TAG Certified Against Piracy Guidelines

Version 2.0
Released January 2018

About the TAG Certified Against Piracy Program

The mission of the TAG Certified Against Piracy Program is to help advertisers and agencies avoid damage to their brands from ad placement on websites and other media properties that facilitate the distribution of pirated content and counterfeit products. This voluntary initiative helps marketers identify sites that present an unacceptable risk of misappropriating copyrighted content and sell counterfeit goods, and it will help them remove those sites from their advertising distribution chain.

In order to guide companies in combatting ad-supported effectively, the TAG Anti-Piracy Working Group developed and maintains the Certified Against Piracy Guidelines – including *Core Criteria for Effective Digital Advertising Assurance* – as well as a suite of anti-piracy tools to aid in compliance with those guidelines.

Companies that are shown to abide by the Certified Against Piracy Guidelines can achieve the Certified Against Piracy Seal and use the seal to publicly communicate their commitment to combatting ad-supported piracy in the digital advertising supply chain.

About the Trustworthy Accountability Group

The Trustworthy Accountability Group (TAG) is the leading global certification program fighting criminal activity and increasing trust in the digital advertising industry. Created by the industry's top trade organizations, TAG's mission is to:

- Eliminate fraudulent traffic,
- Combat malware,
- Prevent Internet piracy, and
- Promote greater transparency in digital advertising.

TAG advances those initiatives by bringing companies across the digital advertising supply chain together to set the highest standards.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

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

Table of Contents

1. Executive Summary

Advertisers want to protect their brands from damage that comes from association with illegal activity. Online advertisers face risks from sites that infringe on the rights of others by facilitating the distribution of pirated content and counterfeit products. Consumers may mistakenly believe that the sites' offerings are authorized by well-known brands. Such misplaced advertising also harms content creators and legitimate content distributors by providing economic resources that fuel these illegal enterprises and putting enormous profits into their coffers. Many of these sites also use fraud or deceptive practices to avoid the standards set by the advertiser or its agency, driving revenue to those who steal copyrighted content or otherwise violate others' trademarks.

TAG launched its Certified Against Piracy Program in 2015 to help advertisers and ad agencies avoid damage to their brands from ad placement on websites and other media properties that facilitate the distribution of pirated content and counterfeit products. This voluntary initiative helps marketers identify sites that present an unacceptable risk of misappropriating copyrighted content and selling counterfeit goods, and remove those sites from their advertising distribution chain. The program was supported at launch by leading organizations and companies in digital advertising, online publishing, media and consumer protection.

Research commissioned by TAG and undertaken by Ernst & Young LLP in 2017 showed the impact of industry efforts to reduce ad-supported content piracy.[1] The study found that anti-piracy steps taken by the digital advertising industry have reduced ad revenue for pirate sites by between 48 and 61 percent, notable progress against the $2.4 billion problem of infringing content measured by Ernst & Young in 2015.[2]

[1] Ernst & Young LLP. (September 2017). *Measuring Digital Advertising Revenue to Infringing Sites: TAG US Benchmarking Study*. Retrieved from https://www.tagtoday.net/piracy/measuringdigitaladrevenuetoinfringingsites
[2] Ernst & Young LLP. (November 2015). *What is an Untrustworthy Supply Chain Costing the US Digital Advertising Industry: IAB US Benchmarking Study*. Retrieved from https://www.iab.com/wp-content/uploads/2015/11/IAB_EY_Report.pdf

2. Certification Process

The TAG Certified Against Piracy Program is voluntary and represents the ongoing process of defining and maintaining guidelines for effectively fighting ad-supported Internet piracy to promote brand integrity in the digital advertising supply chain.

TAG certifies companies at the entity level, rather than certifying a specific product or business line within a legal entity. To achieve the TAG Certified Against Piracy Seal, companies must show that all of its material operations related to ad monetization services within a particular geographic market are in compliance with the relevant requirements of the Certified Against Piracy Guidelines.

