TAG Certified Against Malware Guidelines

DRAFT

Version 3.0
Release July 2019
DRAFT

About the TAG Certified Against Malware Program

The mission of the TAG Certified Against Malware Program is to prevent, mitigate and remediate malware events using the digital advertising supply chain as an attack vector.

In order to guide companies in fighting malware using the digital advertising supply chain as an attack vector effectively, the TAG Anti-Malware Working Group developed and maintains the *Certified Against Malware Guidelines*, as well as 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* can achieve the Certified Against Malware Seal and use the seal to publicly communicate their commitment to combatting malware using the digital advertising supply chain as an attack vector.

DRAFT

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 Trustworthy Accountability Group, please visit www.tagtoday.net.

Table of Contents

DRAFT

DRAFT

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 to generate money for fraudsters. Each participant in the ecosystem has limited visibility into their subset of the problem, but preventing the delivery of malware overall is challenging and results in continued attacks on consumers through various uncoordinated parts of the system.

TAG launched its Certified Against Malware Program in 2016 to provide companies with a roadmap by which to combat malware effectively across the digital advertising supply chain. The TAG Anti-Malware Working Group developed and maintains the *Certified Against Malware Guidelines*, as well as a suite of anti-malware and information-sharing tools to aid in compliance with those guidelines.

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.

DRAFT

1.1. Defining Malware

For TAG's purposes, malware is defined as any malicious software impacting a computer or device (e.g. phone, tablet, connected device, or router) without user consent. This may include but is not limited to spyware, worms, bots, viruses, adware, phishing, auto-subscription, or unwanted changes to system configurations.

Examples of malware events may include, but are not limited to:

- **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.

- **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 downloaded instead and/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.

2. Certification Process

The TAG Certified Against Malware Program is voluntary and represents the ongoing process of defining and maintaining guidelines for effectively combating malware using the digital advertising supply chain as an attack vector.

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 Malware Seal, companies must show that all of their material operations related to ad monetization services within a particular geographic market are in compliance with the relevant requirements of the *Certified Against Malware Guidelines.*

2.1. Application

Before a company can apply for the Certified Against Malware 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 Malware Program in order to begin the process for their company to achieve the Certified Against Malware Seal. In order to participate in the Certified Against Malware Program, the company's TAG membership must include access to that program.

DRAFT

2.1.a. Participation Fee

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

2.2. Qualification

All TAG member companies in good standing and enrolled in the Verified by TAG Program and whose TAG membership includes participation in the Certified Against Malware Program can participate in the Certified Against Malware Program and apply for the Certified Against Malware Seal.

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

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

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

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

2.4. Methods of Certification

Companies can apply to achieve the Certified Against Malware 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 TAG's *Due Process for Allegations of Non-Compliance and Appeal,* available on www.tagtoday.net. The selected method is recorded and displayed on www.tagtoday.net.

DRAFT

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 Malware 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 Malware 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 Malware Guidelines* and that it will maintain compliance throughout the certification period and the company attesting that it will maintain compliance throughout the certification period. A validating company may be any auditing company that includes a specialty in digital media audits.

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

Since the internal processes for both self-attestation and independent validation certification are the same, a company that has achieved the Certified Against Malware 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 Malware Guidelines*.

Entities that wish to achieve the TAG Certified Against Malware Seal through self-attestation should submit to TAG a completed *Certified Against Malware 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 Malware 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 Malware Guidelines*. A validating company may be any auditing company that includes a specialty in digital media audits.

While independent validation is designed to provide limited assurance, ensuring that all *Certified Against Malware 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.

DRAFT

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 Malware Guidelines*.
- 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 internal quarterly review process.

Entities that wish to achieve the TAG Certified Against Malware 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 Malware 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 Malware status.

2.5.a. Certified Against Malware Seal

Companies that are shown to meet the *Certified Against Malware Guidelines* receive the Certified

Against Malware Seal and can use the seal to publicly communicate their commitment to combatting malware using the digital advertising supply chain as an attack vector.

2.6. Continued Compliance

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

2.6.a. TAG Compliance Officer

Companies participating in the Certified Against Malware 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 Malware 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).

DRAFT

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 regarding 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 required requirement to support compliance with the Certified Against Malware 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 Malware Guidelines*.

