Dangers of Submitting Incomplete or Inaccurate Software Audit Results

By Keli Johnson Swan

Although software compliance can sometimes fall low on a company's priority list, a software audit typically brings prior software compliance efforts into sharp focus. An audit, whether initiated by a software publisher, or by one of its representatives such as the Business Software Alliance ("BSA") or Software & Information Industry Association ("SIIA"), is a complicated and lengthy process, with rules set by the auditor.

Many audited companies believe that granting the auditors full access to their networks demonstrates good faith that the ultimate settlement will be more lenient. Even companies with strict internal compliance audits and detailed software and hardware purchase records often discover compliance issues during the course of the audit. For example, sometimes remnants of old software suites are not entirely erased from a computer registry when a new version is installed. Additionally, sometimes a company is unaware that some server software products have varying rules regarding physical and virtual server installations.

Granting an auditor full access to the network is fraught with problems. First, it is likely the audit results will be inaccurate, and include products that are the result of false positives. If the scanning tool does not distinguish between express versions, remnants of older products, and free user tools, the settlement demand will be artificially inflated, resulting in a significantly higher total settlement. Second, allowing a third party to audit the network affords no protections of attorney-client or work-product privilege, and exposes any information to disclosure. If a settlement is not reached, and there is no confidentiality agreement or privilege to protect the audit results, the auditor may use the information against the audited company in court.

Many companies rely on inside counsel or a general corporate attorney, who may not be aware of the risks and strategies for minimizing exposure from software audits. Hiring an experienced software auditing attorney is the key to a good audit defense strategy. An attorney experienced in defending against software audits can navigate the process and protect against the disclosure of inaccurate information, ultimately minimizing total exposure.

About the author Keli Johnson Swan:

As an associate attorney at Scott & Scott, LLP, Keli is primarily focused on software licensing and copyright infringement matters. She advises clients in a variety of industries to ensure compliance with software licenses and develop strategies for maximizing the value of software licenses.

Get in touch: kjohnson@scottandscottllp.com | 800.596.6176