2.1. Application

Before a company can apply for the Certified Against Piracy Seal, that company must first become a TAG member, completing the process of becoming "TAG Registered" and enrolling in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG directly 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 Piracy Program in order to begin the process for that company to achieve the Certified Against Piracy Seal. In order to participate in the Certified Against Piracy Program, a company's TAG membership must include access to that program.

2.1.a. Participation Fee

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

2.2. Qualification

Any TAG member company in good standing that has been enrolled in the Verified by TAG Program and whose TAG membership includes participation in the Certified Against Piracy Program can participate in the Certified Against Piracy Program and apply for the Certified Against Piracy Seal.

Requirements to achieve the TAG Certified Against Piracy 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 Piracy Seal can be achieved in any geographic market. However, upon achieving certification, a company is only permitted to use the Certified Against Piracy Seal in the specific geographic markets in which TAG has found the company's operations to be in full compliance with the Certified Against Piracy 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 Piracy 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 Piracy 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 Piracy Seal solely in that market.

2.4 Methods of Certification

Companies can apply to achieve the Certified Against Piracy Seal using one of two methods: self-attestation and independent validation. A company has the option to choose either method, except in cases noted in Section 5 of this document. The selected method is recorded and displayed on the TAG website.

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 Piracy Guidelines and that it will maintain compliance throughout the certification period.

Certification through independent validation is obtained by the company inviting one of TAG's authorized independent third-party validators to review and validate that the company has achieved full compliance with the Certified Against Piracy Guidelines, and the company attesting that it will maintain compliance throughout the certification period. The full list of TAG Validators can be obtained by contacting TAG directly.

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 Piracy Seal through a self-attestation can move to an independent validation certification at any time by providing the additional paperwork and reports required from the independent auditor.

2.4.a. Certification Through Self-Attestation

Certification through self-attestation is obtained through a series of attestations from the company that it is complying with the Certified Against Piracy Guidelines.

Entities that wish to achieve the TAG Certified Against Piracy Seal through self-attestation should submit to TAG a completed Certified Against Piracy 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 Piracy 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 one of TAG's authorized independent third-party Validators to validate that the company is compliant with the Certified Against Piracy Guidelines. The full list of TAG Validators can be obtained by contacting TAG directly.

While independent validation is designed to provide limited assurance, ensuring that all Certified Against Piracy 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 Piracy Guidelines.
- Policies and procedures related to complaint handling/resolution to ensure compliance with the Certified Against Piracy Guidelines.
- Testing performed by the company as part of the internal quarterly review process.

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

- Compliance Officer and Executive Attestations
- Independent Validation Attestation
- Quarterly audit report

2.5 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 Piracy 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 materials to the company's designated TAG Compliance Officer for use in promoting the company's Certified Against Piracy status.

2.5.a. Certified Against Piracy Seal

Companies that are shown to meet the Certified Against Piracy Guidelines receive the Certified Against Piracy Seal and can use the seal to publicly communicate their commitment to fighting ad-supported Internet piracy to promote brand integrity in the digital advertising supply chain.

2.6. Continued Compliance

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

2.6.a. TAG Compliance Officer

Companies participating in the Certified Against Piracy 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 Piracy Program.

The duties of a TAG Compliance Officer include:

- Serving as the primary point of contact between TAG and the company regarding all aspects of the company's TAG membership. This includes receipt of notice concerning any changes to TAG Certification program(s).
- Completing the required training modules for each TAG Certification program in which the company participates.
- Educating internal teams on the requirements of each TAG Certification program in which the company participates, and notifying those internal teams of any changes.
- Overseeing the company's processes related to compliance with the requirements of each TAG Certification program in which the company participates.
- Facilitating internal review of the company's compliance with the requirements of each TAG certification program in which the company participates, including independent auditor review where appropriate.
- Taking on additional responsibilities applicable to each of the TAG programs in which the company participates (as appropriate).

