TAG Certified Against Malware Guidelines

Version 1.0
Released November 2016

About the TAG Certified Against Malware Program

The mission of the TAG Certified Against Malware Program is to eliminate the distribution of malware throughout the digital advertising supply chain.

In order to guide companies in fighting malvertising effectively, the TAG Anti-Malware Working Group developed these Certified Against Malware Guidelines. The working group will continue to build a suite of anti-malware tools to aid in compliance with those guidelines.

Companies that are shown to abide by the Certified Against Malware Guidelines receive the "Certified Against Malware" Seal and can use the seal to publicly communicate their commitment to combatting malvertising in the digital advertising supply chain.

About the Trustworthy Accountability Group

The Trustworthy Accountability Group (TAG) is a first-of-its-kind, cross-industry accountability program fighting criminal activity across the digital advertising supply chain. TAG works collaboratively with companies throughout the supply chain in four areas critical to the continued growth and development of the $50 billion digital advertising industry:

- Eliminating Fraud
- Combating Malware
- Fighting Internet Piracy
- Promoting Transparency

A joint marketing-media industry program, TAG was created by the American Association of Advertising Agencies (4A's), Association of National Advertisers (ANA), and Interactive Advertising Bureau (IAB).

To learn more about the Trustworthy Accountability Group, please visit www.tagtoday.net.

Table of Contents

1. Executive Summary

Malware delivered through the advertising ecosystem degrades overall trust in the system by generating a poor consumer experience. Additionally, malware infected machines attack the advertising ecosystem in order to generate money for fraudsters. Because each participant in the ecosystem has visibility into only their subset of the problem, preventing the delivery of malware overall is challenging, resulting in continued attacks on consumers through the various uncoordinated parts of the system.

Establishing a method for coordinating the industry in its defense against malware peddlers is a priority for TAG. By defining a process for sharing information about malware in a manner that is trustworthy, legal, and consumer friendly, TAG helps the industry with a foundation to build a common and effective response to these attackers, thereby safeguarding the consumer from malware.

The following certification guidelines were developed as standards in anti-malware processes and cross-partner communication. When a company is TAG Certified Against Malware, that company will be known to follow a procedure that fights against malware and malicious actors.

2. Certification Process

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

Companies that achieve the “Certified Against Malware” Seal enter into an agreement with TAG in which the company is responsible for making inquiries, obtaining relevant and necessary reports, and otherwise regularly reviewing its activities so that it can represent and confirm at all times that it is in compliance with the Certified Against Malware requirements.

2.1 Application

Before a company can apply for the “Certified Against Malware” Seal, that company must first be “TAG Registered.” Companies can learn more and apply for TAG Registration by contacting TAG directly or visiting www.tagtoday.net.

Once a company has been approved as “TAG Registered,” the TAG Compliance Officer designated through the TAG Registration application process may contact TAG directly to begin the process for that company to achieve the “Certified Against Malware” Seal.

2.1.a Certification Fee

There is an annual fee required for participation in the Certified Against Malware Program. The certification fee supports the TAG infrastructure for processing and publishing certification, as well as for the continued development and evolution of the Certified Against Malware Program as needed to meet changes in technology and business practice.

2.2 Qualification

Any company that has been approved as “TAG Registered” can apply to participate in the Certified Against Malware Program.

2.3 Methods of Certification

The “Certified Against Malware” Seal can be achieved at two different tiers: self-certification and independent validation certification. A company has the option to choose one tier or the other. The selected method is recorded and displayed on the TAG website.

Self-certification is obtained with a self-attestation that the company is adhering to the Certified Against Malware Guidelines. Independent validation certification is obtained by inviting an independent vendor to validate that a company is adhering to these guidelines. The process is

parallel for both except that in an independent validation, the validating company submits additional required attestation paperwork.

Since the internal processes for both certification tiers are the same, a company that certifies under self-certification can add independent validation certification at any time to achieve the higher level of certification.

2.3.a Self-Certification

Self-certification is obtained with a self-attestation that the company is adhering to the Certified Against Malware Guidelines. Entities that wish to achieve the TAG "Certified Against Malware" Seal should submit to TAG a completed Certified Against Malware Self- Attestation Checklist and supporting materials for each of the relevant certification requirements. Following review of the self-attestation checklist and materials, TAG will notify the company as to whether they have met the relevant requirements of the Certified Against Malware Guidelines, or whether additional information is needed in order to confirm compliance.

2.3.b Independent Validation

To achieve certification by independent validation, a company must invite an independent vendor to validate that the company is compliant with the Certified Against Malware Guidelines. A validating company may be any accredited auditing company such as a licensed law firm or licensed CPA. In addition, any company that specializes in digital media audits that submits for and is approved by TAG may conduct independent validations.

