

Is it Possible to Short-Circuit a Software Audit?

By Christopher Barnett

Companies react in different ways after receiving a letter from the Business Software Alliance (BSA) or the Software & Information Industry Association (SIIA) demanding a software audit.

Some ignore the letter, assuming it to be some kind of spam or marketing ploy. This is not advisable. Audit demands from the BSA and SIIA generally are very serious matters, and they can result in federal court litigation if they are neglected or if the auditors determine that a company is not cooperating in good faith.

Some companies take the opposite approach and provide all of the requested information to the auditors. While we typically advise our clients to cooperate with the BSA and the SIIA, it is important to know where to draw the line in the information-gathering process to ensure that only relevant data is provided to the auditors. The management of a software audit therefore can be time-consuming and expensive, depending on the size of the business or the IT environments at issue.

Given the prospect of that burden and expense, many companies justifiably are very interested in discovering opportunities to “short-circuit” the software audit by sharing information that makes the auditors go away without going through the full audit process. In our experience, those opportunities are few and far between, though they may be worth exploring in particular cases. For example, it is possible (though relatively rare) that the auditors may provide detailed information regarding the software products alleged to be in use without sufficient licensing. Under those circumstances, it may be possible to provide equally detailed information regarding installations of only those products and the associated licenses owned by the company without discovering and detailing the deployments and licenses of all BSA- or SIIA-member products installed on the company’s computers. As another example, if the audited business is confident that it knows the identity of the auditor’s confidential informant, and if it has information to discredit any allegations that informant may have made to the auditors (such as evidence that the informant installed unlicensed software on the company’s computers before being terminated), then it may be possible to convince the auditors to suspend the audit by attacking their key witness’ credibility.

However, in the vast majority of BSA or SIIA audits, a negotiated outcome requires the submission of information of software installed and licensed owned for all products within the scope of the audit demand. Companies stand a better chance of having realistic expectations in such matters by working with knowledgeable counsel.



About the author Christopher Barnett:

Christopher represents clients in a variety of business, intellectual property and IT-related contexts, with matters involving trademark registration and enforcement, software and licensing disputes and litigation, and mergers, divestments and service transactions. Christopher’s practice includes substantial attention to concerns faced by media & technology companies and to disputes involving new media, especially the fast-evolving content on the Internet.

Get in touch: cbarnett@scottandscottllp.com | 800.596.6176