2.6.c. Training

Certified Against Malware training is required for the company's designated TAG Compliance Officer. The Compliance Officer is encouraged to attend the first training available after their company is enrolled in the Certified Against Malware Program and must complete training in order for the company to achieve the Certified Against Malware Seal. Training must be renewed on an annual basis in order for a company to maintain its Certified Against Malware 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 Malware Seal maintains full compliance with the *Certified Against Malware Guidelines* throughout the year.

DRAFT

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

- The *Certified Against Malware Guidelines* are consistently and completely followed.
- Control activities discussed during Certified Against Malware 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 Malware Seal must be recertified annually. Companies that achieve the Certified Against Malware 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 Malware Program is applicable to several types of entities across the digital advertising supply chain:

- Direct Buyers,
- Direct Sellers,
- Intermediaries, and
- Vendors (including breakout of vendor types)

Companies applying for the Certified Against Malware 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.

DRAFT

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 publisher inventory but does not have a direct, contractual relationship with the publisher.
- An Intermediary may be an Indirect Seller in that it sells a Direct Seller's inventory.

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

Any entity that connects a Direct Seller to a Direct Buyer or an Indirect Seller through an ad technology layer or redirect is also an Intermediary. Additional intermediary companies include media vendors DSPs, SSPs, Exchanges.

3.4. Vendors

There are two ways for a company to be considered a vendor:

- Measurement/analytics companies (referred to as 'vendors' in requirement use cases tables).
- Verification/privacy companies (referred to as 'scanning companies' in requirement use cases tables).

Measurement/analytics companies do not transact inventory, but, depending on company type, they could be appending the creative payload. This covers any company that is dropping script into the creative. This may include DMPs or audience measurement companies.

Verification/privacy companies do not transact inventory but are responsible for providing anti-malware services before transaction of inventory, e.g. anti-malware scanning. These companies are also able to provide reporting and insights on malware threats.

DRAFT

4. Certification Requirements

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

To achieve the Certified Against Malware 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 Buyers	Direct Sellers	Intermediaries	Vendors
Complete TAG Registration and be a TAG Member in Good Standing	Administrative	✓	✓	✓	✓
Have a designated TAG Compliance Officer	Administrative	✓	✓	✓	✓
Attend a Certified Against Malware Training annually	Administrative	✓	✓	✓	✓
Designate a Primary Anti-Malware Contact	Anti-Malware	✓	✓	✓	✓
Document Appropriate Points of Contact at Partner Companies	Anti-Malware	✓	✓	✓	✓
Document Malware Scanning Responsibilities in Any New or Updated Legal Agreements	Anti-Malware	✓	✓	✓	✓
Scan Assets and Landing Page URLs Preceding Initial Delivery and Disclose Initial Scanning Methodologies to TAG	Anti-Malware	✓	✓	✓	✓
Rescan Assets and Landing Page URLs and Disclose Rescanning Methodologies to TAG	Anti-Malware	✓	✓	✓	✓
Employ Internal Procedures for Defining Red Flag Events and Handling of Standard	Anti-Malware	✓	✓	✓	✓

DRAFT

Malware Incidents					
Employ Seat ID Attributes to Troubleshoot and Handle Malware Incidents	Anti-Malware	✓	✓	✓	
Establish Formal Post-Mortem Process for Red Flag Events	Anti-Malware	✓	✓	✓	
Conduct Semi-Annual Reviews of Post-Mortems	Anti-Malware	✓	✓	✓	

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

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

DRAFT

4.3. Have a Designated TAG Compliance Officer

To achieve the Certified Against Malware 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 Malware Training Annually

In order to achieve the Certified Against Malware 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 Malware Program and must complete training in order for the company to achieve the Certified Against Malware Seal. Training must be renewed on an annual basis in order for a company to maintain its Certified Against Malware 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. Designate an Anti-Malware Primary Contact

To achieve the Certified Against Malware Seal, any participating company must designate an Anti-Malware Primary Contact to function as owner of anti-malware responsibilities for that

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. The TAG Compliance Officer's main goal is focused on compliance on quarterly cadence, whereas the Anti-Malware Primary Contact focuses on in-event responsiveness. In-event communication is not required, but the Anti-Malware Primary Contact should provide quarterly/semi-annual check ins.

