



# CORE CRITERIA FOR EFFECTIVE DIGITAL ADVERTISING ASSURANCE

V1.0

FEBRUARY 2015

A Project of the Trustworthy  
Accountability Group

[www.tagtoday.net](http://www.tagtoday.net)

# content

## PREAMBLE

## I. SCOPE AND APPLICATION

## II. LEGAL LIABILITY AND DMCA SAFE HARBOR

## III. DEFINITIONS

1. Ad Risk Entities
2. Digital Advertising Assurance Providers

## IV. CRITERIA FOR EFFECTIVE DIGITAL ADVERTISING ASSURANCE

1. Identify Ad Risk Entities
2. Prevent Advertisements on Undesired Ad Risk Entities
3. Detect, Prevent, or Disrupt Fraudulent or Deceptive Transactions
4. Monitor and Assess Advertisement Placement Compliance
5. Eliminate Payments to Undesired Ad Risk Entities
6. Revision or Amendment to Core Criteria

## V. IMPLEMENTATION

1. Internal Procedures
2. Dispute Resolution

## VI. VALIDATION AND SELF-ATTESTATION PROCESSES

1. Validator
2. Ongoing Validation and Monitoring
3. Self-Attestation

## VII. EDUCATION

- Webpage

## PREAMBLE

Digital advertising has brought advertisers unprecedented opportunities to reach potential customers in a targeted fashion and has a virtually boundless potential for growth. Such advertising occurs within a highly-complex online advertising ecosystem involving many different actors and stakeholders, including advertisers, advertising agencies, ad networks, ad exchanges, ad trading platforms, and the web sites and other media properties on which the advertisements are placed. Ad networks and ad exchanges use advanced computer algorithms to place advertisements on different sites. The placement is often fully automated, pairing an advertisement with available inventory. This automated placement efficiently places an advertisement in front of the appropriate target audience.

While this new model of digital advertising provides great benefits to businesses and consumers alike, new challenges have emerged. One such challenge occurs when advertising is inadvertently placed on sites or other media properties associated with the unauthorized dissemination of materials protected by the copyright laws or illegal dissemination of counterfeit goods (here called “Ad Risk Entities” or AREs). Such advertising can harm consumers, advertisers, content creators, and distributors. Harm may be caused to advertisers by associating their brands with illegal activity. In addition, consumers may mistakenly believe that the sites’ offerings are authorized by well-known brands. Such misplaced advertising also harms content creators and legitimate content distributors by providing economic resources that fuel these illegal enterprises and putting enormous profits into their coffers.

The major advertising trade associations have recognized this issue and have taken a leadership role in addressing it. In 2012, the Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4A’s), supported by the Interactive Advertising Bureau (IAB), adopted a Statement of Best Practices to Address Online Piracy and Counterfeiting, providing language for marketers to use in their media placement contracts and insertion orders to prevent advertisements from appearing on sites dedicated to infringement of intellectual property of others.<sup>1</sup> In July 2013, leading ad networks also announced a set of Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting.<sup>2</sup> Also in 2013, the IAB updated its Network and Exchange Quality Assurance Guidelines to include a ban on selling ad inventory on “copyright infringement” and “warez” sites.<sup>3</sup> In June 2014, the IAB also announced its Trustworthy Digital Supply Chain Initiative, identifying fighting Internet piracy as one of its five objectives, along with eliminating fraudulent traffic, combatting malware, and promoting brand safety through increased transparency, and creating accountability.<sup>4</sup>

---

<sup>1</sup> Association of National Advertisers, “ANA, 4A’s Release Statement of Best Practices Addressing Online Piracy and Counterfeiting,” available at <http://www.ana.net/content/show/id/23408>.

<sup>2</sup> “Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting,” available at <http://www.2013ippractices.com/bestpracticesguidelinesforadnetworkstoaddresspiracyandcounterfeiting.html>

<sup>3</sup> Interactive Advertising Bureau, “Quality Assurance Guideline 2.0,” July 25, 2013, available at <http://www.iab.net/media/file/QualityAssuranceGuidelines7252013.pdf>.

