



# TAG Certified Against Fraud Guidelines

Version 2.0  
Release January 2018

## About the TAG 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.

In order to guide companies in fighting fraud effectively, the TAG Anti-Fraud Working Group developed and maintains the Certified Against Fraud Guidelines, as well as a suite of anti-fraud tools to aid in compliance with those guidelines.



Companies that are shown to abide by the Certified Against Fraud Guidelines can achieve the Certified Against Fraud Seal and use the seal to publicly communicate their commitment to combatting invalid traffic in the digital advertising supply chain.

## About the Trustworthy Accountability Group

The Trustworthy Accountability Group (TAG) is the leading global certification program fighting criminal activity and increasing trust in the digital advertising industry. Created by the industry's top trade organizations, TAG's mission is to:

- Eliminate fraudulent traffic,
- Combat malware,
- Prevent Internet piracy, and
- Promote greater transparency in digital advertising.

TAG advances those initiatives by bringing companies across the digital advertising supply chain together to set the highest standards.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

To learn more about the Trustworthy Accountability Group, please visit [www.tagtoday.net](http://www.tagtoday.net).

# Table of Contents

- 1. **Executive Summary** ..... 5
- 2. **Certification Process** ..... 6
  - 2.1. Application ..... 6
    - 2.1.a. Participation Fee ..... 6
  - 2.2. Qualification ..... 6
  - 2.3. Geographic Applicability of Certification ..... 6
  - 2.4 Methods of Certification ..... 7
    - 2.4.a. Certification Through Self-Attestation ..... 7
    - 2.4.b. Certification Through Independent Validation ..... 8
  - 2.5 Publication of Certification Status ..... 8
    - 2.5.a. Certified Against Fraud Seal ..... 8
  - 2.6. Continued Compliance ..... 9
    - 2.6.a. TAG Compliance Officer ..... 9
    - 2.6.b. Compliance Team ..... 9
    - 2.6.c. Training ..... 10
    - 2.6.d. Quarterly Internal Reviews ..... 10
    - 2.6.e. Recertification ..... 10
- 3. **Covered Parties** ..... 11
  - 3.1. Direct Buyer ..... 11
  - 3.2. Direct Seller ..... 11
  - 3.3. Intermediary ..... 11
  - 3.4. Anti-Fraud & Measurement Services ..... 12
- 4. **Certification Requirements** ..... 13
  - 4.1. Requirements Table ..... 13
  - 4.2. Complete TAG Registration and be a TAG Member in Good Standing ..... 14
  - 4.3. Have a Designated TAG Compliance Officer ..... 14
  - 4.4. Attend a Certified Against Fraud Training Annually ..... 14
  - 4.5. Comply with General Invalid Traffic (GIVT) Detection and Filtration Requirements of Media Ratings Council’s (MRC) Invalid Traffic (IVT) Guidelines ..... 14
    - 4.5.a. Exception Process ..... 15

4.6. Employ Domain Threat Filtering .....	15
4.6.a. Exception for Mobile In-App Inventory .....	16
4.7. Employ Data Center IP Threat Filtering.....	16
4.7.a. Use of TAG Data Center IP List.....	16
4.8. Implement Publisher Sourcing Disclosures .....	17
4.8.a. Exception Process .....	17
4.9. Implement the Payment ID System .....	17
4.10. Implement Ads.txt .....	17
<b>5. Allegations of Non-Compliance &amp; Appeal.....</b>	<b>18</b>

# 1. Executive Summary

Advertisers expect their content will be viewed by legitimate consumers with the potential to buy their products and services. However, criminal organizations have attacked the digital ad ecosystem with malware and other methods that generate invalid traffic and defraud legitimate participants in the supply chain. As a result, advertisers may end up paying a material portion of their campaign dollars to criminals who generate ad impressions that are never seen by legitimate consumers.

The 2017 ANA / White Ops Bot Fraud study estimated that advertisers lost \$6.5 billion that year globally to bot-generated, invalid traffic (IVT). Bot traffic impacted a wide variety of websites including those of well-known and premium publishers. Most of the bots visited real websites run by real companies with real human visitors. Those bots continue to impact 9% of desktop display spending and 22% of desktop video spending.

TAG launched its Certified Against Fraud Program in 2016 to combat invalid traffic in the digital advertising supply chain. The TAG Anti-Fraud Working Group developed and maintains the Certified Against Fraud Guidelines, as well as a suite of anti-fraud tools to aid in compliance with those guidelines.

