ANTI-MALWARE

CERTIFIED AGAINST **MALWARE**

Guidelines

Version 5.1

July 2024

ABOUT THE 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.

Since 2014, TAG (the Trustworthy Accountability Group) has partnered with industry leaders to design and strengthen the Certified Against Malware Program, providing companies with a roadmap for taking on the complicated issue of malvertising.

A survey of U.S. consumers conducted by the Brand Safety Institute (BSI) found that 93% of respondents would reduce their spending on an advertised product if the ad had infected their computers or mobile devices with malware – and 73% would stop buying that product altogether. The digital advertising industry has reacted to that consumer attention with greater vigilance and a strengthening of anti-malware practices, and **the number of companies holding the Certified Against Malware Seal grew by more than 44% in the past year alone,** making it TAG's fastest growing certification program.

ABOUT TAG

TAG 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 international TAG community include the world's largest and most influential brands, agencies, publishers, and ad tech providers.

TAG is the first and only Information Sharing and Analysis Organization (ISAO) for the digital advertising industry. This U.S. Department of Homeland Security designation means TAG is the primary forum for sharing threat intelligence in our industry.

TAG was created by the American Association of Advertising Agencies (4A's), Association of National Advertisers (ANA), and Interactive Advertising Bureau (IAB) and works collaboratively with companies throughout the digital ad supply chain.

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

EXECUTIVE **SUMMARY**

The dangers of malware are nearly as old as computers themselves, but the concept of malvertising is a relatively new one to businesses and consumers alike. While the term malware can mean malicious software of any sort delivered by any means, “malvertising” refers to the use of digital advertisements – including creative, tags and landing pages – specifically to distribute malware, often for financial gain.

Malvertising is now a problem at scale. Recent research suggests that despite improvements in the digital ad landscape, nearly 1 in every 100 ad impressions were still impacted by a malicious or disruptive ad, suggesting that more than 20% of user sessions may be impacted by malvertising. The financial impact of malvertising has grown apace as well. In 2018, it was estimated that the industry lost $210 million annually to auto-redirects, and another $920 million from the ads auto-redirects facilitated with click fraud.

TAG coordinates an industry-wide effort to improve defense against malware to create a safer, more enjoyable experience for consumers and a more trustworthy system for advertisers. In 2017, TAG became the Information Sharing and Analysis Organization (ISAO) for the digital advertising industry, a Department of Homeland Security designation making TAG the primary forum for sharing threat intelligence in our industry.

Since 2014, the Trustworthy Accountability Group (TAG) has partnered with industry leaders to design and strengthen the Certified Against Malware Program, providing companies with a roadmap for taking on the complicated issue of malvertising. The Anti-Malware Working Group coordinates industry-wide efforts, including maintaining and updating the *Certified Against Malware Guidelines*, to improve defense against malvertising attacks to create a safer, more enjoyable experience for consumers and a more trustworthy system for advertisers.

1.1 DEFINING MALWARE AND MALVERTISING

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.

While the term malware can mean malicious software of any sort delivered by any means, “malvertising”, as defined in TAG’s *Malvertising Taxonomy,* refers to the “exploitation of digital advertisements to enable bad actors to spread malware and circumvent systems in a way that harms end users, publishers, and platforms.” [1]

[1] https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy

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 to begin the process for their company to achieve the Certified Against Malware Seal. To participate in the Certified Against Malware Program, the company's TAG membership must include access to that program.

2.1.a Participation Fee

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

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 Malware Seal.

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.

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 how 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*.

A company has the option to choose self-attestation except in cases noted in *TAG's Due Process for Allegations of Non-Compliance and Appeal*, available on .

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 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.

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 and renew their compliance annually..

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).

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 for the company to achieve the Certified Against Malware Seal. Training must be renewed every 12 months in order for a company to maintain its Certified Against Malware Seal from year to year.

TAG provides training through online streaming video available through the TAG Member Portal, so that TAG Compliance Officers are able to obtain training regardless of geographic location or time-zone. TAG Compliance Officers can learn more by emailing info@tagtoday.net.

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.

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 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.

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

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.

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

Vendors are responsible for providing anti-malware services, e.g. anti-malware scanning. These companies are also able to provide reporting and insights on malware threats. Vendors do not transact inventory, but, depending on their techniques and solutions, they could append creative payloads. This includes any company that is dropping script into the creative or on the page itself.