<sup>4</sup> Interactive Advertising Bureau, “Winning the War on Crime in the Supply Chain: A Trust-Building Initiative, to Get Behind, Now,” June 9, 2014, available at <http://www.iab.net/iablog/2014/06/Trustworthy-Digital-Supply-Chain.html>.

Until recently, advertisers who wished to keep their advertisements off all or a subset of AREs had limited options available to effectuate their intentions. In the last few years, however, a number of entities—here called “Digital Advertising Assurance Providers” or DAAPs—have emerged that, in a variety of ways, can assist advertisers, ad agencies, ad networks, trading platforms, and/or other actors in the ad ecosystem avoid the undesired placement of ads on AREs.

In the interest of assisting advertisers in this important endeavor, the advertising community and others in the online media and advertising ecosystem, have come together to create a voluntary program designed to validate that these DAAP entities, and others that will enter the market, effectively provide the services they offer. This document establishes a framework and sets out the criteria and the process for such validation, and for designation of those entities that have successfully completed that process. With this framework, all who have a stake in the online advertising ecosystem can gain confidence that advertisements placed on AREs against the wishes of the advertiser will be greatly diminished, to the benefit of brands, consumers, and creators alike.

## I. SCOPE AND APPLICATION

The framework established by this document is intended to help enable advertisers and their agencies identify designated Digital Advertising Assurance Providers (DAAPs) that meet the core criteria presented in this document. Validation (or self-attestation) as a DAAP and use of DAAPs’ services and tools are entirely voluntary and are not prerequisites to participating in the digital advertising ecosystem. Rather, they are intended to provide a means for advertisers and other industry actors to more efficiently navigate the complex online advertising ecosystem and to enhance both the value and integrity of online advertising.

The core criteria set forth in this document are designed to be technology-neutral and are not intended as an endorsement of any specific technology.

## II. LEGAL LIABILITY AND DMCA SAFE HARBOR

1. Those participating in this framework shall comply with federal and state antitrust laws.
2. Nothing in this document is intended to conflict with the Digital Millennium Copyright Act’s (DMCA) safe harbor provisions found in 17 U.S.C. § 512. These core criteria should not, and cannot, be used in any way as the basis for any legal liability or the loss of any applicable immunity or “safe harbor” from such liability. Knowledge gained in the course of implementing this voluntary commitment should not be used as the basis for any legal liability or loss of any applicable “safe harbor” from such liability.

### III. DEFINITIONS

1. **Ad Risk Entities.** Ad Risk Entities (AREs) are websites or other media properties that have a discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods.

*Commentary:*

*This framework does not seek to bar advertising on every website or other media property that has some potential for a discernible risk of being associated with the unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods. Advertisers ultimately will determine the degree of risk they will assume in their marketing efforts. This framework is designed to assist them in identifying, evaluating, and addressing this particular category of risk should they desire to do so.*

*AREs will normally have a current discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods. However, AREs may also include websites or other media properties, in whole or in part, that have historically been identified as having a discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods, and whose past behavior warrants continued concern, subject to the dispute resolution process discussed in (V)(2).*

*“Other media properties” may include emerging advertising platforms, including mobile apps.*

2. **Digital Advertising Assurance Providers.** Digital Advertising Assurance Providers (DAAPs) are companies that offer, subject to the validation or attestation processes outlined below, technologies, methodologies, or services that, consistent with the advertiser’s instructions, effectively: (1) assess which entities are identified as AREs; and/or (2) assist entities in the advertising ecosystem to prevent undesired placement of advertisements on such AREs; and/or (3) identify and eliminate payment for online advertisements on such AREs (collectively “Offerings”).

