

Seeking Help for an SIIA Audit

By Julie Machal-Fulks

After receiving a request from the Software & Information Industry Association (“SIIA”), many companies choose to conduct an internal audit of software installed on their networks. There are multiple considerations regarding the strategy for conducting an audit, including, but not limited to, the nature of the company’s record-keeping, the size of the company, the size of the network, the type of software at issue, and the IT support.

An internal audit may be more appropriate for a company with fewer computers, either manually or utilizing one of many free software scan tools available online. There are risks associated with this type of audit, most significantly the risk of inadvertently submitting information regarding a free download that may be mislabeled, and inaccurately reporting to the SIIA as unlicensed software.

A large company with multiple computers and users faces a higher potential exposure if the audit results are inaccurate. If a large company seeks to conduct its own audit, the free scanning tools are still an option, as manually checking each computer is both tedious and can lead to mistakes.

Finally, regardless of the size of the company, management may seek a consultant who specializes in software infringement issues and who can assist with network inventory and sorting through software purchasing invoices and receipts.

Prior to disclosing any information related to network inventory to either an internal resource or an external consultant, it is extremely important to obtain a confidentiality agreement to prevent the information from being disseminated to the SIIA. It is also important to obtain legal counsel experienced in defending against SIIA audits.



About the author Julie Machal-Fulks:

As a partner at Scott & Scott, LLP, Julie Machal-Fulks leads a team of attorneys in representing and defending clients in legal matters relating to information technology. Her practice focuses on complex litigation ranging from privacy and network security, data breach notification and crisis management, intellectual property disputes, service provider negligence claims, and content-based injuries such as copyright and trademark infringement in software, the Internet, and all forms of tangible media.

Get in touch: jfulks@scottandscottllp.com | 800.596.6176