CERTIFICATION
REQUIREMENT

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	✓	✓	✓	✓
Define and Identify Key Roles and Resources	Anti-Malware	✓	✓	✓	✓
Define Escalation Process	Anti-Malware	✓	✓	✓	✓
Employ Effective Malvertising Detection and Removal Services	Anti-Malware			✓	
Provide Effective Malvertising Detection and Removal Services	Anti-Malware			✓	✓
Review Monitoring, Reporting and Post-mortem Processes Semi-annually	Anti-Malware			✓	✓
Define Post-Mortem Processes	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.

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

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 for the company to achieve the Certified Against Malware Seal. Training must be renewed on an annual basis 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 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 DEFINE AND IDENTIFY KEY ROLES AND RESOURCES

To achieve the Certified Against Malware Seal, any participating company acting as a Buyer, Seller, Vendor or Intermediary must define and identify to TAG the resources/groups responsible for the detection, analysis and response to malvertising events on behalf of the company and share documentation, such as Vendor Terms of Service, and/or Service Level Agreements, email chains, or business expectations in place that demonstrate compliance with this requirement.

Companies must identify, designate, and document the responsible resource(s) on behalf of their partners as indicated below for each of their partner or client companies:

- 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.

- 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 all three functions.

4.6. DEFINE ESCALATION PROCESS

To achieve the Certified Against Malware Seal, any participating company acting as a Buyer, Seller, Vendor, or Intermediary must define and document to TAG their process for assessing malvertising events and determining whether an event is an incident as well as a process for escalating malvertising incidents within their companies and with their partners to enable appropriate and timely resolution. A company's Escalation Process must include steps for timely communication of malvertising events to its documented anti-malvertising resources as listed in Section 4.5 with appropriate and affected partners and vendors.

While not all malvertising incidents require immediate and timely escalation, each participating company must document, as a minimum, the appropriate process in place to assess incidents requiring escalation and define escalation procedures for malvertising incidents that reach a level of significance dependent on the following factors, relative to each company:

- Significant revenue impact
- Negative or detrimental consumer experience
- Involving highly publicized, typically known industry-wide threat(s) or bad actor(s)
- High degree of sophistication

Vendors must also employ procedures to warn their clients of significant malvertising events and/or incidents and respond to queries from them.

4.6.a. Use of TAG Malvertising Taxonomy

TAG's *Malvertising Taxonomy*[2] is available to assist companies in communicating malvertising incidents to their partners. This tool was created to provide detailed and consistent terminology and standardize the definition of malvertising to foster transparency and collaboration in the fight against malvertising.

While the goal of the *Malvertising Taxonomy* is to provide sufficient granularity in terminology to help partners in the digital advertising supply chain troubleshoot and escalate appropriate issues, this tool is intended to be employed in addition to operations that companies employ internally or through third-party vendors to assess and escalate events identified within the Taxonomy that reach a level of significance as defined in Section 3.3. While the *Malvertising Taxonomy* is a powerful tool aggregated from malvertising vendors and intermediaries 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 malvertising vendor.

4.7. EMPLOY EFFECTIVE MALVERTISING DETECTION AND REMOVAL SERVICES

To achieve the Certified Against Malware Seal, any company participating as an Intermediary must employ effective malvertising detection and removal services across all their advertising assets and landing pages prior to and throughout the duration of a campaign execution. Advertising campaign assets include physical files such as images and scripts associated with a campaign, with the exception of first party generated, controlled and hosted assets. Landing

[2] https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy

page click-through URLs must also be reviewed, irrespective of hosting and creation of advertising campaign.

- If an Intermediary uses proprietary, in-house technology to employ malvertising detection and removal, that company must be certified that its service capabilities meet all of the elements within the Core Criteria as listed in Section 4.8, AND/OR
- If an Intermediary relies on one or more third-party vendor(s) for malvertising detection and removal services, that company must ensure that the relevant third-party vendor(s) certify that their service capabilities meet all of the elements within the Core Criteria as listed in Section 4.8.

Intermediaries must disclose to TAG:

- That they are employing effective malvertising detection and removal across all of the digital advertising campaign assets that then control, serve and/or track.
- The vendor or vendor(s) used for effective malvertising detection and removal.
- The methodology(ies) the company uses to allocate effective malvertising detection and removal when rescanning digital advertising campaign assets.

Intermediaries must also have the capability to report accurate and timely indicators of compromise and/or parameters involved in detecting the source of malvertising to their Vendors and/or partners upon request. TAG's *Malvertising Taxonomy*[3] is available, but is not required to assist companies in streamlining such reporting and communication, both internally and with partners.