The minimum qualifications for a TAG Compliance Officer include:

- Reporting relationships whereby compliance assessments are not influenced or biased by operations personnel being tested for compliance.
- Adequate technical training and proficiency in testing and assessing compliance.
- Adequate knowledge of the subject matter covered in each of the TAG Certification programs in which the company participates (i.e., advertising technology, various functions within the digital advertising supply chain, etc.).
- Adequate independence within the company to avoid conflicts of interest with regard to assessing compliance with TAG program requirements.

A TAG Compliance Officer does not need to hold a particular title or job description within the organization, as long as that individual has independence from sales and marketing functions.

The role of the TAG Compliance Officer is further described in the TAG Compliance Officer Role Description on the TAG website.

2.6.b. Compliance Team

While the only required requirement to support compliance with the Certified Against Piracy 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 Piracy Guidelines.

2.6.c. Training

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

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

- The Certified Against Piracy Guidelines are consistently and completely followed.
- Control activities discussed during Certified Against Piracy 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 Piracy Seal must be recertified annually. Companies that achieve the Certified Against Piracy Seal must apply for recertification by January 30 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 been recertified by March 1.

3. Covered Parties

The Certified Against Piracy Program is applicable to three types of entities across the digital advertising supply chain:

- Direct Buyers,
- Digital Advertising Assurance Providers (DAAPs), and
- Publishers.

Companies applying for the Certified Against Piracy Seal must apply for the Seal under all relevant covered party categories, meeting the requirements relevant to each category, as described in Section 4.

3.1. Direct Buyer

Direct Buyers are advertisers who own advertisements for placement in inventory on the publisher's websites or other media properties, or advertising agencies that directly 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. To qualify as a Direct Buyer, the agency must directly represent the advertiser.

3.2. Digital Advertising Assurance Provider (DAAP)

Digital Advertising Assurance Providers (DAAPs) are companies that offer, subject to the validation or attestation processes outlined below, technologies, methodologies, or services that, consistent with the advertiser's instructions, that effectively:

(1) assess which entities are identified as At-Risk Entities (AREs); and/or
(2) assist entities in the advertising ecosystem to prevent undesired placement of advertisements on such AREs; and/or
(3) identify and eliminate payment for online advertisements on such AREs.

3.2.a. Self-Attested DAAP

Self-Attested DAAPs are ad tech companies that use their own proprietary technology to provide other digital advertising companies with anti-piracy services that limit advertising on websites or other media properties that have a discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods. Such services are provided by Self-Attested DAAPs only on their own platforms using their own proprietary technology.

3.2.b. Validated DAAP

Validated DAAPs are anti-piracy vendors that specialize in providing other digital advertising companies with anti-piracy services to limit advertising on websites or other media properties that have a discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods. Such services are provided using the Validated DAAP's own proprietary technology and are sold to their clients.

3.3. Publisher

A publisher is a publishing company that provides content to an audience through website or other media properties. Publishers sell ad space inventory on their websites or other media properties that offer value to advertisers depending on the size and demographics of the audience.

Publishers may be categorized by the content sources used on their media properties in the following ways.

3.3.a. Category 1 Publisher

A publisher using only first-party content that the publisher owns on its websites or other media properties.

3.3.b. Category 2 Publisher

A publisher using licensed content alone or in combination with first-party content that the publisher owns on its websites or other media properties.

3.3.c. Category 3 Publisher

A publisher using user-generated content (UGC) alone or in combination with licensed content and/or first-party content that the publisher owns on its websites or other media properties.

4. Certification Requirements

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

To achieve the Certified Against Piracy Seal, a company must meet the requirements for all the categories in which it operates, according to the table below.

