Written Testimony of Mike Zaneis
President and CEO, Trustworthy Accountability Group

U.S. House of Representatives, Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

Hearing Entitled "Understanding the Digital Advertising Ecosystem"

June 14, 2018

Chairman Latta, Ranking Member Schakowsky, and distinguished Members of the Subcommittee, it is an honor to appear before you today at this important hearing to better understand the digital advertising ecosystem. In the past, I have been fortunate to testify twice before this Subcommittee on issues impacting our industry; as well as briefing the Subcommittee's Privacy Working Group several years ago. These are vital issues impacting the core of America's digital and data-driven economy.

Today, I come before you wearing a slightly different hat. As the President and CEO of the Trustworthy Accountability Group, or "TAG", I run an industry organization focused on fighting criminal activity in the digital advertising supply chain. In 2016, research showed that such criminal activity – primarily in the form of malware distribution, ad-supported piracy, and advertising fraud – had cost the U.S. economy at least $8.2 billion.[1] However, since that time, the digital advertising industry has joined hands and fought back hard, developing and supporting strong self-regulatory standards that have proven effective in significantly decreasing this negative economic impact.

[1] Ernst & Young LLP. (November 2015). What is an Untrustworthy Supply Chain Costing the US Digital Advertising Industry: IAB US Benchmarking Study. Retrieved from https://www.iab.com/wpcontent/uploads/2015/11/IAB_EY_Report.pdf.

I. Digital Advertising is the Engine that Powers the Internet Economy

Digital advertising is the predominant means of supporting both large and small digital businesses. This has always been the case, as a dispersed advertising supply chain democratized the digital economy by allowing anyone with a website to imbed ads and begin receiving revenue within a matter of weeks. This trend continues as consumers and time spent with media shifts towards mobile devices and high-quality video content.

A recent study by the Interactive Advertising Bureau ("IAB") found that the ad-supported internet ecosystem generated $1.12 trillion for the U.S. economy and was responsible for 10.4 million U.S. jobs in 2016, accounting for 7.3 percent of the country's total non-farm employment. The industry doubled both the number of digital advertising jobs and its economic contribution from 2012 to 2016, and increased its employment by 19.6 percent annually during that same period, while the U.S. total non-farm employment grew by just 1.8 percent in that period.

The ad-supported internet ecosystem accounts for 6 percent of the U.S. gross domestic product ("GDP"), representing a 20 percent compound annual growth rate from 2012 to 2016 – five times the average American GDP growth during the same period. These important economic and employment impacts are not restricted to conventional centers of internet industry concentration. Instead, 86 percent of the ad-supported internet economy's direct employment and value currently lie outside the San Francisco Bay Area, New York's Manhattan, Virginia's Arlington County, Boston's Route 128, and the Seattle/Tacoma area. Today, every U.S. Congressional district boasts jobs created by the ad-supported internet, with some of the biggest numbers of jobs in such states as North Carolina, Texas, and Utah.[2]

[2] Prof. John Deighton, the Baker Foundation Professor and the Harold M. Brierley Professor of Business Administration, Emeritus, at the Harvard Business School. (March 2017). The Economic Value of the Advertising-

II. With Prosperity Comes Threats and Challenges

The tremendous economic and employment growth seen in the digital advertising industry has made it one of the most important industries in the U.S. – and one of the most targeted by criminal enterprises. Fraudulent impressions, infringed content, and malvertising cost the U.S. digital marketing, advertising, and media industry $8.2 billion annually. More than half of these losses derive from "non-human traffic" – fake advertising impressions that are neither generated by real consumers nor received by actual marketers. Eliminating these fraudulent impressions would save advertisers more than $4 billion annually.[3] The aforementioned IAB study identified three primary supply chain costs:

- Invalid Traffic – As described above, ad fraud accounts for the largest portion of costs, at a total of $4.6 billion. Seventy-two percent of the loss associated with the web's fraudulent traffic happens on desktops and 28 percent on mobile.
- Infringed Content – At $2.4 billion, infringed content – stolen video programming, music, and other editorial content that is illegally distributed on the web – represents the most significant share of lost revenue opportunity costs. Two billion dollars of that total is based on an estimate of approximately 21 million U.S. consumers' willingness to spend $8 per month on what is currently classified as infringed content. The additional $456 million represents the loss of potential advertising dollars. The findings show that unless the industry takes significant steps, there is a likelihood that the number of people consuming stolen content on digital platforms will increase.