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

Independent validation will include review 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 adding new partners, including how new partners are vetted (and "re-vetted")
- Policies and procedures related to complaint handling/resolution to ensure compliance with the Certified Against Malware Guidelines.
- Testing performed by the company as part of the quarterly review process (refer below for additional details regarding the quarterly review).

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

- Compliance Officer and Executive Attestations

- Independent Validation Attestation
- Quarterly audit report

2.4 Publication of Certification Status

With training and consistent monitoring procedures in practice, the company is certified when required documentation is submitted and certification status is posted to TAG's website. Upon certification, TAG sends materials to the company's TAG Compliance Officer on file for promoting the company's Certified Against Malware status.

The TAG publishes announcements for companies that have successfully implemented the Certified Against Malware Guidelines. The TAG website is updated as needed to reflect all current Certified Against Malware companies.

2.4.a "Certified Against Malware" Seal

Companies that are shown to abide by the Certified Against Malware Guidelines use the "Certified Against Malware" Seal to publicly communicate their commitment to combating malware in the digital advertising supply chain.

2.5 Continued Compliance

Recognizing that companies both large and small apply for Certified Against Malware certification, no requirements are made for the resources needed to support Certified Against Malware compliance aside from the requirements that Certified Against Malware companies must always have a designated TAG Compliance Officer.

2.5.a TAG Compliance Officer

To ensure that Certified Against Malware companies continue to maintain compliance with these guidelines, the compliant company must designate a TAG Compliance Officer. This is usually done during the TAG Registration application process, which is prior to participation in the Certified Against Malware Program.

No requirements are made for the job description or specific title or role requirement of the Compliance Officer, aside from its independence from sales and marketing as described below. The role of the TAG Compliance Officer is described on the TAG website.

The TAG Compliance Officer oversees the quarterly review process to ensure compliance with the Certified Against Malware Guidelines. If the company chooses to achieve certification by independent validation, the TAG Compliance Officer facilitates an independent vendor review for initial certification and each year thereafter for renewal. The independent vendor submits a letter of attestation validating the company's compliance with the Certified Against Malware Guidelines.

2.5.b Compliance Team

While the only requirement for the resources needed to support Certified Against Malware compliance is the designation of a TAG Compliance Officer, it is also recommended that a company have in place a Compliance Team that includes and assists the TAG Compliance Officer in monitoring compliance with the Certified Against Malware Guidelines.

2.5.c Training

“Certified Against Malware” training is required for the company’s TAG Compliance Officer, and is scheduled during the application process. The Compliance Officer is encouraged to attend the first training available after beginning the application process and must complete training within three months of the company having achieved the “Certified Against Malware” Seal. Training must be renewed on an annual basis.

2.5.d Quarterly Reviews

Certified Against Malware training for compliance focuses on outlining the principles for internal quarterly reviews. Quarterly reviews create consistency across the industry.

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

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

Internal quarterly reviews should also include a risk analysis of key control functions to assess how much testing is needed to validate adherence. Also, actual testing of data (i.e., web site traffic logs, etc.), both statistically and judgmentally based, should be used to validate that the existing control structure is designed correctly and operating effectively.

2.5.e Remediation

Independent Validation may result in findings that require remediation. In these situations, it is the responsibility of the Independent Validator to inform the TAG that remediation is required before the Independent Validation is complete. This will ensure complete transparency during the process. The details provided to TAG by the Independent Validator will remain confidential.

Upon successful remediation, Independent Validation Attestation will be submitted accordingly.

2.5.f Renewal

Certification under the Certified Against Malware Program is an ongoing process and must be renewed each year. The renewal documentation must be provided by January 31 for the

previous calendar year, which allows for independent validation to be completed in January and announcement of all compliant companies in March. TAG sends renewal notifications to all certified companies prior to the January 31 renewal submission date.

3. Covered Parties

The TAG Certified Against Malware Program is applicable to entities across the digital advertising ecosystem:

- Buyers;
- Sellers;
- Intermediaries (may be an indirect buyer/seller);
- Third parties/Vendors (e.g. creative scanning, verification companies).

4. Certification Requirements

In order to achieve the “TAG Certified Against Malware” Seal, companies must meet the following criteria in accordance with TAG best practices. Please refer to implementation guideline documents for further details relevant to company type.

