



ANTI- FRAUD

CERTIFIED AGAINST FRAUD

Guidelines
Version 10
July 2024



ABOUT THE 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.

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 TAG

TAG, the Trustworthy Accountability Group, is the leading global initiative fighting criminal activity and increasing trust in the digital advertising industry. TAG's mission is to:

- [eliminate fraudulent traffic.](#)
- [facilitate the sharing of threat intelligence.](#)
- [promote brand safety and](#)
- [enabling transparency](#)

by connecting industry leaders, analyzing threats, and sharing best practices worldwide. The TAG community include the world's largest and most influential brands, agencies, publishers, and ad tech providers.

To learn more about the TAG, please visit www.tagtoday.net.

1. Executive Summary	4
2. Certification process	6
2.1. Application	7
2.1.a. Participation Fee	7
2.2. Qualification	7
2.3. Geographic Applicability of Certification	7
2.4. Method of Certification	8
2.4.a. Certification Through Self-Attestation	8
2.4.b. Certification Through Independent Validation	9
2.5. Publication of Certification Status	9
2.5.a. Certified Against Fraud Seal	9
2.6. Continued Compliance	10
2.6.a. TAG Compliance Officer	10
2.6.b. Compliance Team	10
2.6.c. Training	11
2.6.d. Quarterly Internal Reviews	11
2.6.e. Recertification	11
3. Covered Parties	12
3.1. Direct Buyers	13
3.2. Direct Sellers	13
3.3. Intermediaries	13
3.4. Anti-Fraud & Measurement Services	14
4. Certification Requirements	15
4.1. Requirements Table	16
4.2. Complete TAG Registration and Be a TAG Member in Good Standing	17
4.3. Have a Designated TAG Compliance Officer	17
4.4. Attend a Certified Against Fraud Training Annually	18
4.5. Employ Invalid Traffic (IVT) Detection and Removal	18
4.5.a. Exception Process	18
4.5.b. Use of a Sampling Methodology in IVT Detection and Removal	19
4.6. Employ Domain Threat Detection and Removal	19
4.7. Employ App Threat Detection and removal	20
4.8. Employ Data Center IP threat Detection and Removal	20
4.8.a. Use of TAG Data Center IP List	20
4.9. Implement a TAG-Recognised Follow-the-Money Solution	21
4.10. Implement and Honor Ads.txt and App-Ads.txt Files	21
4.11. Employ Ads.cert Authenticated Connections for SSAI Billing Notifications and Tracking	22
4.12. Employ Header Information in SSAI Ad TRACKING Requests	22
4.13. Define and identify Key roles and resources	23
4.14. Employ User Agent Structure for podcasting environments	23
5. Allegations of Non-Compliance & Appeal	25
6. Appendix A - TAG-Recognized Standards for IVT Detection and Removal	27
7. Appendix B - Change Log	29



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 **2018-2019 ANA / White Ops Bot Baseline** study projected losses to fraud to reach \$5.8 billion globally in 2019 while digital ad spending increased by 25.4 percent between 2017 and 2019¹.

TAG launched its Certified Against Fraud Program in 2016 to combat invalid traffic in the digital advertising supply chain. Companies that are shown to abide by **the Certified Against Fraud Guidelines** receive the Certified Against Fraud Seal and use the seal to publicly communicate their commitment to combating fraud.

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. With over 950 billion impressions analyzed globally across several advertising channels, IVT rates in TAG Certified Channels were reported as below 1% across all of TAG's Fraud research studies in 2022². Measured against the wider industry's IVT rate, TAG Certified Channels are at least over a third cleaner (in some cases 3 times cleaner) than non-certified channels.

¹ The Association of National Advertisers / White Ops. "The Bot Baseline: Fraud in Digital Advertising", April 2019.

² TAG's Data and Insights page - <https://www.tagtoday.net/insights>

The background features large, overlapping green geometric shapes in the corners, resembling stylized chevrons or arrows pointing towards the center. The colors range from a bright, vibrant green to a darker, forest green.