By encouraging legitimate participants in the digital advertising supply chain to meet these standards, the TAG Certified Against Fraud Program has been shown to be an effective tool in reducing fraudulent invalid traffic in the digital advertising supply chain. The 2017 TAG Fraud Benchmarking Study, conducted by The 614 Group, found that the use of TAG Certified distribution channels for digital advertising cut the IVT rate to 1.48 percent across more than 6.5 billion display and video impressions, reducing the level of fraud by more than 83% compared to the broader industry average.

## 2. Certification Process

The TAG Certified Against Fraud Program is voluntary and represents the ongoing process of defining and maintaining guidelines for effectively combating fraudulent invalid traffic in the digital advertising supply chain.

TAG certifies companies at the entity level, rather than certifying a specific product or business line within a legal entity. To achieve the TAG Certified Against Fraud Seal, companies must show that all of its material operations related to ad monetization services within a particular geographic market are in compliance with the relevant requirements of the Certified Against Fraud Guidelines.

### 2.1. Application

Before a company can apply for the Certified Against Fraud Seal, that company must first become a TAG member, completing the process of becoming “TAG Registered” and enrolling in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG directly or visiting [www.tagtoday.net](http://www.tagtoday.net).

Once a company has been approved as “TAG Registered” and enrolled in the Verified by TAG Program, the company’s designated TAG Compliance Officer may contact TAG directly to request enrollment in the Certified Against Fraud Program in order to begin the process for that company to achieve the Certified Against Fraud Seal. In order to participate in the Certified Against Fraud Program, a company’s TAG membership must include access to that program.

#### *2.1.a. Participation Fee*

There is an annual fee, which is encompassed in annual membership dues, for participation in the Certified Against Fraud Program.

### 2.2. Qualification

Any TAG member company in good standing that has been enrolled in the Verified by TAG Program and whose TAG membership includes participation in the Certified Against Fraud Program can participate in the Certified Against Fraud Program and apply for the Certified Against Fraud Seal.

Requirements to achieve the TAG Certified Against Fraud Seal differ according to a company’s role in the digital advertising supply chain. These roles and requirements are outlined in Sections 3 and 4 of this document.

### 2.3. Geographic Applicability of Certification

The Certified Against Fraud Seal can be achieved in any geographic market. However, upon achieving certification, a company is only permitted to use the Certified Against Fraud Seal in the specific geographic markets in which TAG has found the company’s operations to be in full compliance with the Certified Against Fraud Guidelines. Additionally, any use of the seal must identify the geographic markets to which it applies.

At minimum, TAG requires that a company bring its full operations in the US market into compliance in order to achieve the Certified Against Fraud Seal. Companies can also choose to certify operations in additional markets, either by country (e.g.: Brazil), by region (e.g.: South America), or globally.

If a company wants to certify its operations in geographic markets beyond the US, it must clearly state the markets – either by country, by region, or globally – in which it is applying for certification in its application for the Certified Against Fraud Seal.

If a company does not clarify the geographic areas in which it wants to be certified, TAG will assume the company is applying solely for certification of its operations in the US market and the company will be licensed to use the Certified Against Fraud Seal solely in that market.

## 2.4 Methods of Certification

Companies can apply to achieve the Certified Against Fraud Seal using one of two methods: self-attestation and independent validation. A company has the option to choose either method, except in cases noted in Section 5 of this document. The selected method is recorded and displayed on the TAG website.

Certification through self-attestation is obtained with a series of binding attestations from the company in which it attests to have achieved full compliance with the Certified Against Fraud Guidelines and that it will maintain compliance throughout the certification period.

Certification through independent validation is obtained by the company inviting an independent auditor to review and validate that the company has achieved full compliance with the Certified Against Fraud Guidelines, and the company attesting that it will maintain compliance throughout the certification period. A validating company may be any auditing company that includes a specialty in digital media audits.

The certification processes for self-attestation and independent validation are parallel except that in an independent validation, the independent auditor submits required attestation paperwork and reports to TAG, in addition to the paperwork submitted by the company itself.

Since the internal processes for both self-attestation and independent validation certification are the same, a company that has achieved the Certified Against Fraud Seal through a self-attestation can move to an independent validation certification at any time by providing the additional paperwork and reports required from the independent auditor.

### *2.4.a. Certification Through Self-Attestation*

Certification through self-attestation is obtained through a series of attestations from the company that it is complying the Certified Against Fraud Guidelines.