4.1 Requirements Table

Requirement	Scope	Required for Certification
Complete TAG Registration	Administrative	✓
Have a designated TAG Compliance Officer	Administrative	✓
Document appropriate points of contact at partner companies	Anti-Malware	✓
In any new or updated legal agreements, document malware scanning responsibilities	Anti-Malware	✓
Scan a reasonable percentage of total creative inventory	Anti-Malware	✓
Company should have internal procedure around defining Red Flag Events and handling of standard malware incidents	Anti-Malware	✓
Designate an Anti-Malware Primary Contact	Anti-Malware	✓
Establish a formal post-mortem process for Red Flag malware incidents	Anti-Malware	✓
Conduct semi-annual reviews of post-mortems	Anti-Malware	✓

4.2 Complete TAG Registration

In order to achieve the “Certified Against Malware” Seal, a company must first be “TAG Registered.” Companies can learn more and apply for TAG Registration by contacting TAG directly or visiting www.tagtoday.net.

4.3 Designate TAG Compliance Officer

In order to achieve “Certified Against Malware” Seal, a company must have identified a TAG Compliance Officer. (The TAG Compliance Officer is usually designated in the course of that company’s application for TAG Registration.)

The role of the TAG Compliance Officer is described in greater detail in the “Continued Compliance” section of the Guidelines.

4.4 General Principles of Certification Requirements

- Each company placing ads on behalf of another is responsible for what the party they represent puts into the ad placement, and for the supply chain within one hop.
- Each company should employ technical and/or business process measures to prevent malware that are applicable, and feasible, for its position and role in the chain.
- Each company should regularly update its technical and business process measures to keep up with TAG guidelines and best practices, as such may be published or revised from time to time.
- Additional video and mobile guidelines may be provided by TAG to provide additional certification criteria for these environments.

4.5 Know your Partner

Companies should have in place processes and procedures to proactively evaluate the trustworthiness of buy-side clients. Additionally, companies should document responsibilities and accountabilities with regards to malware.

- Establish a strong, persistent identity for the next company taking responsibility for malware both in the direction of demand and in the direction of supply. Understanding the supply chain partners allows rapid and precise escalation and notification.
    - Document the appropriate contact person and their redundancies, as available, at these partners.
    - Fall back to the Anti-Malware Primary Contact designated to TAG as needed.

- In any new or updated legal agreements, whether B2B contract language, ToS, SLA, public policies, or other places that a business expectation is set with a partner, document malware scanning responsibilities and accountabilities.
    - This requirement is only for new and updated legal agreements, not for those that aren’t updated.
    - Create an updated plan for legal agreements that are untouched for other reasons.

4.6 Continuously Verify

In order to protect against malware, companies should scan ad tags, creatives, and landing pages for malware as suggested by TAG guidance. Companies should have in place monitoring procedures to evaluate in an ongoing manner the technical and business risks of malware delivery from all sources and partners.

- Follow industry best practices, like TAG's Best Practices for Scanning Malware, to properly schedule scanning of ad tags, creatives and landing pages.
    - Scan a reasonable percentage of total inventory.
    - Understand and vary the depth of scanning for tags, creatives, and landing pages.

4.7 Be Prepared

Companies should educate their employees and customers about malware prevention, including Red Flags to watch for and how to escalate concerns to appropriate persons within their organization.

- Companies should have internal procedure around defining Red Flag events and handling of standard malware incidents relative to their business.
    - Escalate malware incidents based on the definition/scope of Red Flag Event (see glossary section for examples).
    - Malvertising Red Flag Event will be defined relative to each company based on one or more of these factors: revenue impact, user experience, or sophistication of malware attack.
    - Incidents may be communicated to upstream vendors or business partners without qualifying the incident as a Red Flag Event.
        - Use communication with other companies in determination if the incident is a Red Flag Event, utilizing any available TAG hosted communication tools.
- A designated Anti-Malware Primary Contact functions as an owner of Anti-Malware responsibilities from each certified company.
    - The Anti-Malware Primary Contact should come from ad operations, development, or policy enforcement roles. The primary contact manages communications and networks of people who resolve malware events. There may also be a preferred point of contact such as a group alias to communicate on malware events.
    - The Anti-Malware Primary Contact must maintain communication with their representative TAG Compliance Officer.
        - TAG Compliance can be informed by either TAG or Anti-Malware internal team. Main goal of TAG Compliance Officer is compliance on quarterly cadence, main goal of Anti-Malware Primary Contact is in-event

responsiveness. No in-event requirement of communication, but rather on quarterly/semi-annual check ins.
    - The Anti-Malware Primary Contact will be available or have assigned responsibility to appropriate staff for handling malware-related escalations or notifications during all hours that staff would otherwise be available.
    - The Primary Contact is notified of a malware Red Flag event and is then responsible for procedure leading to resolution and enforcement.
        - Red Flag response procedure may include investigation, action, and communication with appropriate staff.
        - Red Flag event notification should be addressed immediately.
        - Primary Contact must ensure goodwill communication with partners having B2B contracts, ToS, SLA, or any business expectations.
- Establish a formal post-mortem process for Red Flag malware incidents and follow this process.
    - Companies will ensure that an internal post-mortem process is in place, which will examine Red Flag Events as defined above.
    - Post-mortem for a Red Flag event should occur as promptly as possible after the investigation and resolution. Within one week is recommended.
    - Post-mortem process may require time to research and refine as each company determines scope for post-mortem triggers.
- Conduct a semi-annual (or, optionally, more frequent) review of post mortems, aligning these to the documented response strategy, updating the response strategy as needed.
    - Review post-mortem process to account for resources or function growth/change.