The Anti-Malware Primary Contact should be available or assign responsibility to appropriate staff for handling malware-related escalations or notifications during all hours that staff would otherwise be available.

The Anti-Malware Primary Contact should be notified of a Red Flag malware event (as defined in Section 4.10) and be responsible for procedures leading to resolution and enforcement. The Anti-Malware Primary Contact must ensure goodwill communication with partners having business-to-business contracts, Terms of Service, Site Level Agreements, or any business expectations.

DRAFT

4.6. Document Appropriate Points of Contact at Partner Companies

To achieve the Certified Against Malware Seal, any participating company must document appropriate points of contact for their partner or client companies. Any participating company placing ads on behalf of another company is responsible for any assets ingested into an ad placement by either company. To do this, any participating company must 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. Identifying key contacts at a company's supply chain partners allows rapid and precise escalation and notification.

Each covered party must document contacts for their partners as follows:

- Direct Buyers must document support contacts at scanning companies.
- Direct Sellers will document contacts at intermediary companies in the supply chain.
- Intermediaries will document points of contact with their partners in the supply chain.
- Vendors will document points of contact with client companies.

4.7. Document Malware Scanning Responsibilities in Any New or Updated Legal Agreements

To achieve the Certified Against Malware Seal, any participating company must document malware scanning responsibilities in new or updated legal agreements with partner companies. Such legal agreements may include, but are not limited to business-to-business contract language, Terms of Service, Site Level Agreements, publicly-available policies or other agreements in which a business expectation is set with a partner.

In such legal agreements, each company must employ technical and/or business process measures to prevent malware that are applicable, and feasible, for its position and role in the chain and proactively evaluate the trustworthiness of buy-side clients.

Depending on the covered party categories (see Section 3) into which a participating company falls, malware scanning responsibilities will vary as follows:

- Direct Buyers must document their responsibility to allow inventory to be scanned by a scanning company. Creatives to be delivered (not placeholders) must be scanned, and Direct Buyers must contract with their intermediary partners about appropriate malware scanning responsibilities.
- Direct Sellers must document responsibilities with their intermediary partners. Direct Sellers must also validate that their partners are scanning for malware by documenting what vendors they use.
- Intermediaries must document malware scanning responsibilities. Creatives to be delivered (not placeholders) must be scanned. Intermediaries must also have the capability to scan and shut off malicious demand sources upon request from sell-side partners.
- Vendors must specify responsibilities when handling creative and/or in media transactions. Vendors must indicate what script(s) could be appended to the creative and communicate to partners about their responsibility for scanning.
- Scanning companies must inform clients on recommended scanning frequencies in order for the service to operate effectively. Creatives to be delivered (not placeholders) must be scanned.

DRAFT

4.8. Scan Assets and Landing Page URLs Preceding Initial Delivery and Disclose Initial Scanning Methodologies to TAG

To achieve the Certified Against Malware Seal, any participating company must scan a reasonable percentage of the following prior to first delivery:

- Advertising campaign assets including physical files such as images and scripts associated with a campaign, with the exception of first-party generated, controlled and hosted assets; and
- Landing page click-through URLs, irrespective of hosting and creation of advertising campaign.

Initial scanning processes should follow industry best practices as specified in the *Technical Best Practices Against Malware*.

The best path to compliance with this requirement depends on the covered party categories (see Section 3.0) into which it falls and the way it employs scanning within its organization. A participating company may choose to rely on one or more vendor(s) and/or use proprietary, in-house technology for campaign asset and/or landing page URL scanning, but the company must be able to show that all of assets and landing page click-through URLs being handled are scanned for malware prior to first delivery.

When any participating company identifies a malicious ad experience on any asset or landing

page click through URL through an initial scan, that company must take action to identify, investigate and attempt to remediate and/or disable issues attributed to the scanned malicious ad experience.

Any participating company must also disclose to TAG the practices by which it complies with this requirement. Specifically, companies must disclose to TAG a total estimated percentage of campaign assets and landing page click-through URLs scanned (within +/- 5%) prior to initial delivery, a description of the methodolog(ies) used such scans, and the list of vendors used to execute such scans.

These disclosures must be made for each quarter of the calendar year. Disclosures must be updated quarterly to reflect any changes to a participating company's scanning practices from quarter to quarter. Exhibit A provides an example disclosure for a single quarter.