Entities that wish to achieve the TAG Certified Against Fraud Seal through self-attestation should submit to TAG a completed Certified Against Fraud Self-Attestation Checklist and supporting materials for each of the relevant certification requirements, as well as a signed TAG Compliance Officer Attestation and Business Executive Attestation. Following examination of the self-attestation application materials, TAG will notify the company as to whether they have

met the relevant requirements of the Certified Against Fraud Guidelines, or whether additional information is needed in order to confirm compliance.

#### ***2.4.b. Certification Through Independent Validation***

To achieve certification through independent validation, a company must invite an independent auditor to validate that the company is compliant with the Certified Against Fraud Guidelines. A validating company may be any auditing company that includes a specialty in digital media audits.

While independent validation is designed to provide limited assurance, ensuring that all Certified Against Fraud Guidelines are being met within the company's operations, technology and supporting documentation may take some time to examine. Examination time depends on several factors such as company operations maturity level, organization size and complexity and technology.

Independent validation will include examination of, but is not limited to, the following:

- Job description of the compliance officer.
- Training policy and procedures.
- Internal audit policies and procedures.
- Established policies and procedures related to internal control.
- Policies and procedures related to the requirements of the Certified Against Fraud Guidelines.
- Policies and procedures related to complaint handling/resolution to ensure compliance with the Certified Against Fraud Guidelines.
- Testing performed by the company as part of the internal quarterly review process.

To achieve independent validation, the validating company must submit the following to TAG:

- Compliance Officer and Executive Attestations
- Independent Validation Attestation
- Quarterly audit report

### **2.5 Publication of Certification Status**

With training and consistent monitoring procedures in practice, the company is certified when TAG determines the company to be in full compliance with the Certified Against Fraud Guidelines, based on the required documentation submitted. TAG notifies the company of its certification status, and that certification status is posted to the TAG Registry. Upon certification, TAG sends materials to the company's designated TAG Compliance Officer for use in promoting the company's Certified Against Fraud status.

#### ***2.5.a. Certified Against Fraud Seal***

Companies that are shown to meet the Certified Against Fraud Guidelines receive the Certified Against Fraud Seal and can use the seal to publicly communicate their commitment to combatting fraudulent, invalid traffic in the digital advertising supply chain.



## 2.6. Continued Compliance

Companies that are shown to meet the Certified Against Fraud Guidelines and achieve the Certified Against Fraud Seal must maintain compliance throughout the certification period.

### *2.6.a. TAG Compliance Officer*

Companies participating in the Certified Against Fraud program must designate a qualified TAG Compliance Officer. This is usually done in the process of the company's application for TAG Registration, prior to participation in the Certified Against Fraud Program.

The duties of a TAG Compliance Officer include:

- Serving as the primary point of contact between TAG and the company regarding all aspects of the company's TAG membership. This includes receipt of notice concerning any changes to TAG Certification program(s).
- Completing the required training modules for each TAG Certification program in which the company participates.
- Educating internal teams on the requirements of each TAG Certification program in which the company participates, and notifying those internal teams of any changes.
- Overseeing the company's processes related to compliance with the requirements of each TAG Certification program in which the company participates.
- Facilitating internal review of the company's compliance with the requirements of each TAG certification program in which the company participates, including independent auditor review where appropriate.
- Taking on additional responsibilities applicable to each of the TAG programs in which the company participates (as appropriate).

The minimum qualifications for a TAG Compliance Officer include:

- Reporting relationships whereby compliance assessments are not influenced or biased by operations personnel being tested for compliance.
- Adequate technical training and proficiency in testing and assessing compliance.
- Adequate knowledge of the subject matter covered in each of the TAG Certification programs in which the company participates (i.e., advertising technology, various functions within the digital advertising supply chain, etc.).
- Adequate independence within the company to avoid conflicts of interest with regard to assessing compliance with TAG program requirements.

A TAG Compliance Officer does not need to hold a particular title or job description within the organization, as long as that individual has independence from sales and marketing functions.

The role of the TAG Compliance Officer is further described in the TAG Compliance Officer Role Description on the TAG website.

### *2.6.b. Compliance Team*

While the only required requirement to support compliance with the Certified Against Fraud

Program is the designation of a TAG Compliance Officer, it is also recommended that a company have in place a Compliance Team to assist in meeting and maintaining compliance with the Certified Against Fraud Guidelines.

### *2.6.c. Training*

Certified Against Fraud training is required for the company's designated TAG Compliance Officer. The Compliance Officer is encouraged to attend the first training available after a company is enrolled in the Certified Against Fraud Program and must complete training within three months of the company having achieved the Certified Against Fraud Seal. Training must be renewed on an annual basis in order for a company to maintain its Certified Against Fraud Seal from year to year.

