Bots & Spiders List, or merely prevent ads from serving on website domains with historically high levels of bot traffic? If the latter, what evidence exists that can demonstrate specific websites are getting blocked, deliberately or inadvertently, from ad campaigns and thus de-monetized?
4. If the verification vendors do not receive access to the User-Agent and cannot block declared bots, did these vendors make false advertising claims and engage in deceptive trade practices when promoting their pre-bid bot avoidance or suspicious activity blocking technology?
5. What is the extent of the resulting financial harm to the United States government and non-profit advertisers, as well as to publishers that paid for this ineffective bot avoidance technology?

This investigation is vital to prevent further waste of the advertising dollars of American businesses, non-profits, government entities, and by extension, American taxpayers. I encourage you to look closely at this issue, and the roles of all actors in this field that facilitate fraudulent activity in the online market.

Sincerely,

Mark R. Warner
United States Senator