Supported Internet Ecosystem. Retrieved from https://www.iab.com/news/ad-supported-internet-brings-1-trillion-u-s-economy-doubling-contribution-since-2012-according-iab-study/.

[3] Ernst & Young LLP. (November 2015). What is an Untrustworthy Supply Chain Costing the US Digital Advertising Industry: IAB US Benchmarking Study. Retrieved from https://www.iab.com/wpcontent/uploads/2015/11/IAB_EY_Report.pdf.

- Malvertising-Related Activities – Combating malware that can be distributed within digital advertising creative, often referred to as "Malvertising", comes in at $1.1 billion, with $781 million of those losses being generated from ad blocking instigated due to security and malware concerns. Costs associated with investigating, remediating, and documenting direct incidents of malicious advertising total $204 million. The consumer costs inflicted by malvertising are likely to be even higher than industry costs.

Each of these seemingly unrelated crimes actually represent a single link in an interconnected chain of criminal activity. Rather than investing millions of dollars in creating quality, original content, criminal networks prefer to steal digital content. Once misappropriated, this content – ranging from simple blog posts or social media photos to platinum grossing music and box office movie hits – can be placed on domains that are cheaply and easily available. Even the best content requires an audience, so criminals then distribute malware that is capable of hijacking consumers' computers and devices. One study shows that internet users are twenty-eight times more likely to get malware from content theft sites.[4] Once under their control, these underground networks can stich thousands of devices together into botnets that are capable of browsing the web or utilizing mobile apps without the consumer being aware of the infection. Armed with this web browsing capacity, criminals can generate what appear to be real human visits to their own websites. Now that the sites have seemingly legitimate content and a large audience, they can attract advertising revenue from legitimate players in the ecosystem, resulting

[4] Digital Citizens Alliance study conducted by RiskIQ. (December 2015). Digital Bait: Internet Users At High Risk Of Malware From Content Theft. Retrieved from https://www.digitalcitizensalliance.org/news/press-releases-2015/digital-bait-internet-users-at-high-risk-of-malware-from-content-theft-70-million-underground-market/.

in advertising fraud. This is the predominant way criminals are able to cause massive harm to consumers and businesses.

III. TAG Represents Effective Industry Self-Regulation to Combat Criminal Activity

Founded in January 2015, TAG is an industry-led 501(c)(6) not-for-profit organization. It is the leading member-based global certification program fighting criminal activity and increasing trust in the digital advertising industry. TAG's mission is to eliminate fraudulent traffic, combat malware, prevent internet piracy, and promote greater transparency in the digital advertising supply chain. TAG advances those initiatives by bringing member companies from across the digital advertising supply chain together in a variety of working groups to set the highest standards for its certification programs in these four areas of our mission. The working groups develop and maintain suites of compliance tools to aid companies in complying with the certification program guidelines. Companies that are shown to abide by the standard for a TAG program can achieve the certification seal for that program and use the seal to publicly communicate their commitment to combatting criminal activity in the digital advertising supply chain.

To date, more than 100 companies have achieved at least one of the certification seals associated with the following four certification programs:

TAG's Certified Against Fraud Program

The mission of the TAG Certified Against Fraud Program is to combat fraudulent, invalid traffic in the digital advertising supply chain. The program provides companies with Certified Against Fraud Guidelines, as well as a suite of anti-fraud tools to aid in compliance:

- The Payment ID System creates a chain of custody for digital advertising transactions, helping companies to ensure that payments made in the digital ad ecosystem are going to legitimate partners.
- The Data Center IP List is a common list of IP addresses with invalid traffic coming from data centers where human traffic is not expected to originate. TAG publishes this list on a monthly basis to assist companies in meeting the requirement in the Certified Against Fraud Guidelines that companies employ data center IP threat filtering across all of the monetizable transactions that they handle.
- The Publisher Sourcing Disclosure Requirements (PSDR) foster trust in the marketplace by disclosing the amount of sourced traffic for a given publisher. This policy tool outlines the requirements for publishers to disclose the volume of traffic acquired through paid sources.
- The Ads.txt Specification creates greater transparency in the inventory supply chain by creating a public record of Authorized Digital Sellers, giving publishers greater control over their inventory in the market, and making it harder for bad actors to profit from selling counterfeit inventory across the ecosystem.