### *2.6.d. Quarterly Internal Reviews*

Quarterly internal reviews ensure that a company that has been awarded the Certified Against Fraud Seal maintains full compliance with the Certified Against Fraud Guidelines throughout the year.

The TAG Compliance Officer is responsible for overseeing quarterly internal reviews, which should insure that:

- The Certified Against Fraud Guidelines are consistently and completely followed.
- Control activities discussed during Certified Against Fraud training are formally documented.
- Potentially criminal activity is detected in a timely fashion.
- Appropriate corrective measures are taken in a timely fashion.

Internal reviews should also include a risk analysis of certain control functions to assess how much testing is needed to validate adherence. Also, actual testing of data, both quantitatively and qualitatively, should be used to validate that the existing control structure is designed correctly and operating effectively.

### *2.6.e. Recertification*

Certification is an ongoing process and companies that achieve the Certified Against Fraud Seal must be recertified annually. Companies that achieve the Certified Against Fraud Seal must apply for recertification by January 30 each year in order to be considered for recertification in that calendar year. TAG sends recertification notifications to all certified companies prior to the start of the recertification submission period.

TAG reviews all applications for recertification and notifies companies whether they have been recertified by March 1.

## 3. Covered Parties

The Certified Against Fraud Program is applicable to several types of entities across the digital advertising supply chain:

- Direct Buyers,
- Direct Sellers,
- Intermediaries, and
- Anti-Fraud and Measurement Services.

Companies applying for the Certified Against Fraud Seal must apply for the Seal under all relevant covered party categories, meeting the requirements relevant to each category, as described in Section 4.

### 3.1. Direct Buyer

Direct Buyers are advertisers who own advertisements for placement in inventory on the publisher's websites or other media properties, or advertising agencies that directly represent such advertisers.

The most Direct Buyer is an advertiser – a brand company represented in the advertisements that it wants to place in the publisher's inventory.

However, many brands hire an advertising agency to manage their advertising campaigns. A brand-appointed agency is also a Direct Buyer, except in cases it operates as an Intermediary. To qualify as a direct buyer, the agency must directly represent the advertiser.

### 3.2. Direct Seller

The most Direct Seller is a publisher that provides content to an audience. This type of Direct Seller sells ad space inventory on its websites or other media properties that offer value to advertisers depending on the size and demographics of the audience.

While a publisher may sell this inventory directly, larger publishers may appoint an agent to manage and sell this inventory. Such an agent is also a Direct Seller. To qualify as a Direct Seller, the agency must directly represent the publisher.

### 3.3. Intermediary

An Intermediary is a company that owns and/or operates a technology or service that allows for the purchase of digital inventory for the purpose of ad placement.

Intermediaries include both Indirect Sellers and Indirect Buyers.

- An Intermediary may be an Indirect Seller in that it sells a Direct Seller's inventory.
- An Intermediary may be an Indirect Buyer in that it is qualified to assign a Direct Buyer's advertisements to a Direct Seller's inventory.

Any entity that connects a Direct Seller to a Direct Buyer or an Indirect Seller through an ad technology layer or redirect is also an Intermediary.

### **3.4. Anti-Fraud & Measurement Services**

Anti-Fraud & Measurement Services are entities able to assist Direct Buyers, Direct Sellers and/or Intermediaries in the detection, measurement and/or filtering of invalid traffic from the digital advertising supply chain.

These entities do not transact inventory, but may be able to append to the creative payload or be declared in the campaign.

## 4. Certification Requirements

Requirements to achieve the Certified Against Fraud Seal differ according to a company's role in the digital advertising supply chain. To achieve the Certified Against Fraud Seal, an entity must meet relevant criteria based on the types of functions a given entity undertakes.

To achieve the Certified Against Fraud Seal, a company must meet the requirements for all the categories in which it operates, according to the table below.

