TAG Certified Against Fraud Guidelines

Version 5.0
Release July 2019

DRAFT

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 combating 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.

Table of Contents

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)[1]. Bot traffic impacts a wide variety of websites including those of well-known and premium publishers. Such bots continue to impact 9% of desktop display spending and 22% of desktop video spending in 2017.

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* – commissioned by TAG and conducted by The 614 Group - found that the use of TAG Certified distribution channels for digital advertising cut the IVT rate to 1.48% 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].

[1] The Association of National Advertisers / White Ops. "*The Bot Baseline: Fraud in Digital Advertising",* May 2017.

[2] Trustworthy Accountability Group / The 614 Group: "*TAG Fraud Benchmark Study",* December 2017.

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, complete the process of becoming "TAG Registered" and enroll in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG at info@tagtoday.net or visiting 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 their company to achieve the Certified Against Fraud Seal. To participate in the Certified Against Fraud Program, the 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.

Companies can choose to certify operations either by country (e.g. Brazil), by region (e.g. South America), or globally. Companies 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.

Companies choosing to certify operations for one or more countr(ies) in Europe, the geographic region of Europe, or globally, must apply to achieve the Certified Against Fraud Seal through independent validation rather than self-attestation.

2.4 Methods of Certification

Companies can apply to achieve the Certified Against Fraud Seal using one of two methods: self-attestation or independent validation.

A company has the option to choose either method, except in cases noted in Section 4.5 of the *Certified Against Fraud Guidelines* and in TAG's *Due Process for Allegations of Non-Compliance and Appeal*, available on www.tagtoday.net. In cases when a company chooses to certify its operations for one or more countr(ies) in Europe, the geographic region of Europe, or globally, that company is required to certify through independent validation. The certification method is recorded and displayed on www.tagtoday.net.

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, as well as a detailed description of the means by which a company is complying with each relevant requirement.

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*, as well as 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. 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 through 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*.

A company has the option to choose self-attestation except in cases noted in Section 4.5 of the *Certified Against Fraud Guidelines* and in TAG's *Due Process for Allegations of Non-Compliance*

and Appeal, available on www.tagtoday.net, as well in cases when a company chooses to certify its operations for one or more countr(ies) in Europe, the geographic region of Europe, or globally.

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.

Companies choosing to certify operations for one or more countr(ies) in Europe, the geographic region of Europe, or globally, must apply to achieve the Certified Against Fraud Seal through independent validation.

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.

Entities that wish to achieve the TAG Certified Against Fraud Seal through independent validation should have the validating company submit to TAG: an *Independent Validation Attestation* and a quarterly audit report, as well as a signed TAG *Compliance Officer Attestation* and *Business Executive Attestation*.

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

certification seal 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*, available on www.tagtoday.net.

2.6.b. Compliance Team

While the only 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 in order for the company to achieve 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 ensure 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 31 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 achieved recertification by March 1.

3. Covered Parties

The Certified Against Fraud Program is applicable to several types of covered parties 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 4.1.

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 covered party 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 it 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
Complete TAG Registration and be a TAG Member in Good Standing	Administrative	✓	✓	✓	✓
Have a designated TAG Compliance Officer	Administrative	✓	✓	✓	✓
Attend a Certified Against Fraud Training annually	Administrative	✓	✓	✓	✓
Comply with GIVT Detection and Filtration Requirements of MRC IVT Guidelines	Anti-Fraud	✓	✓	✓	✓
Employ Domain Threat Filtering	Anti-Fraud	✓	✓	✓	✓
Employ Data Center IP Threat Filtering	Anti-Fraud	✓	✓	✓	✓
Employ App Threat Filtering	Anti-Fraud	✓	✓	✓	✓
Implement Publisher Sourcing Disclosures	Transparency		✓		
Implement Payment ID System	Transparency			✓	
Implement and Honor Ads.txt Flles	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, complete the process of becoming "TAG Registered" and enroll in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG at info@tagtoday.net or visiting 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 designate 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, any participating company's designated TAG 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 in order for the company to achieve 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.

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.

4.5. Comply with General Invalid Traffic (GIVT) Detection and Filtration Requirements of Media Rating 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 Rating Council's (MRC) *Invalid Traffic (IVT) Detection and Filtration Guidelines Addendum*[3].

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.

[3] http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf

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 MRC's *IVT Detection and Filtration Guidelines Addendum*.

To request such an exception, the participating company should provide an attestation on company letterhead signed by 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.

4.5.b. Use of a Sampling Methodology in GIVT Measurement

Recognizing that the MRC has identified a path to compliance with the GIVT provisions of the MRC's *IVT Detection and Filtration Guidelines Addendum* using IVT sampling (i.e. not applying IVT techniques on a census impression basis to 100% of monetizable transactions) as outlined in the MRC's interim guidance related to IVT Sampling[4], companies may seek to meet the requirement to comply with the GIVT provisions of the MRC's *IVT Detection and Filtration Guidelines Addendum* using a sampling methodology in the following limited cases:

- 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) using a sampling methodology accepted by the MRC in the course of accreditation.