TAG's Certified Against Malware Program

The mission of the TAG Certified Against Malware Program is to eliminate the distribution of malware throughout the digital advertising supply chain. Malware delivered through the advertising ecosystem degrades overall trust in the system by generating a poor consumer experience. Additionally, malware infected machines attack the advertising ecosystem in order to generate money for fraudsters. Because each participant in the ecosystem has

visibility into only their subset of the problem, preventing the delivery of malware overall is challenging, resulting in continued attacks on consumers through the various uncoordinated parts of the system.

The Certified Against Malware Program provides companies with a roadmap by which to combat malware in the digital advertising supply chain effectively, improving consumer experience and stopping botnet attacks that fund fraudsters. By coordinating cross-industry information sharing, TAG enables companies to partner in thwarting attacks that they would not be able to stop alone.

TAG's Certified Against Piracy Program

The mission of the TAG Certified Against Piracy Program is to help advertisers and agencies avoid damage to their brands from ad placement on websites and other media properties that facilitate the distribution of pirated content and counterfeit products. This voluntary initiative helps marketers identify sites that present an unacceptable risk of misappropriating copyrighted content and sell counterfeit goods, and it will help them remove those sites from their advertising distribution chain.

The Certified Against Piracy Program provides companies with the Certified Against Piracy Guidelines, as well as a suite of anti-piracy tools**,** to aid in compliance with the program requirements.

- In order to achieve the Certified Against Piracy Seal, Direct Buyers must operationalize and comply with the TAG Anti-Piracy Pledge**.**

- In order to achieve the Certified Against Piracy Seal, Self-Attested DAAPs and Validated DAAPs must meet all of the elements in one or more of the five Core Criteria for Effective Digital Advertising Assurance.

- The TAG Pirate Mobile App List is a common list of mobile apps that were removed from App Stores for infringing on protected intellectual property rights. TAG publishes this list on a quarterly basis to assist companies in meeting the requirement in the Certified Against Piracy Guidelines that companies employ pirate mobile app filtering for all advertising displayed in a mobile app environment.

TAG's Inventory Guidelines Program

The TAG Inventory Quality Guidelines (IQG) Program promotes the flow of advertising budgets into digital advertising with industry regulation that offers a framework for brand safety. The mission of the IQG Program is to reduce friction and foster an environment of trust in the marketplace by providing clear, common language that describes characteristics of advertising inventory and transactions across the advertising value chain. The goals of the IQG Program are to: (i) support the information needs of advertising buyers; (ii) define a common framework of disclosures that sellers can use across the industry; (iii) offer clear language that enables buyers to make informed decisions; and (iv) review compliance and facilitate the resolution of disputes and complaints.

Proven Results

Industry self-regulation is an effective means of addressing the challenges facing the digital advertising ecosystem. During the past year, independent research has measured the effectiveness of TAG's anti-fraud and anti-piracy efforts and found them to be highly successful at combatting criminal activity in the digital advertising supply chain.

In December 2017, The 614 Group released a study commissioned by TAG showing that the use of TAG Certified distribution channels for digital advertising reduced the level of fraud by more than 83% in comparison to broader industry averages. The study was conducted by examining more than 6.5 billion display and video impressions in campaigns run through TAG Certified Channels by three major media agencies for their clients.[5] Among the study's findings:

- Analyses by verification technology providers found the levels of fraud, often referred to as "Invalid Traffic" (IVT), in digital advertising average 8.83 percent for display inventory in North America (and rise to 12.03 percent when video inventory is included).
- The 614 Group examined comparable rates of fraud for campaigns run through "TAG Certified Channels", in which multiple entities involved in the transaction – such as the media agency, buy-side platform, sell-side platform and/or publisher – had achieved the TAG Certified Against Fraud Seal.
- In such TAG Certified Channels, the IVT rate fell to 1.48 percent, a reduction of 83 percent over industry averages.

