MARK R. WARNER
VIRGINIA

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

United States Senate
WASHINGTON, DC 20510–4606

March 24, 2025

The Honorable Pamela Bondi
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

Dear Attorney General Bondi:

I am writing to express my deep concern regarding significant evidence that several advertising technology companies contracted by U.S. Government (USG) agencies have, for at least five years, failed to deliver the services they promised. This failure has resulted in harm to taxpayers and has undermined the efficacy of public awareness campaigns, recruitment efforts, and critical government services. Research indicates that ad verification firms Integral Ad Science (IAS), DoubleVerify (DV), and HUMAN Security (HUMAN) have misrepresented their capabilities to perform real-time bot detection and filtration to USG agencies, as well as to commercial advertising technology firms that rely on their verification services to make assurances to their own USG customers.

New research from cybersecurity and digital forensics firm Adalytics[1] reveals that several federal agencies[2], such as the U.S. Army, U.S. Navy, U.S. Department of Health and HUMAN Services (HHS), the U.S. Census Bureau (Census), the Department of Homeland Security (DHS), the Center for Disease Control and Prevention (CDC), and the United States Postal Service (USPS), have had their advertisements served to easily-identifiable bots, rather than the intended human audiences since at least 2020.[3] These findings suggest that ad verification companies have charged or received payment from the federal government for services that do not perform as represented in their contracts and advertising, thereby misusing taxpayer dollars.[4] Earlier research indicates that verification firms have offered faulty products since at least 2016. This raises questions of whether government payment for services not rendered began

[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] In addition to the federal agencies listed, several state and municipal government entities also had their ads served to bots for several years, including government agencies in New York (nystateofhealth.com, and NYPD), Utah, Oregon, Florida, Indiana, and Virginia.
[3] On pre-bid bot detection and filtration, *supra* note 1.
[4] *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").

even earlier[5], and continues to this day, to the detriment of the American government and at taxpayers' expense.

The claims made by these ad verification firms—that they provide real-time bot detection to filter out invalid (e.g. bot)[6] traffic—appear to be false. While these companies advertise their technology as able to filter out invalid traffic before ads are served ("pre-bid"), evidence shows that they have failed to prevent ads from reaching easily identifiable bots, even when they are included in industry-recognized bot lists, such as the Interactive Advertising Bureau's (IAB) Bots & Spiders List and TAG Data Center IP List.[7] For example, while IAS claims publicly to offer "the most accurate detection and prevention," its technology appeared to label certain bots as legitimate human traffic 77% of the time.[8]

Several of these ad verification firms, such as HUMAN Security[9], claim publicly[10] to perform real-time bot detection by evaluating every potential ad impression to avoid bidding on or

---

[5] *See* Shailin Dhar, *Mystery Shopping Inside the Ad-Verification Bubble*, SLIDESHARE (2016), https://www.slideshare.net/slideshow/mystery-shopping-inside-the-adverification-bubble/62857862 (last visited Mar 23, 2025) (IAS was able to correctly identify only 17% of the bot traffic Mr. Dhar paid to run against an artificial website he created. Mr. Dhar says: "83% of the robotic traffic we purchased was considered human by the Integral Ad Science filter. When I informed the source traffic vendor that the rate was 17% they said that the Integral Ad Science sampling got lucky because it's usually around 5%".).

[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] 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); Trustworthy Accountability Group, *Eliminate Fraudulent Traffic*, https://www.tagtoday.net/fraud (last visited Mar 22, 2025); admin, *Trustworthy Accountability Group (TAG) and Digital Ad Leaders Announce New Program to Block Fraudulent Data Center Traffic*, https://www.tagtoday.net/pressreleases/tag-and-dal-announce-new-program-to-block-fraudulent-data-center-traffic (last visited Mar 22, 2025) ("TAG will initially use Google's database of data center IP addresses and enhance it based upon broader industry intelligence.").

[8] 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).

[9] 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* Transcript of Bench Trial at 56, United States v. Google LLC, No. 1:23-cv-00108 (E.D. Va. Sept. 24, 2024) (PM Session) (Brinkema, L.) (testimony of Per Bjorke) (Montgomery, Court Reporter). 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*, (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.")

[10] *See* e.g. Brand Suitability Series Part 3: How Blocking Works, DOUBLEVERIFY (Mar. 18, 2020), https://web.archive.org/web/20241009000816/https://doubleverify.com/brand-suitability-series-part-3-how-blocking-works/ (last visited Mar 5, 2025) (On a DV webpage apparently removed some time after October 2024: "DV offers the most comprehensive and accurate pre-bid avoidance targeting available in the market [...] Our millions of fraud signatures are updated nearly 100 times per day (every 15 minutes) in our DSP integrations to ensure near-immediate programmatic protection from invalid traffic."); Capabilities - Fraud, DOUBLEVERIFY, https://doubleverify.com/capabilities-fraud/ (last visited Mar 23, 2025)("We're accredited by the Media Rating Council (MRC) for monitoring and blocking across devices — including mobile app, and our AI-backed deterministic methodology results in greater accuracy, fewer false positives and, ultimately, superior protection for brands."); IAS Xandr DSP User Guide, https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf (last visited