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 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 to begin the process for that company to achieve the Certified Against Fraud Seal. 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 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 The People’s Republic of China or Special Administrative Regions of China, one or more country/countries 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. METHOD 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 2.3 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 The People’s Republic of China or Special Administrative Regions of China, one or more country/countries 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 having 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 having 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 with 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 country/countries 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 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 The People's Republic of China or Special Administrative Regions of China, one or more country/countries 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 certification 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 combating 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 at www.tagtoday.net.

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 in order for the company to achieve the Certified Against Fraud Seal. Training must be renewed every 12 months 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 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.

The page features decorative green geometric shapes at the top and bottom. The top shape is a large, downward-pointing chevron composed of three overlapping layers in shades of green. The bottom shape is a large, upward-pointing chevron composed of three overlapping layers in the same shades of green. The text is centered between these two shapes.

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 BUYERS

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 SELLERS

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. INTERMEDIARIES

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

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	✓	✓	✓	✓
Employ Invalid Traffic (IVT) Detection and Removal	Anti-Fraud	✓	✓	✓	✓
Employ Domain Threat Detection and Removal	Anti-Fraud	✓	✓	✓	✓
Employ Data Center IP Threat Detection and Removal	Anti-Fraud	✓	✓	✓	✓
Employ App Threat Detection and Removal	Anti-Fraud	✓	✓	✓	✓
Implement a TAG-Approved Follow the Money Solution	Transparency			✓	
Implement and Honor Ads.txt and App-Ads.txt Files	Transparency	✓	✓	✓	

Cont.

Requirement	Scope	Direct Buyer	Direct Seller	Intermediary	Anti-Fraud & Measurement Services
Employ Ads.cert Authenticated Connections for SSAI Billing Notifications	Anti-Fraud			✓	
Employ Header Information in SSAI Ad Tracking Requests	Anti-Fraud			✓	
Define and Identify Key Roles and Resources	Anti-Fraud	✓	✓	✓	✓
Employ User Agent Structure for Podcasting Environments	Anti-Fraud		✓	✓	

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 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 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

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 every 12 months 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 can obtain training regardless of geographic location. TAG Compliance Officers can learn more and RSVP for training sessions by visiting www.tagtoday.net.

4.5. EMPLOY INVALID TRAFFIC (IVT) DETECTION AND REMOVAL

To achieve the Certified Against Fraud Seal, any participating company must ensure that 100% of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are filtered for both general invalid traffic (GIVT) and sophisticated invalid traffic (SIVT) in a manner compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.

The best path to compliance with this requirement depends on a participating company's internal business practices, as well as the way it employs IVT detection and removal within its organization:

- If a participating company uses proprietary, in-house technology to filter for IVT, that company must be certified by an independent auditor that its GIVT and SIVT detection and removal capacities are compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.
- If a participating company relies on one or more third-party vendor(s) for IVT measurement and filtration services – including fraud detection vendors, measurement services or third-party ad servers – that company must ensure that the relevant third-party vendor(s) are certified by an independent auditor that their GIVT and SIVT detection and removal capacities are compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.
- If a participating company acting as a Direct Seller relies on one or more Intermediary partners for IVT detection and removal, that company must ensure that 100% of its direct and/or reseller Intermediary partners have been awarded, and continue to hold, TAG's Certified Against Fraud Seal.

All inventory handled by a participating company – 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 – must be filtered for GIVT and SIVT in a manner compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.

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 filtered for IVT in a manner compliant with a TAG-recognized standard for IVT detection and removal, as referenced in Appendix A.

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 filter for IVT in a manner compliant with a TAG-recognized standard for IVT detection and removal, as referenced in Appendix A.

