

Vendor Dispute and False Positive Resolution Process

Anti-Spyware vendors are often approached by software publishers alleging that their programs have been unfairly flagged as "spyware." This document provides an overview of generally accepted practices for processing and resolving such disputes. The document is meant as a common, transparent set of best practices that anti-spyware vendor practices may exceed. To be clear: vendor dispute processes are run by individual anti-spyware companies or software publishers. The Anti-Spyware Coalition neither runs such a process independently nor acts as a party in them.

Publisher Disputes/False Positive Claims

1. Process Overview

a. Submission

- A software publisher may wish to initiate a review if it believes that a program or associated files have been incorrectly classified by a particular anti-spyware vendor, or it has recently updated the behavior of its program and believes it should no longer be classified as spyware.
- To initiate the review, the software publisher visits the Web site for the anti-spyware vendor and submits a designated form. Alternatively, if the anti-spyware publisher does not have a Web form, the software publisher can send an email or postal inquiry to a designated email or postal address.
- The Software publisher must supply all required information in order to request review by the anti-spyware vendor.
- The anti-spyware vendor will acknowledge receipt of the disputing publisher's request.

Note: Anti-spyware vendors may handle queries submitted by third parties and end users (not the software publisher) using a separate process or channel.

- During the dispute resolution process, the anti-spyware vendor may request additional information such as:
 - A copy of the current version or versions of the software;
 - Information about all substantial means by which the software is distributed, potentially including specific information about one or more affiliates or distributors;
 - A listing of specific distribution requirements placed on affiliates or distributors, ways in which the requirements are enforced, and any known deviations from them;
 - Known ways in which the behavior of any submitted software can be changed from its default behavior;
 - Ways in which any submitted versions differ from other versions including descriptions of how the behavior of the software has changed and how the underlying files can be distinguished;
 - The version of the anti-spyware software and signature file that the dispute concerns;

- Any additional information the anti-spyware vendor believes is relevant to its analysis.

This information will typically be requested either as part of the publisher dispute form or in a follow-up e-mail. In order for the review to continue, the software publisher must respond to these queries.

- If a disputing publisher fails to provide required information to the anti-spyware vendor, the case may be closed by the anti-spyware vendor. If a case is closed the software publisher must resubmit a vendor dispute form or send a new email (including all required information) to activate a new dispute.
- The anti-spyware vendor may decide to have the entire dispute resolution process handled by an independent third-party chosen by the vendor.

b. Analysis and Response: The anti-spyware vendor will acknowledge, in writing, upon receipt of the complaint and start the dispute resolution process.

- The anti-spyware vendor will attempt to fairly and accurately recreate the user experience and compare the behavior of the product against the anti-spyware vendor's current analysis criteria. Data collection for researching an application includes screen shots, video captures, log files, characteristics of the application analyzed, the signature criteria, and the detection technology.
- If the application meets the anti-spyware vendor's criteria for detection, detection may persist. The software publisher will be notified at this point in writing with a general indication of the criteria that were matched.
- If the application does not meet a sufficient amount of criteria, the anti-spyware vendor may choose to remove detection of the software from the signature library or change the way the product is described. The software publisher will be notified in writing of the results in a timely manner. The notice will include information on a timeframe to implement the decision. Other versions of the same software may continue to be detected so long as they still meet a sufficient amount of the anti-spyware vendor's criteria for detection. In the case of a clear false positive, the anti-spyware vendor may contact the software vendor via e-mail to confirm the issue and discuss next steps for resolution.
- The anti-spyware vendor will respond to all complaints within a reasonable timeframe. Response time is dependant on several factors including, but not limited to:
 - The potential impact on users of ceasing detection
 - The technical demands of analysis
 - The completeness of the information provided
 - The complexity of a particular case.
- In communicating the dispute decision to the disputing software publisher, the anti-spyware vendor will state to the software publisher that decisions are subject to change if alterations are made to the program over time or as classification criteria and/or detection technology employed by the anti-spyware program changes over time to address the evolving landscape.

c. Resubmission

- A software publisher may choose to resubmit its program for reconsideration if it has implemented updates that change a program behavior sufficiently that it reasonably believes address the anti-spyware publisher's concerns.
- Anti-spyware vendors may establish limits to the number of times a program is submitted for review. These requirements can be time-bound by a reasonable waiting period and/or activity bound (e.g. only when the software vendor's program changes).
- In general, it is not the responsibility of anti-spyware vendors to enter into ongoing relationships with adware makers or other software publishers in order to assist them in revising their software and business practices. Anti-spyware vendors may choose to give advice, but should not be expected to serve as free consultants, to police software distribution networks, or to provide a general vetting service for software development.

2. Suggested best practices

- **Publishing overview of criteria:** Anti-spyware vendors should publish an overview of their analysis approach and criteria to give software publishers and users a better understanding of how programs will be reviewed. It is not necessary, however, to disclose detail or point-by-point review analysis.
- **Published process for resolving disputes:** Anti-spyware vendors should publish their process for resolving disputed detections. This should include how a software publisher can submit a dispute and what it can expect throughout the process and the policy on resubmission.
- **Electronic submission of vendor disputes:** Anti-spyware vendors should provide an easy means for software publishers to contest detection/classification in the signature library. A publisher dispute form provides software publishers with an understanding of how to get the process started. It should be available through the Internet and should clearly indicate the information needed from the software publisher to start the analysis.
- **Documented publisher dispute process:** Anti-spyware vendors should keep appropriate records of publisher disputes received, as well as documentation for the analysis conducted and support for the conclusion. The anti-spyware vendor should provide appropriate documentation on its conclusions to the software publisher.
- **Communications in writing:** Communications between the software publisher and the anti-spyware vendor should generally be in writing. This provides a documented record of interactions and reduces the potential for misunderstandings.
- **Setting expectations:** Regardless of whether the review was in favor of the software publisher or not, the anti-spyware vendor should highlight to the software publisher that decisions are subject to change if alterations are made to the disputed programs over time or as the signature criteria and/or detection technology employed by the anti-spyware program changes over time to address the evolving landscape. However, see note above about the reasonable expectations of the role of anti-spyware companies in ongoing review.