### 4.1. Requirements Table

Requirement	Scope	Direct Buyer	Direct Seller	Intermediary	Anti-Fraud & Measurement Services
<b>Complete TAG Registration and be a TAG Member in Good Standing</b>	Administrative	✓	✓	✓	✓
<b>Have a designated TAG Compliance Officer</b>	Administrative	✓	✓	✓	✓
<b>Attend a Certified Against Fraud Training annually</b>	Administrative	✓	✓	✓	✓
<b>Comply with GIVT Detection and Filtration Requirements of MRC IVT Guidelines</b>	Anti-Fraud	✓	✓	✓	✓
<b>Employ Domain Threat Filtering</b>	Anti-Fraud	✓	✓	✓	✓
<b>Employ Data Center IP Threat Filtering</b>	Anti-Fraud	✓	✓	✓	✓
<b>Implement Publisher Sourcing Disclosures</b>	Transparency		✓		
<b>Implement Payment ID System</b>	Transparency			✓	
<b>Implement Ads.txt</b>	Transparency		✓		

## 4.2. Complete TAG Registration and be a TAG Member in Good Standing

To achieve the Certified Against Fraud Seal, any participating company must first become a TAG member, completing the process of becoming “TAG Registered” and enrolling in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG directly or visiting [www.tagtoday.net](http://www.tagtoday.net).

Companies seeking the Certified Against Fraud Seal must also have active TAG memberships that include participation in the Certified Against Fraud Program, have a valid TAG membership agreement in place, and be current on payment for all TAG membership fees.

## 4.3. Have a Designated TAG Compliance Officer

To achieve the Certified Against Fraud Seal, any participating company must have designated a qualified TAG Compliance Officer.

The role of the TAG Compliance Officer is described in section 2.6.a of this document.

## 4.4. Attend a Certified Against Fraud Training Annually

In order to achieve the Certified Against Fraud Seal, the designated TAG Compliance Officer at any participating company must, at least once in a 12-month period, attend a Certified Against Fraud training.

TAG provides training on a regular basis via a virtual platform so that TAG Compliance Officers are able to obtain training regardless of geographic location. TAG Compliance Officers can learn more and RSVP for training sessions by visiting [www.tagtoday.net](http://www.tagtoday.net).

## 4.5. Comply with General Invalid Traffic (GIVT) Detection and Filtration Requirements of Media Ratings Council’s (MRC) Invalid Traffic (IVT) Guidelines

To achieve the Certified Against Fraud Seal, any participating company must ensure that all of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are measured and filtered in a manner compliant with the General Invalid Traffic (GIVT) provisions of the Media Ratings Council’s (MRC) [Invalid Traffic \(IVT\) Detection and Filtration Guidelines Addendum](#).

The best path to compliance with this requirement depends on a participating company’s internal business practices, as well as the way it employs fraud detection and measurement within its organization.

If a participating company uses proprietary, in-house technology for fraud detection and measurement, that company must:

- achieve an MRC accreditation for digital services (including GIVT detection and filtration),

*or*

- be certified by an independent auditor that the company's fraud detection and measurement capacities are compliant with the GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum.

If a participating company relies on one or more third-party vendor(s) for fraud detection and measurement services – including fraud detection vendors, measurement services or third-party ad servers – that company must ensure that the relevant third-party vendor(s):

- achieve an MRC accreditation for digital services (including GIVT detection and filtration),  
*or*
- be certified by an independent auditor that its fraud detection and measurement capacities are compliant with the GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum.

Regardless of whether a participating company employs proprietary in-house technology or works with third-party vendors for fraud detection and measurement, the participating company must be able to show that all of the ad transactions and/or inventory that it handles is measured and filtered in a manner compliant with the GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum. This requirement is intended to encompass all types of digital ad inventory, including but not limited to desktop display, video, mobile web, social, in-app, audio, over-the-top (OTT), etc.

This requirement also means that all of the inventory handled by a participating company must be measured in a manner that is compliant – including inventory on that company's owned and operated media properties as well as any inventory handled by that company on behalf of a third-party partner.

#### ***4.5.a. Exception Process***

In rare cases, a participating company may find that it is not possible to ensure that a portion of its monetized ad transactions and/or inventory is measured and filtered in a manner compliant with the GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum. For example, this might be true in instances where the marketplace does not yet include vendors providing measurement and/or filtering services compliant with GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum for a specific type of digital ad inventory.

In such instances, a participating company may seek an exception to this requirement solely for the portion of its monetized ad transactions and/or inventory for which it is not currently possible to measure and filter in a manner compliant with the GIVT provisions of the IVT Detection and Filtration Guidelines Addendum.

To request such an exception, the participating company should provide an attestation on company letterhead from a Business Executive stating the scope of the requested exemption and the reason(s) why it is not currently possible to comply with the requirement.

## **4.6. Employ Domain Threat Filtering**

To achieve the Certified Against Fraud Seal, any participating company must implement domain

threat filtering across all of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles.