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 IVT Detection and Removal

Companies may seek to meet the requirement to comply with the GIVT and SIVT provisions of a TAG-recognized standard for IVT detection and removal, as referenced in Appendix A, using a sampling methodology in the following limited cases:

- If a participating company uses proprietary, in-house technology to filter for IVT, that company must be certified by an independent auditor that its GIVT and SIVT detection and removal capacities are compliant with a TAG-recognized standard for IVT detection and removal, as referenced in Appendix A, using a sampling methodology accepted by the independent auditor in the course of certification or accreditation.
- If a participating company relies on one or more third-party vendor(s) for IVT measurement and filtration services – including fraud detection vendors, measurement services or third-party ad servers – that company must ensure that the relevant third-party vendor(s) are certified by an independent auditor that their GIVT and SIVT detection and removal capacities are compliant with a TAG-recognized standard for IVT detection and removal, as referenced in Appendix A, using a sampling methodology accepted by the auditor in the course of certification or accreditation.

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

4.6. EMPLOY DOMAIN THREAT DETECTION AND REMOVAL

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

Domain threat detection and removal 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 detection and removal 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 detection and removal 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 DETECTION AND REMOVAL

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

App threat detection and removal 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 detection and removal is accomplished by developing or 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 DETECTION AND REMOVAL

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

- Data center IP threat detection and removal 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 detection and removal 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 detection and removal 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*³.

The TAG Data Center IP List is intended to be employed in addition to the data center IP threat detection and removal 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 threat detection and removal is use of the TAG Data Center IP List will not be considered compliant with this requirement.

³ 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.

4.9. IMPLEMENT A TAG-RECOGNISED FOLLOW-THE-MONEY SOLUTION

To achieve the Certified Against Fraud Seal, any participating company acting as an Intermediary must implement a TAG-recognized follow-the-money solution:

- The TAG Payment ID System or
- SupplyChain object and Sellers.json.

For additional guidance on how to implement the Payment ID System, companies should reference the *TAG Product Specification for Payment ID System*⁴.

If an Intermediary implements Sellers.json, they must disclose to TAG the company's methodology for timely maintenance of their Sellers.json file. Such Intermediaries must ensure that the accuracy of their Sellers.json file is assessed – at a minimum – as part of the company's Quarterly Internal Review Process.

Intermediaries are also required to implement *Identifier Names* within their Sellers.json file. Specifically, Intermediaries must use "TAG-ID" as a NAME, and include their TAG ID as the VALUE for that NAME, within the IDENTIFIER object in their Sellers.json file.

Companies may find their TAG ID within the company information section, at the top of their homepage on the TAG Member Portal. Otherwise, a company may email info@tagtoday.net for assistance regarding their TAG ID.

For additional guidance on how to implement Supply Chain Object and Sellers.json, companies should reference the *IAB Tech Lab OpenRTB Extension (SupplyChain) Object*⁵ and the *IAB Tech Lab Sellers.json Specification*.⁶

4.10. IMPLEMENT AND HONOR ADS.TXT AND APP-ADS.TXT FILES

To achieve the Certified Against Fraud Seal, any participating company must implement and honor ads.txt and app-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 on every domain that it monetizes through digital advertising. If that company owns and operates properties in the app environment, it must also create a public record of its Authorized Sellers and Resellers by publishing an app-ads.txt file for every app that it monetizes through digital advertising.
- Direct Sellers must develop procedures for the effective maintenance and accuracy of their applicable ads.txt and app_ads.txt file(s), and ensure that – at a minimum – a assessment of these files is conducted as part of the company's Quarterly Internal Review Process.
- Direct Sellers must also utilize the Certification Authority field for each ads.txt and app-ads.txt file which the Direct Seller publishes. Where applicable, the Certification Authority field must include, at a minimum, the TAG ID for each Intermediary listed as having a DIRECT or RESELLER relationship with the Direct Seller. In instances where a DIRECT or RESELLER Intermediary partner is not a member of TAG and does not have a TAG ID, the Direct Seller may leave the related Certification Authority field blank.

⁴ Access to TAG's Product Specification for Payment ID System and corresponding implementation specs are available to all TAG members through their onboarding packets.

⁵ <https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/supplychainobject.md>

⁶ https://iabtechlab.com/wp-content/uploads/2019/07/Sellersjson_Final.pdf

- If a participating company is acting as a Direct Buyer and/or 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. If that company is transacting with app inventory, it must also honor a Direct Seller’s app-ads.txt file if one has been published, buying only from entities identified within the published app-ads.txt file.