Exhibit A – Example: Initial Scanning Disclosures to TAG

Q2 2018	Total Percentage Scanned (+/- 5%) prior to First Delivery	Description of Scanning Methodolog(ies)	Vendors used (if applicable)
Advertising campaign assets, with the exception of first-party generated, controlled and hosted assets	%		
Landing page click-through URLs	%		

DRAFT

4.8.a. Exception for Direct Sellers

A company operating as a Direct Seller may request an exemption from this requirement in the event that it is able to verify and disclose to TAG that all of its partners handling campaign assets and/or landing page URLs associated with the Direct Seller currently hold the TAG Certified Against Malware Seal.

The granting of such an exemption to a company operating as a Direct Seller does not exempt that company from complying with this requirement when it operates as a Direct Buyer, Intermediary or Vendor.

4.9. Rescan Assets and Landing Page URLs and Disclose Rescanning Methodologies to TAG

To achieve the Certified Against Malware Seal, any participating company must rescan all of the following at a reasonable frequency:

- Active advertising campaign assets including physical files such as images and scripts associated with a campaign, with the exception of first-party generated, controlled and hosted assets; and
- Landing page click-through URLs, irrespective of hosting and creation of advertising campaign.

Rescanning is defined as scanning of any active campaign that has been scanned at least once,

either pre-flight or in-flight. Active campaigns are live campaigns and may or may not include asset changes.

Any active advertising campaign with a known campaign asset change must be rescanned before commencing delivery of the new campaign asset. A campaign with one or more asset change means that along the way, rotating creatives/image files or landing page URLs are swapped or changed up during the execution of an active campaign in a number of scenarios.

Rescanning procedures should follow industry best practices as specified in the *Technical Best Practices against Malware* document.

The best path to compliance with this requirement depends on the covered party categories (see Section 3.0) into which it falls and the way it employs scanning within its organization. A participating company may choose to rely on one or more vendor(s) and/or use proprietary, in-house technology for asset and/or landing page URL scanning.

When any participating company identifies a malicious ad experience on any asset or landing page click through URL through a re-scan, that company must take action to identify, investigate and attempt to remediate and/or disable issues attributed to the scanned malicious ad experience.

Any participating company must also disclose to TAG the practices by which it complies with this requirement. Specifically, companies must disclose to TAG a total estimated percentage of active advertising campaign assets and landing page click-through URLs rescanned (within +/- 5%); a description of the methodolog(ies) used in such rescans, and list of vendors used to execute such rescans, if applicable.

DRAFT

These disclosures must be made for each quarter of the calendar year. Disclosures must be updated quarterly to reflect any changes to a participating company's scanning practices from quarter to quarter. Exhibit B provides an example disclosure for a single quarter.

Exhibit B – Example: Rescanning Disclosures to TAG

Q2 2018	Total Percentage Rescanned (+/- 5%)	Description of Rescanning Methodolog(ies), including frequency of rescanning	Vendors used (if applicable)
Active advertising campaign assets, with the exception of first-party generated, controlled and hosted assets	%		
Landing page click-through URLs from active advertising campaigns	%		

4.9.a. Exception for Direct Sellers

A company operating as a Direct Seller may request an exemption from this requirement in the event that it is able to verify and disclose to TAG that all of its partners handling campaign assets

and/or landing page URLs associated with the Direct Seller currently hold the TAG Certified Against Malware Seal.

The granting of such an exemption to a company operating as a Direct Seller does not exempt that company from complying with this requirement when it operates as a Direct Buyer, Intermediary or Vendor.

4.10. Employ Internal Procedures for Defining Red Flag Events and Handling of Standard Malware Incidents

To achieve the Certified Against Malware Seal, any participating company must employ internal procedures for defining Red Flag events and handling of standard malware incidents.

TAG defines a Red Flag malware event as any event using the digital advertising supply chain as an attack vector 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 malware event

Red Flag response procedure may include investigation, action, and communication with appropriate staff. Red Flag event notification should be addressed immediately. These procedures must be employed to evaluate in an ongoing manner the technical and business risks of malware delivery from all sources and partners.

Any participating company must educate its employees and customers about malware prevention, including Red Flags to watch for and how to escalate concerns to appropriate persons within the organization, based on the definition and scope of a Red Flag Event.

