BSA Informants: How to Protect Your Company against Copyright Infringement Claims by Disgruntled Employees Seeking a Reward

By Keli Johnson Swan

In an effort to enforce the copyrights of its members, BSA |The Software Alliance ("BSA") offers the potential for monetary rewards to any informant that shares information related to software copyright infringement against a company. Many of our clients are facing audits because an informant has turned them in.

Even if a company is able to demonstrate that its software is properly licensed, it is difficult to hold the informant accountable for the time and expense incurred as a result of the audit because the BSA protects the identity of its informants.

There are a few tips on how to deal with disgruntled former employees seeking revenge through a BSA reward.

1) **Prevention.** In many instances prevention simply is not possible because a company learns of the potential informant at the same time it receives an audit demand from the BSA. However, if you have not yet received an audit request, a company should manage its network to protect against potential claims.

   Lock down the network. Limiting the individuals who are able to access, download, or install software, scanning tools or any other information to or from the network is an essential safeguard against creating potential copyright infringement claims. First, by preventing downloads, you are able to control what is installed on the network and limit it to only licensed software. Second, you can prevent any potential informants from stealing raw data from the network and delivering it to the BSA in an effort to obtain a reward. Third, limiting access to administrators ensures that an employee cannot create a compliance problem on his or her way out in an effort to damage the company.

2) **Recourse.** Sometimes a company may have a suspicion about who the informant is based on the timing of an acrimonious departure of a former employee and the initial audit letter. However, the BSA will not release the name of the individual. Even in litigation, it could be difficult to obtain the informant's identity. However, if the BSA relied on specific information relating to its claims, it may be forced to identify the informant. The question remains: what is a company's recourse?

   Employee Non-disclosure Agreement. If the informant signed a non-disclosure agreement, it may be possible to pursue the individual for breaching that agreement, depending on the language of the agreement. However, even if this action is ultimately successful, a company should be mindful of the cardinal rule of litigation: never sue a poor person. Aside from the satisfaction of holding an individual accountable, the company may never receive damages or attorney's fees.

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333
Scott & Scott, LLP
Website · Disclaimer

Request Informant Not Be Rewarded. Once an audit is resolved, if a company believes that the informant may have been directly responsible for intentionally or negligently creating the compliance gap, the company should request that the informant not receive a reward. Although the BSA's attorney typically indicates that he or she has no control over the reward, the BSA may take the information into consideration. It is important to wait to make this request after the audit is complete and a settlement is reached.

3) **Mitigation.** The best way to prevent current employees from turning into informants is to ensure that software compliance is a priority.

Software Asset Management. Following the audit, companies should consider implementing a comprehensive software asset management plan that includes procurement, installation, live management, internal audits, and license maintenance. Ensuring that all software is properly licensed at all times will save significant time and potential penalties from false claims. It is essential that a company maintain accurate records for all software purchases regardless of the age of the product. A plan to manage software compliance in conjunction with appropriate security protocols to prevent individuals from accessing the network or downloading or installing software is the best way to mitigate potential copyright infringement claims.

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