4.11. EMPLOY ADS.CERT AUTHENTICATED CONNECTIONS FOR SSAI BILLING NOTIFICATIONS AND TRACKING

To achieve the Certified Against Fraud Seal, any participating company identifying as an SSAI vendor, who fires billing notifications on behalf of devices on their server(s), needs to implement Authenticated Connections. An SSAI Vendor must establish call sign domains and operational capabilities required for Authenticated Connections, and they must utilize those capabilities when required by a partner.

SSAI Vendors are defined as Intermediaries that interface between a video-player and an ad-server, with the purpose of mediating the placement of ads into video content via Server-Side Ad Insertion (SSAI).

SSAI vendors must disclose their ads.cert call sign domain names directly to TAG. This data will be utilized as part of TAG’s metadata through the SSAI Billing Validations tool and will not be shared publicly.

The purpose of a secure authentication mechanism is to allow upstream “demand chain” participants (SSPs, DSPs, measurement vendors) to validate that the billing notifications coming from arbitrary cloud IP addresses do belong to the sellers who claims to be firing those notifications.

For additional guidance on how to set up Ads.cert Call Sign Domains and use them to implement Authenticated Connections, as well as utilize TAG’s registry to look up TAG registry metadata using Ads.cert Call Sign Domains, companies should reference *IAB Tech Lab’s Ads.cert Primer*⁷, *Call Sign Protocol*⁸ and *Authenticated Connections*⁹ documents, as well as TAG’s *Domain Certifications API Endpoint*¹⁰ document.

4.12. EMPLOY HEADER INFORMATION IN SSAI AD TRACKING REQUESTS

To achieve the Certified Against Fraud Seal, any participating company acting as an SSAI vendor as defined in Section 4.11 who fires ad tracking requests from servers across Server-Side Ad Insertion environments must employ the following HTTP headers with their ad tracking requests as called out in Section 1.1.2 of the *IAB Tech Lab Video Ad Serving Template (VAST) Specification*¹¹:

- X-Forwarded-For or X-Device-IP to indicate the IP address of the client device on behalf of which the notification is being sent.

⁷ <https://iabtechlab.com/wp-content/uploads/2021/09/1-ads-cert-primer-pc.pdf>

⁸ <https://iabtechlab.com/wp-content/uploads/2021/09/2-ads-cert-call-signs-pc.pdf>

⁹ <https://iabtechlab.com/wp-content/uploads/2021/09/3-ads-cert-authenticated-connections-pc.pdf>

¹⁰ Access to TAG Member Registry through SSAI Validations Tool available to TAG members upon request.

¹¹ https://iabtechlab.com/wp-content/uploads/2019/06/VAST_4.2_final_june26.pdf

- `X-Device-User-Agent` to indicate the User Agent of the client device on behalf of which the notification is being made

For additional guidance on how to implement headers in server-to-server ad tracking requests, companies should reference the *IAB Tech Lab Video Ad Serving Template (VAST) Specification*.

4.13. DEFINE AND IDENTIFY KEY ROLES AND RESOURCES

To achieve the Certified Against Fraud Seal, any participating company acting as a Buyer, Seller, Vendor, or Intermediary must define and identify the internal resource(s) responsible for the response to ad fraud events on behalf of the company. Internal resources are considered the personnel and/or team(s) responsible for responding to ad fraud events, as well as tools utilized by those personnel and/or team(s) to identify, mitigate and/or manage ad fraud events.

Companies must also document the responsible external resource(s) responsible for the response of ad fraud events. External resources are considered the personnel and/or team(s) with whom the identified internal resources communicate with regarding ad fraud events. The list below defines which external resource(s) must be documented for each applicable Covered Party type the company fulfills:

- Direct Buyers must document the responsible resource(s) with each of their vendor companies.
- Direct Sellers must document the responsible resource(s) with their direct intermediary companies in the supply chain.
- Intermediaries must document the responsible resource(s) with their buy-side and sell-side partners in the supply chain, as well as with their Anti-Fraud and Measurement Vendor(s).
- Vendors must document the responsible resource(s) for each client company for whom they are providing services as defined in Section 3.4.