Red Flag incidents may be communicated to upstream vendors or business partners without qualifying the incident as a Red Flag Event.

Participating companies must use communication with other companies in its determination of whether an incident is a Red Flag Event. A participating company's path to complying with this requirement may vary, depending on the covered party categories (see Section 3.0) into which it falls and its role in the digital advertising supply chain as follows:

- Direct Buyers will recognize Red Flag events based on the factors above relative to their business and user experience of creatives. Buyers can then communicate with scanning partners and industry resources to share information.
- Direct Sellers will recognize Red Flag events based on the factors above relative to their business and user experience of the web pages represented. Direct Sellers can communicate up and down transaction chain about the event, and also share information across the industry.
- Intermediaries will recognize Red Flag events based on the factors above relative to their business and user experience of the web pages represented. Intermediaries can communicate up and down transaction chain about the event, and also share information

DRAFT

across the industry.

- Vendors will recognize Red Flag events that occur on any creatives or landing pages that are associated with the client's inventory passed through the vendors technology or service. Vendor must act as a trustworthy partner to clients.

To achieve the Certified Against Malware Seal, scanning companies must employ procedures to warn clients of red flag events and respond to queries from clients.

4.11. Employ Seat ID Attributes to Troubleshoot and Handle Malware Incidents

To achieve the Certified Against Malware Seal, any participating company acting as a Direct Buyer, Direct Seller or Intermediary must employ Seat ID object attributes to troubleshoot and handle Red Flag events, as defined in Section 4.10. Additionally, any participating company acting as a Direct Seller or Intermediary must build or set up the capability to turn off Seat IDs or a company's direct partner to whom the Seat ID belongs, should a Red Flag event occur.

As stated within IAB Tech Lab's OpenRTB API specifications, a seat is defined as "an advertising entity (e.g., advertiser, agency) that wishes to obtain impressions and uses bidders to act on their behalf; a customer of a bidder and usually the owner of the advertising budget."[1] Seat ID attributes are defined for the bid response model as follows:

Object: SeatBid
A bid response can contain multiple SeatBid objects, each on behalf of a different bidder seat and each containing one or more individual bids.

Attribute	Type	Description
Seat	String	ID of the buyer seat (e.g., advertiser, agency) on whose behalf this bid is made.

DRAFT

A participating company's path to complying with this requirement will vary, depending on the covered party categories (see Section 3.0) into which it falls and its role in the digital advertising supply chain. As a minimum, companies must ensure that all programmatic buying disclosures fully comply with OpenRTB specifications v.2.2 or higher[2] and include the SeatBid object and Seat (ID) attribute information when making and honoring bid responses.

4.12. Establish Formal Post-Mortem Process for Red Flag Events

To achieve the Certified Against Malware Seal, any participating company acting as a Direct Buyer, Direct Seller or Intermediary must establish formal post-mortem processes for Red Flag events, as defined in Section 4.10.

A post-mortem is defined as a series of response procedures that occur 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.

[1] https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf

[2] http://www.iab.com/guidelines/real-time-bidding-rtb-project/

Companies must ensure that an internal post-mortem process is in place, which will examine Red Flag events. Such post-mortems should occur as promptly as possible after the investigation and resolution, recognizing that post-mortem processes may require time to research and refine as a company determines the scope for its post-mortem triggers.

A participating company's path to complying with this requirement may vary, depending on the covered party categories (see Section 3.0) into which it falls and its role in the digital advertising supply chain as follows:

- A Direct Buyer's post-mortem process may include tracking the source of a Red Flag Event, and adjusting creative implementations and anti-malware efforts as needed
- A Direct Seller or Intermediary's post-mortem process may include tracking the source of malware and improving anti-malware efforts accordingly.

4.13. Conduct Semi-Annual Reviews of Post-Mortems

To achieve the Certified Against Malware, any participating company acting as a Direct Buyer, Direct Seller or Intermediary must conduct semi-annual reviews of its post-mortems for Red Flag events, aligning these to the documented response strategy, and updating the response strategy as needed to account for resourcing and/or function growth/change.

DRAFT

5. Allegations of Non-Compliance & Appeal

Companies that achieve the Certified Against Malware Seal must meet and maintain compliance with the relevant requirements set forth in the *Certified Against Malware 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 Malware 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.

DRAFT