Domain threat filtering is the practice of filtering out domains that have been identified through business and technical means to have a high risk of being the destination for invalid traffic, and therefore of generating invalid ad impressions. Domain threat filtering is accomplished by developing or subscribing to a list of domain threats and of applying this list to current and future transactions.

Participating companies may choose to employ domain threat filtering pre-bid or post-bid as long as all of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are filtered for domain threats.

#### *4.6.a. Exception for Mobile In-App Inventory*

This requirement does not apply to mobile in-app inventory, except in cases when such in-app inventory is within an embedded browser (otherwise known as a mobile web browser) where the mobile app renders HTML pages in a browser. Examples include clicking on a link to a webpage from within a social app that leverages embedded browsers.

## 4.7. Employ Data Center IP Threat Filtering

To achieve the Certified Against Fraud Seal, any participating company must implement data center IP threat filtering across all of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles.

Data center IP threat filtering is the practice of filtering out IP addresses that have been identified through business and technical means to have a high risk of being the origin of invalid traffic, and therefore of generating invalid ad impressions, and of applying this list to current and future transactions. Data center IP threat filtering is accomplished by developing or subscribing to a list of data center IP addresses and of applying this list to current and future transactions.

Companies may choose to employ data center IP threat filtering pre-bid or post-bid as long as all of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are filtered for data center IP addresses.

#### *4.7.a. Use of TAG Data Center IP List*

The TAG Data Center IP List is available to assist companies in meeting this requirement. This tool is a common list of IP addresses with invalid traffic coming from data centers where human traffic is not expected to originate. This common list is not intended to include data center IP addresses where a mix of human and invalid traffic is expected to originate. The full process for utilizing the list is outlined in the *TAG Compliance Standard for the Data Center IP List*.

The TAG Data Center IP List is intended to be employed in addition to the data center IP threat filtering operations that companies employ internally or through third-party vendors. While the TAG Data Center IP List is a powerful tool aggregated from fraud detection vendors across the industry, it does not include the proprietary insights that would be available through a company's in-house detection or that of a third-party fraud detection vendor. For that reason, companies whose only means of employing data center IP filtering is use of the TAG Data Center IP List



will not be considered compliant with this requirement.

## 4.8. Implement Publisher Sourcing Disclosures

To achieve the Certified Against Fraud Seal, any company acting as a Direct Seller must disclose its practices related to paid traffic sourcing by implementing the requirements in the *TAG Publisher Sourcing Disclosure Requirements*.

### 4.8.a. Exception Process

A Direct Seller that does not source traffic from paid traffic sources, as defined in the *TAG Publisher Sourcing Disclosure Requirements*, may seek an exception to this requirement.

To request an exception, the Direct Seller should provide an attestation on company letterhead from a Business Executive stating that the company does not source traffic from paid traffic sources as defined in the *TAG Publisher Sourcing Disclosure Requirements*.

Once granted, an exception can be revoked for 12 months if a vendor that has achieved an MRC accreditation for digital services (including GIVT detection and filtration) or been certified by an independent auditor as compliant with the GIVT provisions of the MRC's IVT Detection and Filtration Guidelines Addendum reports to TAG a finding of more than 5% GIVT on inventory representing at least 10% of the Direct Seller's inventory pool.

## 4.9. Implement the Payment ID System

To achieve the Certified Against Fraud Seal, any participating company acting as an Intermediary must implement the TAG Payment ID System. Companies must participate in the Payment ID System for all transactions using the OpenRTB protocol.

The objective of the TAG Payment ID System is to reduce the volume of illegitimate ad inventory sold by enabling media buyers to avoid untrustworthy parties in the supply chain; and take effective remedial action if necessary.

## 4.10. Implement Ads.txt

To achieve the Certified Against Fraud Seal, any participating company acting as a Direct Seller must create a public record of its Authorized Digital Sellers by publishing an ads.txt file.

The required implementation of Ads.txt is described in the [IAB Tech Lab Ads.txt Specification](#).

## 5. Allegations of Non-Compliance & Appeal

Companies that achieve the Certified Against Fraud Seal must meet and maintain compliance with the relevant requirements set forth in the Certified Against Fraud Guidelines throughout the certification period. Failure to comply can result in consequences, including but not limited to the loss of certification and use of the Certified Against Fraud Seal. Certified companies are permitted to review allegations of non-compliance, submit rebuttal evidence, seek review of decisions of non-compliance and appeal any final decision.

The formal process governing non-compliance can be found in TAG's *Due Process for Allegations of Non-Compliance and Appeal*.