Such responsible parties may include internal and external teams, provided that they demonstrate clear lines of communication across partners.

4.14. EMPLOY USER AGENT STRUCTURE FOR PODCASTING ENVIRONMENTS

To achieve the Certified Against Fraud Seal, any participating company identifying as a Podcast Distribution Player and/or a Podcast Creator must use the following user agent structure for all RSS feeds and audio files:

`<app name>/<app version><device info> <osname>/<os version><other info>`

For example, `AppName/1.2.3 Device Brand Device model OSName/1.2.3 LibName/1.2.3`

A User Agent is effectively an ID for any software that interacts with another software on behalf of an end user; each User Agent includes a string that is also shared with a server upon request for content, typically via request headers.

Podcast Creators are defined as entities which create Podcast content, and which may work with an agent to monetize Podcast content. Such Podcast Creators are considered as Direct Sellers.

Podcast Distribution Players (Agents) are defined as entities which own and operate a technology layer which enables the monetization and distribution of podcast content. Such agents are not required, and typically may not provide, podcast-player functionality. Such agents are considered as Intermediaries.



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.



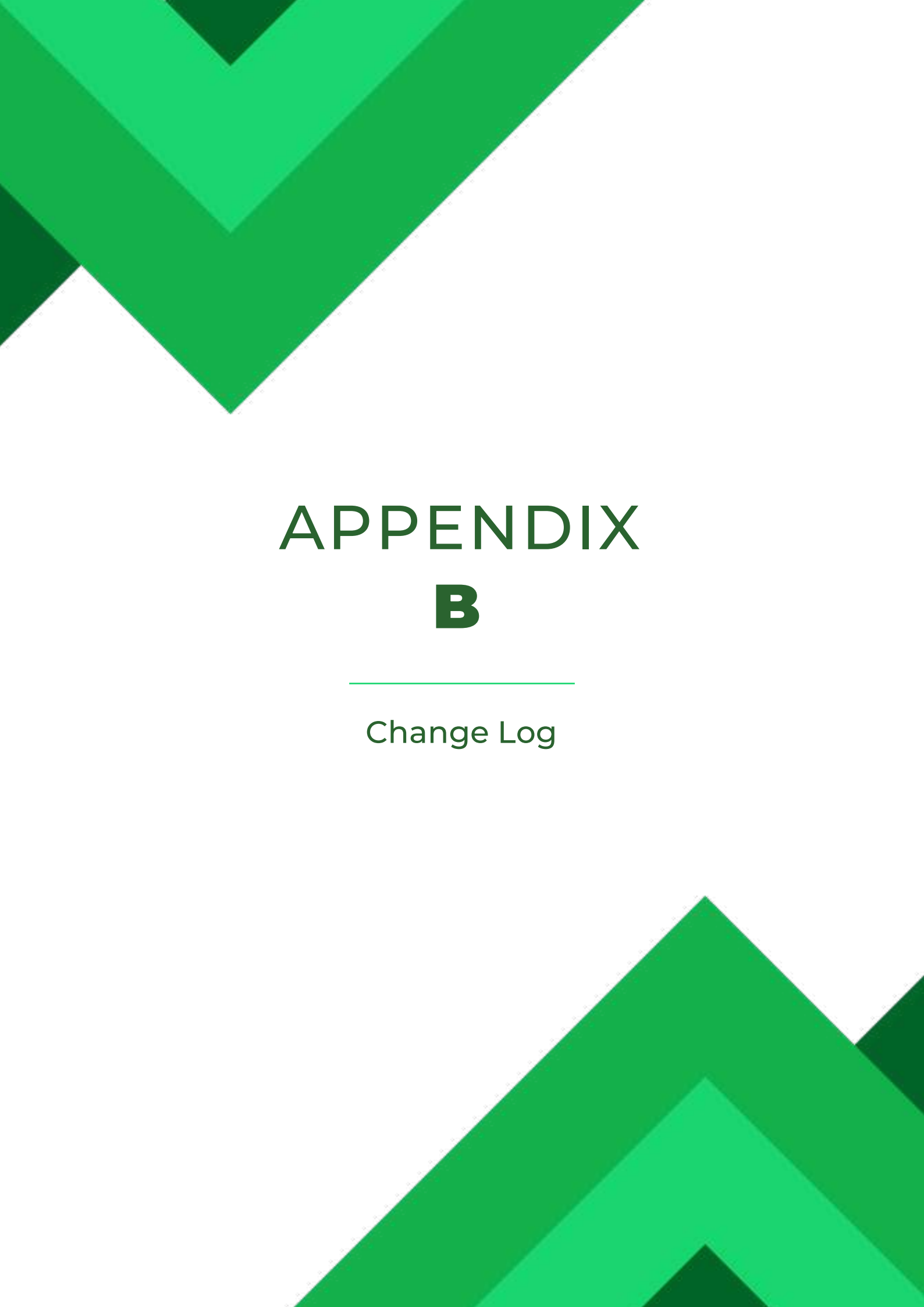
APPENDIX **A**

TAG Recognized Standards for IVT
Detection and Removal

A company choosing to comply with the requirement by accreditation to a TAG-Recognized standard must provide evidence of accreditation via the provisions of the following TAG-recognized standards as follows:

- *China Digital Advertising Delivery Monitoring and Verification Requirements T/CAAD 002-2020*
- Media Rating Council's (MRC) *Invalid Traffic (IVT) Detection and Filtration Guidelines Addendum*¹²

¹² <http://mediaratingcouncil.org/IVT%20Addendum%20Update%20062520.pdf>



APPENDIX **B**

Change Log

Version	Date Released	Changes
10.0	July 2024	v10 to update requirements around auditing sellers.json, app-ads.txt and ads.txt quarterly and ad new user agent requirements for podcasting environments.
9.1	December 2023	V9.1 to update IVT detection and removal requirement, enabling Direct Sellers to rely on one or more CAF-certified Intermediary partners for IVT detection and removal