4.8. PROVIDE EFFECTIVE MALVERTISING DETECTION AND REMOVAL SERVICES

To achieve the Certified Against Malware Seal, any company participating as a Vendor or an Intermediary who chooses to employ their own technology(ies) to detect/filter malvertising must demonstrate that they are able to provide effective malvertising detection and removal services across advertising assets and landing pages prior to and throughout the duration of a campaign execution for which the company is responsible.. Advertising campaign assets include physical files such as images and scripts associated with a campaign, with the exception of first party generated, controlled and hosted assets. Landing page click-through URLs must also be reviewed, irrespective of hosting and creation of advertising campaign.

Companies may utilize one or more technique(s) to build an effective detection and removal process including, but not limited to:

- Scanning of campaign assets and landing pages, including initial and rescanning (during the lifecycle of a campaign)
- Real-time detection based on blocklists, code analysis or third-party verification knowledge repositories
- Run-time behavioral analysis

All Vendors and Intermediaries who employ their own technology(ies) to detect/filter malvertising must offer technologies, methodologies or services that meet all four criteria for effective malvertising detection and removal as defined below:

[3] https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy

1. Malvertising detection and removal services must have tools to assess and identify malvertising techniques/tactics such as those defined in Section 3.3 of TAG's *Malvertising Taxonomy.*

2. Malvertising detection and removal services must include protocols and capabilities to detect, prevent, or disrupt advertising campaigns that show evidence of malvertising events, such as those defined in Section 3.3 of TAG's *Malvertising Taxonomy*.

3. Malvertising detection and removal services must have the protocols and capabilities to monitor and report malvertising events, such as those defined in Section 3.3 of TAG's *Malvertising Taxonomy*, thus enabling partners and/or clients to implement remedial action.

4. Malvertising detection and removal services must be able to identify and provide relevant indicators of compromise and/or parameters involved in detecting the source of malvertising when reporting malvertising events to partners and/or clients. *Malvertising Taxonomy*[4] is available to assist companies, but is not required in meeting this requirement.

5. Malvertising detection and removal services must periodically assess (at least annually) their service offerings to determine whether their capabilities require changes to malvertising detection and removal techniques, approaches and analyses to account for new or evolving malvertising threats. Such services must retain evidence and results (such as meeting minutes, desk review documentation, related data analyses, legal review input, etc.) for audit purposes related to the consideration and inclusion of new and/or evolving malvertising threats within required periodic risk assessments. If material impairments to capabilities arise, those services must research the impact and generally disclose those limitations to users, as well as actively research alternative approaches to comply where possible. TAG's *Malvertising Taxonomy*[5] is available to assist companies, but is not required in meeting this requirement.

Vendors and Intermediaries who employ their own technology(ies) to detect/filter malvertising must disclose to TAG how it complies with each criterion for effective malvertising detection and removal. Disclosures must include descriptions of the methodology(ies) used to comply with each criterion and used to execute such services. Please note that Intermediaries who rely solely on third party vendors and/or services are not expected to comply with this requirement.

4.9 REVIEW MONITORING, REPORTING AND POST-MORTEM PROCESSES SEMI-ANNUALLY

To achieve the Certified Against Malware Seal, any participating company acting as a Vendor or Intermediary must conduct semi-annual reviews of its monitoring, reporting and post-mortem processes. These reviews must align to the documented response strategy, and the response strategy updated as needed to account for resourcing and/or function growth/change.

4.10 DEFINE POST-MORTEM PROCESSES

To achieve the Certified Against Malware Seal, any participating company acting as a Buyer, Vendor or Intermediary must establish formal post-mortem processes for qualifying malvertising incidents affecting their company. While not all malvertising incidents require extensive post-mortem investigation, each participating company must document, as a minimum, the appropriate post-mortem processes in place for malvertising incidents that reach a level of significance dependent on the following factors, relative to each company:

- Significant revenue impact

[4] https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy

[5] https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy

- Negative or detrimental consumer experience
- Involving highly publicized, typically known industry-wide threat(s) or bad actor(s)
- High degree of sophistication

A post-mortem is defined as a process used to identify the cause of the incident that occurs after the identification and resolution of a malvertising incident, to effectively share knowledge of the event. Post-mortems will produce feedback into learning and improving anti-malvertising policy and procedure.

Companies must ensure that an internal post-mortem process is in place, which will examine reported malvertising incidents.

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 malvertising event and adjusting creative implementations and anti-malvertising efforts as needed.
- An Intermediary's post-mortem process may include tracking the source of malvertising and improving anti-malware efforts accordingly.

A vendor's post-mortem process may include tracking indicators and signs of malvertising and improving malvertising notifications accordingly.

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.

tagtoday.net