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, there is reason to believe that these firms do not receive this information 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. The failure to deliver these services as claimed would mean that the taxpayers are not getting what they have paid for. Further, by failing to disclose their inability to perform contracted services, these firms may have concealed or avoided an obligation to repay funds to the government, potentially creating additional liability under the False Claims Act.[14]

This is not the first time that ad verification firms misrepresented their real-time fraud detection capabilities in furtherance of fraud. Indeed, on March 20th, 2025, the former CEO of ad verification firm Kubient was sentenced to prison in the Southern District of New York for defrauding investors. According to acting U.S. Attorney Matthew Podolsky, the convicted former CEO "lied to investors and auditors about his company's revenue and about his company's premier product: an AI-powered tool that, ironically, was supposed to detect fraud in the digital advertising industry."[15] Kubient, like IAS, DV, and HUMAN, made lofty claims about its "real-time" bot prevention capabilities, and boasted its good standing with industry self-regulatory bodies.[16] Today, we see that these same misrepresentations harm not only the investing public, but American taxpayers at large.

The apparent misrepresentations and non-performance of these firms represents not only a failure to meet their contractual obligations, but also a potential violation of the False Claims Act[17]. If

---

Mar 5, 2025) ("IAS' Ad Fraud Solution utilized multiple detection methodologies for maximum protection. This three-pillar approach is marketed as being "powered by unmatched scale and machine learning, providing the most accurate detection & prevention.")

[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] While HUMAN Security *may* receive special access to some data, which may include User-Agent through its partnerships directly with advertising technology platforms, there is reason to believe his may not be the case for DV and IAS. Nevertheless, each of these entities has been unsuccessful in preventing ads from serving to easily-identifiable bots on industry bot lists. In addition, in relation to Senators Blackburn and Blumenthal's inquiry regarding CSAM monetization, DoubleVerify recently stated that its measurement methodology relies on historical ad impression volume rather than real-time scanning of internet content at scale. See DoubleVerify, Statement on Adalytics Report (2025), https://doubleverify.com/statement-on-adalytics-report/ (last visited Mar. 5, 2025). This statement appears contradictory to previous claims of comprehensive coverage related to their brand safety products referenced by the Senators, raising questions regarding the validity of similar advertising claims about DoubleVerify's bot detection capabilities. See Letter from Sens. Marsha Blackburn & Richard Blumenthal to Mark Zagorski, CEO, DoubleVerify (2025) (on file with author). See also Transcript of Bench Trial at 57, United States v. Google LLC, No. 1:23-cv-00108 (E.D. Va. Sept. 24, 2024) (PM Session) (Brinkema, L.) (testimony of Per Bjorke) (Montgomery, Court Reporter) ("Because an outside vendor will not have access to all of the data we have. A lot of the data is, for business and commercial and contractual reasons, confidential, and they couldn't have access to all of that information.").

[14] 31 U.S.C. § 3729

[15] Southern District of New York: Former CEO Of Kubient, Inc. Sentenced To Prison In Connection With Accounting Fraud Scheme | United States Department of Justice, (Mar. 20, 2025), https://www.justice.gov/usao-sdny/pr/former-ceo-kubient-inc-sentenced-prison-connection-accounting-fraud-scheme (last visited Mar 22, 2025).

[16] *Id.*; Kubient Approved For Tag Registry By Trustworthy Accountability Group, PRESS RELEASE, https://www.prweb.com/releases/kubient_approved_for_tag_registry_by_trustworthy_accountability_group/prweb14869508.htm (last visited Mar 22, 2025).

[17] 31 U.S.C. § 3729

ad verification companies are knowingly misrepresenting their capabilities and continuing to charge the federal government for services they do not provide, this may constitute fraudulent conduct that warrants investigation under the FCA.

I also urge you to consider whether the misleading marketing claims made by ad verification firms fall under unfair or deceptive practices prohibited by the Federal Trade Commission Act (15 U.S.C. § 45(a)(1)), which the Justice Department may enforce in cases of criminal conduct.

I request that the Department of Justice investigate the following:

1. Whether ad verification companies such as IAS, DV, and HUMAN have knowingly misrepresented their capabilities to federal government clients or government contractors, particularly regarding their ability to detect and filter bot traffic in real-time.

2. Whether the ad verification firms involved in these failures violated the False Claims Act by charging the government – or government contractors – for services they did not deliver.

The harm to American citizens and the broader implications for market competition are significant.

This investigation is vital to prevent further waste of the advertising dollars of American businesses, 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; and urge you to take swift action to investigate these matters thoroughly.

Thank you for your attention to this critical issue. I look forward to your response.

Sincerely,

Mark R. Warner
United States Senator