4.1. Requirements Table

	Scope	Direct Buyer	DAAP	Publisher		
				Category 1	Category 2	Category 3
Complete TAG Registration and be a TAG Member in Good Standing	Administrative	✓	✓	✓	✓	✓
Have a designated TAG compliance officer in good standing	Administrative	✓	✓	✓	✓	✓
Attend Certified Against Piracy Training Annually	Administrative	✓	✓	✓	✓	✓
Comply with the TAG Anti-Piracy Pledge	Anti-Piracy	✓				
Comply with at least one of the Core Criteria for Effective Digital Advertising Assurance	Anti-Piracy		✓			
Employ Pirate Mobile App Filtering	Anti-Piracy	✓	✓			
Attest to owning the rights to all content on owned and/or operated media properties	Anti-Piracy			✓		
Attest to owning or licensing the rights to all content on owned and/or operated media properties	Anti-Piracy				✓	
Employ commercially available means to ensure that owned and/or operated media properties do not host nor stream infringing content	Anti-Piracy					✓
Ensure that owned and/or operated media properties do not block or unduly restrict or disrupt the use of anti-piracy software	Anti-Piracy			✓	✓	✓

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

To achieve the Certified Against Piracy Seal, any participating company must first become a TAG member, completing the process of becoming "TAG Registered" and enrolling in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG directly or visiting www.tagtoday.net.

Companies seeking the Certified Against Piracy Seal must also have active TAG memberships that include participation in the Certified Against Piracy 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 in Good Standing

To achieve the Certified Against Piracy Seal, any participating company must have designated a qualified TAG Compliance Officer.

The role of the TAG Compliance Officer is described in section 2.6.a of this document.

4.4. Attend a Certified Against Piracy Training Annually

In order to achieve the Certified Against Piracy Seal, the designated TAG Compliance Officer at any participating company must, at least once in a 12-month period, attend a Certified Against Piracy training.

TAG provides training on a regular basis via a virtual platform so that TAG Compliance Officers are able to obtain training regardless of geographic location. TAG Compliance Officers can learn more and RSVP for training sessions by visiting www.tagtoday.net.

4.5. Comply with the TAG Anti-Piracy Pledge

In order to achieve the Certified Against Piracy Seal, Direct Buyers must operationalize and comply with the TAG Anti-Piracy Pledge.

The TAG Anti-Piracy Pledge represents advertisers and agencies (i.e., Direct Buyers) commitment to take commercially reasonable steps to minimize the inadvertent placement of digital advertising on websites or other media properties that have an undesired risk of being associated with the unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods.

The pledge should be fulfilled in a manner consistent with the Core Criteria for Effective Digital Advertising Assurance, which may include:

(i) directly employing the services of validated Digital Advertising Assurance Providers;
(ii) directly employing advertising placement services that carry the TAG Certified Against Piracy logo; and/or

(iii) placing online advertisements through Advertising Agencies that do business exclusively with advertising placement services that carry the TAG Certified Against Piracy logo.

TAG, as well as Direct Buyers taking the pledge, recognize that, despite these efforts, some digital advertising may nonetheless appear on such websites or other digital properties. In undertaking this pledge, Direct Buyers do not create legal liability for any such inadvertent advertising.

4.6. Comply with at least one of the five Core Criteria for Effective Digital Advertising Assurance

In order to achieve the Certified Against Piracy Seal, Self-Attested DAAPs and Validated DAAPs must meet all of the elements in one or more of the five *Core Criteria for Effective Digital Advertising Assurance*.

4.6.a. Criterion #1: Identify At-Risk Entities (ARE).

As defined in the *Core Criteria for Effective Digital Advertising Assurance*, an Ad Risk Entity (ARE) is a website or other media property that has a discernible risk of being associated with unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods.

- A DAAP should assess whether entities are AREs;
- A DAAP should provide tools to help advertisers and/or their agencies decide the extent to which they wish to limit or restrict the display of their advertisements on entities deemed to be AREs in (IV)(1)(a); and
- A DAAP should have an objective review and evaluation process for claims from entities of erroneous designation or scoring or determination of those entities as AREs in (IV)(1)(a).

4.6.b. Criterion #2: Prevent Advertisements on Undesired AREs.