*Commentary:*

*Those entities that have successfully completed the validation process in (VI)(2) by a validator authorized under (VI)(1) may be designated under this framework as a “Validated DAAP.”*

*Those entities that have successfully completed the self-attestation process in (VI)(3) may be designated under this framework as a “Self-Attested DAAP.” If a Self-Attested DAAP subsequently completes the validation process in (VI)(2) either at its own election or pursuant to the process set forth in (VI)(3), such entity may elect to be designated as a “Validated DAAP” going forward provided it complies with the annual validation process set forth in (VI)(2).*

*A DAAP may assess the risk associated with AREs, such as through risk scoring, to assist the advertisers and/or their agencies in determining an advertising placement strategy in accordance with the advertiser’s risk tolerance. Advertisers determine the degree of risk they will assume.*

Where such Offerings seek to prevent undesired placements of advertisements, the Offerings represent a DAAP's best effort consistent with the advertiser's instructions.

Whether a website or other media property is deemed an ARE is determined in accordance with the core criteria in (IV)(1).

Examples of "entities in the advertising ecosystem" include, but are not limited to, advertisers, ad agencies, ad networks, ad exchanges, trading desks, demand-side and sell-side platforms, yield optimizers, data providers, ad servers, and other ad buying, selling, or serving platforms. These various entities in the ecosystem can individually and collectively prevent the delivery of advertisements to AREs. As a result, each has a respective role to play in combating undesired advertisement placement.

## IV. CRITERIA FOR EFFECTIVE DIGITAL ADVERTISING ASSURANCE

A DAAP elects to be designated as to one or more of the criteria listed below. To meet a particular criterion, a DAAP should competently and effectively meet each element listed under that criterion.

### 1. Criterion #1: Identify AREs.

#### Elements:

- a. A DAAP should assess whether entities are AREs;
- b. A DAAP should provide tools to help advertisers and/or their agencies decide the extent to which they wish to limit or restrict the display of their advertisements on entities deemed to be AREs in (IV)(1)(a); and
- c. A DAAP should have an objective review and evaluation process for claims from entities of erroneous designation or scoring or determination of those entities as AREs in (IV)(1)(a).

*Commentary:*

*"Objective" means evaluating each entity under the same criteria.*

### 2. Criterion #2: Prevent Advertisements on Undesired AREs.

#### Elements:

- a. A DAAP should restrict or enable the restriction of the display of advertisements on undesired AREs in accordance with the direction of an advertiser and/or its agency as set forth in (IV)(1)(b) ("Undesired AREs"); and
- b. A DAAP should provide or enable the provision of real-time solutions as a means to effectively prevent advertisements on Undesired AREs.

**3. Criterion #3: Detect, Prevent, or Disrupt Fraudulent or Deceptive Transactions.**

**Elements:**

- a. A DAAP should have protocols and capabilities to detect, prevent, or disrupt advertising placements on Undesired AREs that are transacted fraudulently or deceptively (e.g., through the use of intermediary sites or other means to disguise the ARE's identity or purpose);
- b. In the event that a DAAP identifies the use of intermediary sites or other means as set forth in (IV)(5)(a), a DAAP should have protocols and capabilities to prevent further advertisement exposure through such means; and
- c. A DAAP should have an objective review and evaluation process for claims from entities of erroneous determination of fraudulent or deceptive transactions in (IV)(5)(a).

**4. Criterion #4: Monitor and Assess for Advertisement Placement Compliance.**

**Element:**

A DAAP should detect and report on advertisements on AREs that may not be in compliance with advertiser/agency instructions, thus enabling advertisers and agencies to implement remedial action.

*Commentary:*

*Such a report should enable the advertiser or agency to provide adjustments to advertisement placements based on the reporting results. Additionally, the report should enable the advertiser or agency to put advertising intermediaries on notice of improper advertising placements. In the event payment has been made to AREs, the report from the DAAP should enable the advertiser or agency to reverse or reclaim such payment outlined in (IV)(4).*

**5. Criterion #5: Eliminate Payments to Undesired AREs.**

**Elements:**

- a. A DAAP should have technology and protocols in place that prevent or enable the prevention of payments resulting from advertisements displayed on Undesired AREs; and
- b. In the event payment has been made to Undesired AREs, a DAAP should have technology and protocols in place that enable the reversal or reclamation of such payment.