[5] The 614 Group. (December 2017). TAG Fraud Benchmark Study.
Retrieved from https://www.tagtoday.net/fraud_benchmark_research_us.

Similarly, a 2017 Ernst & Young study commission by TAG found that anti-piracy steps taken by the digital advertising industry – including the TAG Certified Against Piracy Program – have reduced ad revenue for pirate sites by between 48 and 61 percent, which represents notable progress against the $2.4 billion problem of infringing content. Among the study's findings:

- Digital ad revenue linked to infringing content was estimated at $111 million last year, the majority of which (83 percent) came from non-premium advertisers.
- If the industry had not taken aggressive steps to reduce piracy, those pirate site operators would have potentially earned an additional $102-$177 million in advertising revenue, depending on the breakdown of premium and non-premium advertisers.
- Ongoing industry efforts against piracy have therefore reduced the advertising revenue of pirate sites by 48 to 61 percent.[6]

This research proves that when the industry works together, it is possible to solve even the most nefarious threats in the digital marketplace.

IV. Collaboration is Prevalent Across the Digital Advertising Ecosystem

A myth promulgated by industry naysayers suggests that, because criminal activity can often provide higher ad revenue to certain parts of the digital supply chain, the industry has a perverse incentive to not police itself. History has shown just the opposite to be true.

[6] Ernst & Young LLP. (September 2017). Measuring Digital Advertising Revenue to Infringing Sites: TAG US Benchmarking Study. Retrieved from https://www.tagtoday.net/piracy/measuringdigitaladrevenuetoinfringingsites.

When research uncovered the full extent of criminal activity that had infiltrated the legitimate digital advertising supply chain, the entire industry jumped into action to achieve a healthier, cleaner ecosystem through the creation and support of TAG. Advertising networks and exchanges – the third parties that could potentially benefit from fraudulently inflated traffic rates – were among the earliest supporters of TAG. The recognition that legitimate companies benefit long-term from a cleaner, healthier ecosystem has driven more than 680 companies to apply for TAG membership. Furthermore, the TAG membership includes companies from every sector of the digital supply chain – from marketers and agencies, to ad tech firms and web publishers – and extends across 27 countries and 6 continents.

TAG's efforts also benefit from collaboration with Federal law enforcement. We have formed information-sharing partnerships with the Department of Homeland Security's Intellectual Property Rights Center and the Federal Bureau of Investigation's Cybercrimes and Financial Crimes Divisions. TAG also serves as the first Information Sharing and Analysis Organization ("ISAO") for the digital advertising industry to register with the ISAO Standards Organization, a non-governmental organization established by Congress to strengthen the nation's cybersecurity defense through information sharing. As the only ISAO for the digital ad industry, TAG serves as the lead information sharing organization around threats, incidents, and best practices, particularly those related to ad-related malware, ad-supported piracy, ad fraud and associated threats.

This culture of collaboration has always existed within our industry. In 2006, the Digital Advertising Alliance ("DAA") was established to promote more responsible privacy practices across the industry for relevant digital advertising, providing consumers with enhanced transparency and control through multifaceted principles that apply to multi-site data and cross-

app data gathered in either desktop, mobile web, or mobile app environments. The DAA is an independent non-profit organization led by leading advertising and marketing trade associations.

More recently, the leading international trade associations and companies involved in online media formed the Coalition for Better Ads ("CBA") to improve consumers' experience with online advertising. CBA leverages consumer insights and cross-industry expertise to develop and implement new global standards for online advertising that address consumer expectations.

V. Conclusion

TAG appreciates the Subcommittee's interest in helping Congress and the public better understand the digital advertising ecosystem. The digital advertising industry is one of the key drivers of the U.S. economy, empowering companies large and small. Although serious challenges face this vital industry, companies have rallied together to create effective self-regulatory solutions. I look forward to answering any questions that you may have.