- 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) using a sampling methodology accepted by the MRC in the course of accreditation.

Companies must be able to provide documentation that the relevant MRC accreditation was achieved using a sampling methodology that was submitted to and approved by the MRC.

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 origin and/or destination for invalid traffic, and therefore of generating invalid traffic. Domain threat filtering is accomplished by developing or subscribing to one or more list(s) of domain threats and of applying the list(s) 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.

4.7. Employ App Threat Filtering

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

App threat filtering is the practice of filtering out apps that have been identified through business and technical means to have a high risk of being the origin and/or destination for invalid traffic, and therefore of generating invalid traffic. App threat filtering is accomplished by developing or

[4] http://mediaratingcouncil.org/RP020817_IVT%20Sampling.pdf

subscribing to one or more list(s) of app threats and of applying the list(s) to current and future transactions.

Participating companies may choose to employ app 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 app threats.

4.8. 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 traffic, 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.

4.8.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*[5].

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.

4.9. Implement Publisher Sourcing Disclosures

To achieve the Certified Against Fraud Seal, any company acting as a Direct Seller that provides content to an audience through its website(s) or other media properties (herein described as a "publisher") must disclose its paid traffic sourcing practices.

[5] Access to TAG's Data Center IP List and all onboarding material, including TAG's *Compliance Standard for the Data Center IP List*, is available to TAG Certified Against Fraud program participants or to TAG members as an ala carte option upon request.

Paid traffic sourcing is defined as any method by which a publisher increases the number of visits to its websites or other media properties by providing monetary consideration to a third party.

A **visit** is defined in the *IAB Audience Reach Measurement Guidelines*[6] as:

- The activities from a uniquely identified client that ends when there are 30 consecutive minutes of inactivity between the client and the server. HTTP inactivity is specified rather than mouse/keyboard inactivity.
- Visits are counted in the reporting interval that they start in.
- In streaming environments, use best effort to determine user inactivity, given that there might not be client-to-server communication between the client and the ad server (VAST 4.0 / Server-Side Ad Stitching).
- A visit is considered "acquired through paid sources" if the first page view is from a paid source.
- A visit is determined to be from a Paid Traffic Source based only on attributes collected during that visit.

A **paid traffic source** is defined as any third party that receives monetary consideration, including, without limitation, payment-in-kind, from a publisher to drive traffic to that publisher's website(s) or other media properties. Paid traffic sources include, but are not limited to, the following categories:

- Direct Native / Sponsored Content
- Paid Email Marketing
- Social media
- Affiliate Links
- Programmatic
- CPC / Paid Search

Publishers must disclose the percent of visits acquired through paid traffic sources representative of total visits. Those disclosures must be made against each of the four most recent quarters of the calendar year, as shown in Exhibit A.

Exhibit A – Example: Paid Sourced Traffic Disclosure Published in Q2 2018

Quarter	Percentage
Q3, 2017	5.1%
Q4, 2017	18.2%
Q1, 2018	12.6%
Q2, 2018	7.5%

[6] https://www.iab.com/wp-content/uploads/2015/06/AudienceReachMeasurementGuidelines.pdf

Paid traffic sourcing disclosures must be updated quarterly to reflect the updated percentages of paid traffic sourced to a website or other media property, as well as any changes in a publisher's paid traffic sourcing practices.

Paid traffic sourcing disclosures must be made easily and publicly available. For example, publishing a visible link in the footer of a publisher's website or other media property would be a compliant manner in which to provide a paid traffic sourcing disclosure.

To enable increased transparency and further quantify risk, a participating company may choose to make additional points or disclosures available as recommended in the *TAG Best Practices for Publisher Sourcing Disclosures*.

4.9.a. Exception Process

A Direct Seller that does not generate traffic from paid traffic sources, as defined in the *TAG Best Practices for Publisher Sourcing Disclosures,* may seek an exception to this requirement.

To request an exception, the Direct Seller should provide an attestation on company letterhead signed by a business executive stating that the company does not source traffic from paid traffic sources as defined in the *TAG Best Practices for Publisher Sourcing Disclosures*.

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.

4.10. 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.

4.11. Implement and Honor Ads.txt Files

To achieve the Certified Against Fraud Seal, any participating company must implement and honor ads.txt files as required for each covered party category in which that company falls, as defined in Section 3.0.

- If a participating company is acting as a Direct Seller, that company must publish an ads.txt file. The required implementation of ads.txt is described in the *IAB Tech Lab*

Ads.txt Specification[7].

- If a participating company is acting as a Direct Buyer, that company must honor a Direct Seller's ads.txt file if one has been published, buying only from entities identified within the published ads.txt file.

- If a participating company is acting as an Intermediary, that company must honor a Direct Seller's ads.txt file if one has been published, buying only from entities identified within the published ads.txt file.

[7] https://iabtechlab.com/wp-content/uploads/2017/09/IABOpenRTB_Ads.txt_Public_Spec_V1-0-1.pdf

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*, available on www.tagtoday.net.