- A DAAP should restrict or enable the restriction of the display of advertisements on undesired AREs in accordance with the direction of an advertiser and/or its agency as set forth in (IV)(1)(b) ("Undesired AREs"); and
- A DAAP should provide or enable the provision of real-time solutions as a means to effectively prevent advertisements on Undesired AREs.

4.6.c. Criterion #3: Detect, Prevent, or Disrupt Fraudulent or Deceptive Transactions.

- A DAAP should have protocols and capabilities to detect, prevent, or disrupt advertising placements on Undesired AREs that are transacted fraudulently or deceptively (*e.g.*, through the use of intermediary sites or other means to disguise the ARE's identity or purpose);

- In the event that a DAAP identities the use of intermediary sites or other means as set forth in (IV) (5)(a), a DAAP should have protocols and capabilities to prevent further advertisement exposure through such means; and
- A DAAP should have an objective review and evaluation process for claims from entities of erroneous determination of fraudulent or deceptive transactions in (IV)(5)(a).

4.6.d. Criterion #4: Monitor and Assess for Advertisement Placement Compliance.

- A DAAP should detect and report on advertisements on AREs that may not be in compliance with advertiser/agency instructions, thus enabling advertisers and agencies to implement remedial action.

4.6.e. Criterion #5: Eliminate Payments to Undesired AREs. Elements:

- A DAAP should have technology and protocols in place that prevent or enable the prevention of payments resulting from advertisements displayed on Undesired AREs; and
- In the event payment has been made to Undesired AREs, a DAAP should have technology and protocols in place that enable the reversal or reclamation of such payment.

4.7. Employ Pirate Mobile App Filtering

To achieve the Certified Against Piracy Seal, Direct Buyers, Self-Attested DAAPs and Validated DAAPs must employ pirate mobile app filtering for all advertising displayed in a mobile app environment.

Pirate Mobile App filtering is the practice of filtering out mobile apps that were removed from App Stores for infringing on protected intellectual property rights in order to stem the flow of ad revenue to mobile apps with pirated content.

Pirate Mobile App filtering is accomplished by developing or subscribing to a list of pirate mobile apps that were removed from App Stores for infringing on protected intellectual property rights and applying this list to current and future transactions.

4.7.a. Use of TAG Pirate Mobile App List

The TAG Pirate Mobile App List is available to assist companies in meeting this requirement, but use of the tool is not required.

The TAG Pirate Mobile App List is a common list of mobile apps that were removed from App Stores for infringing on protected intellectual property rights. The full process for utilizing the list is outlined in the *TAG Compliance Standard for the Pirate Mobile App List*.

4.8. Attest to Owning the Rights to all Content on Owned and/or Operated Media Properties

In order to achieve the Certified Against Piracy Seal, Category 1 Publishers must provide TAG with an attestation on company letterhead from a Business Executive that they own the rights to all content appearing on their owned and/or operated media properties.

4.9. Attest to Owning or Licensing the Rights to all Content on Owned and/or Operated Media Properties

In order to achieve the Certified Against Piracy Seal, Category 2 Publishers must provide TAG with an attestation on company letterhead from a Business Executive that they own or have licensed the rights to all content appearing on their owned and/or operated media properties.

4.10. Employ Commercially Available Means to Ensure that Owned and/or Operated Media Properties do not Host Nor Stream Infringing Content

In order to achieve the Certified Against Piracy Seal, Category 3 Publishers must show that they employ commercially available means to ensure that their owned and/or operated media properties do not host nor stream infringing content.

4.11. Ensure that Owned and/or Operated Media Properties do not Block Nor Unduly Restrict or Disrupt the Use of Anti-Piracy Software

In order to achieve the Certified Against Piracy Seal, Publishers – including Category 1, Category 2 and Category 3 Publishers – must show that their owned and/or operated media properties do not block nor unduly restrict or disrupt the use of anti-piracy software.

5. Allegations of Non-Compliance & Appeal

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