4.8 Glossary of Certified Against Malware Terms

- Anti-Malware Primary Contact: A designated representative for TAG Anti-Malware incident response.
- Red Flag Event: A malware event that reaches a level of significance dependent on the following factors, relative to each company:
    - Significant revenue impact
    - Consumer experience (or a highly publicized event)
    - Sophistication of the malvertising event
- Post Mortem: A response procedure that that occurs after the identification and resolution of a malware event, in order to effectively share knowledge of the event. Post-mortems will produce feedback into learning and improving anti-malware policy and procedure.
- Malware: Any malicious software impacting a computer or device (e.g. phone, tablet, connected device, or router) without user consent. This can include (but not limited to) spyware, worms, bots, viruses, adware, phishing, auto-subscription, or unwanted changes to system configurations.

- Examples of Malware events can include:
  - **Drive-by-Download -** Users unintentionally download malicious software to their device, without their knowledge.
    - This may occur via an ad impression.
  - **Deceptive Download** - Users authorize a download. However malicious software is download either instead or in addition to the authorized download.
    - This may occur via an ad click, a deceptive ad posing as other content, or via a link on a landing page.
  - **Auto-Redirecting -** Without interaction, an advertisement or script automatically redirects users to a website or app (typically an app store). The site or app can deliver malicious software to the user.

Any of the above can be coupled with personalized or interest based advertising, targeting specific users.

5. Governance, Enforcement & Appeal

Compliance with the Certified Against Malware Program is peer-enforced. In order to ensure that the value of the Certified Against Malware Program is maintained, formal processes should be in place regarding governance and oversight of the program, as well as for companies to make complaints about non-compliance, and to appeal such complaints.

5.1 Governance and Oversight

The Certified Against Malware Program is governed by the TAG Board of Directors (Board). The TAG Board will:

- Evaluate any complaints made against companies that have achieved the “Certified Against Malware” Seal and determine the responsible party and penalty.
- Provide guidance and vision for current and future Certified Against Malware Program efforts.
- Oversee and ensure progress of Certified Against Malware efforts.
- Evangelize the program in the marketplace.
- Ensure any policy issues within the Certified Against Malware effort are properly shared with the TAG Policy Leadership.

5.2 Complaints of Non-Compliance

Reports made against companies that have achieved the “Certified Against Malware” Seal may be one of two complaint types:

- Generalized non-compliance with Certified Against Malware Guidelines
- Non-compliance with a subcomponent of Certified Against Malware Guidelines

Reports regarding Certified Against Malware non-compliance may affect certification.

A company that is party to a transaction involving entities “Certified Against Malware” may submit a complaint against another party of the transaction regarding any non-compliance experienced. The report must include specific evidence of non-compliance and must be signed by someone of at least manager level at the company making the complaint.

End-users, security companies, or other parties not specific to the transaction may report about malware events, but this information does not necessarily impact Certification.

To submit a complaint of non-compliance, please email antimalware@tagtoday.net.

5.3 Validating Complaints

Upon receiving a complaint, the Board votes on whether the complaint is valid. If deemed valid, the accused Certified Against Malware company is notified of the complaint before the Board makes a judgment regarding the complaint.

Before judgment on a complaint is made, the accused company may repudiate the allegation of noncompliance or remediate any alleged incidents of non-compliance.

If the Board makes a judgment against the accused company, the company must work in a good faith effort to resolve the complaint as quickly as possible.

5.4 Loss of Certification

If three or more complaints against a single company are deemed valid within a six-month period and valid complaints are not resolved within that six-month period, certification for the Certified Against Malware-certified company is removed. The company must cease to market itself as a Certified Against Malware-certified company and the company name is removed from the published list of companies that are certified to TAG's Certified Against Malware Certification Requirements. Complaints are not made public.

5.5 Appeal and Recertification

Within 10 days of the Board decision to remove certification, the company may appeal before the full Board.

In order to become recertified, the company must provide documentation on how and when the complaint was addressed and the steps it has taken to ensure that similar problems will not occur in the future. Documentation of complaint resolution must be presented before the full Board.

If the majority of the Board is satisfied with the explanations and evidence of resolution, the company may pay a recertification fee to TAG and resume marketing itself as a "Certified Against Malware" Seal company. The company is also republished to the list of companies that have achieved the "Certified Against Malware" Seal.