*Commentary:*

*AREs often employ intermediary sites under their or others' ownership or control to fraudulently disguise their activities in order to gain access to the online advertising ecosystem marketplace. Advertisers determine the extent to which they will tolerate such behavior.*

*The validators in (VI) determine the acceptable amount of time within which prevention of further advertisement exposure through such intermediary sites should occur.*

6. **Revision or Amendment of Core Criteria.** The Trustworthy Accountability Group (TAG) will initially oversee this framework. These Core Criteria for Effective Digital Advertising Assurance may be revised and amended through TAG.

## V. IMPLEMENTATION

1. **Internal Procedures.** A DAAP should maintain documented and internal procedures designed to implement the enumerated criteria in (IV) for which the DAAP has elected to be designated.
2. **Dispute Resolution.** A DAAP electing to be designated as to the criterion in (IV)(1) and/or the criterion in (IV)(3) should have a dispute resolution process as set forth in (IV)(1)(c) and (IV)(3)(c) respectively.

## VI. VALIDATION AND SELF-ATTESTATION PROCESSES

1. **Validator**
  - a. **Establishment and Selection of Authorized Validators.** In order to balance the interests of affording DAAPs some degree of choice while maintaining reasonably consistent quality standards for the validation process, there shall be no more than three independent third-party entities authorized to validate whether an entity meets the criteria required for designation as a Validated DAAP as set forth in (IV).
  - b. **Criteria for Eligibility for Selection.** An entity must meet the following criteria to be eligible for selection as an authorized third-party validator under the framework:
    - i. Understanding of the online advertising ecosystem.
    - ii. Proven capability to conduct technical, business practice, and protocol evaluations.
    - iii. Capability to determine whether entities applying to be designated as a DAAP meet each element listed under the enumerated criteria in (IV) for which they are seeking designation.
2. **Ongoing Validation and Monitoring.** A Validated DAAP shall be evaluated at least annually to validate the effectiveness of the Validated DAAP.

*Commentary:*

*An entity electing to be validated as to one or more of the criteria in (IV) shall submit to the validation and monitoring processes described in (VI)(2).*

*TAG shall designate an entity as a “Validated DAAP” (meeting the designated criteria) under the framework upon the successful completion of the validation process by a validator in (VI)(1).*



3. **Self-Attestation.** An entity may choose to self-attest to one or more of the criteria outlined in (IV) and be designated as a Self-Attested DAAP for Offerings covered under this framework that it provides to itself (“In-House Offerings”). Entities that choose to self-attest shall provide the attestation to TAG annually. Such entities shall be subject to an evaluation by a validator in (VI)(1) in the event that credible information is provided to TAG that suggests that the entity is not meeting these core criteria.

*Commentary:*

*The purpose of self-attestation is designed for entities who provide DAAP In-House Offerings.*

*To the extent that an entity seeks to provide Offerings to a business other than itself and wishes to attest to the criteria outlined in (IV) under this framework, the entity shall not utilize the self-attestation process in (VI)(3) and instead shall submit to the validation and monitoring processes described in (VI)(2).*

*An entity choosing to self-attest to one or more of the criteria in (IV) and which seeks designation as a Self-Attested DAAP for In-House Offerings covered under this framework, shall self-attest with TAG and specify the criterion or criteria in (IV) to which the entity chooses to self-attest.*

*(A) TAG shall designate that entity as a “Self-Attested DAAP” for In-House Offerings (meeting the designated criteria) under the framework.*

*(B) TAG may withhold or withdraw designation as a “Self-Attested DAAP” in the event that credible information is presented to TAG that suggests that the entity is not meeting the core criteria.*

## VII. EDUCATION

**Webpage.** A centralized informational webpage should highlight key points, issues, principles, and developments regarding AREs.



[www.tagtoday.net](http://www.tagtoday.net)