9.0	July 2023	V9.0 requires all parties to identify key roles and resources, utilize TAG-ID in sellers.json and ads.txt files, and employ header information in SSAI ad requests and tracking
8.0	July 2022	V8.0 requires ads.cert Authenticated Connections implementation for SSAI billing notifications and tracking
7.3	February 2022	V7.3 to add Appendix calling out TAG-recognized standards for IVT detection and removal
7.2	March 2021	V7.2 to update independent validation requirements to apply to China
7.1	October 2020	V7.1 to update IVT detection and removal to include callouts to MRC IVT Guidelines for compliance.
7.0	July 2020	V7.0 to update IVT detection and removal, approved Follow-the-Money solution, and add app-ads.txt requirements.
6.0	January 2020	V6.0 to remove Publisher Sourcing Disclosure requirements and best practices, adding Change Log, updating research references and clarifying training requirement.
5.0	July 2019	V5.0 requires app threat filtering for companies working within in-app environments and removes in-app exceptions for domain threat filtering.
4.0	January 2019	V4.0 requires entities be certified via independent validation when certifying for European or Global operations, and extends ads.txt requirements to Direct Buyers and Intermediaries
3.0	July 2018	V3.0 allows for sampling under limited circumstances to meet the MRC IVT Guidelines compliance requirement, and expands the definition of “paid traffic source” in the Publisher Sourcing Disclosure requirement
2.0	January 2018	V2.0 clarifies existing requirements and includes new requirements for all types of covered parties , including: <ul style="list-style-type: none"> • All covered parties will be required to attend a Certified Against Fraud Training annually. • Direct Buyers will be required to meet existing requirements to employ domain threat filtering and data center IP threat filtering. • Direct Sellers will be required to create a public record of their Authorized Digital Sellers by publishing an ads.txt file.
1.0	November 2016	Initial Release

The background consists of several overlapping geometric shapes in two shades of green: a medium green and a darker forest green. The shapes are primarily triangles and quadrilaterals, creating a dynamic, abstract pattern. The medium green forms the base, while the darker green shapes are layered on top, some pointing towards the corners and others towards the center.

tag

tagtoday.net