Employees as Whistleblowers: Source of Software Piracy Tips to BSA & SIIA

Regardless of whether you think Edward Snowden, the IT contractor who leaked news about the National Security Agency (NSA) electronic surveillance program, is a martyr or a traitor, his actions have put the spotlight on "whistleblowing". According to Scott & Scott, LLP, whistleblower reports to software trade associations - BSA | The Software Alliance and the Software Information & Industry Association- involving alleged software piracy are frequently under the radar, number in the thousands annually, and are very costly to businesses. Scott & Scott, LLP recommends the following proactive measures to mitigate the risk of becoming a target of the BSA or SIIA.

Southlake, Texas (PRWEB) June 27, 2013 -- The term "whistleblowing" has been in the daily news associated with a contracted IT Booz Allen Hamilton hire. Edward Snowden, the elusive American whistleblower, disclosed he was the source of how the U.S. Government collects data on billions of Americans' phone calls and Internet activities. According to a June 25th article in The Telegraph, Snowden admits that he "deliberately went to work for the US intelligence contractor in order to harvest highly classified evidence of the National Security Agency (NSA) surveillance programs".

Although rarely in the headlines, whistleblowing is a frequent threat to businesses from software publishing trade associations – BSA| The Software Alliance and The Software & Information Industry Association – whose nationwide advertising campaigns incite businesses' employees or former employees to report employers who allegedly run unlicensed software products with offers of cash rewards in exchange for tips produces thousands of software piracy reports. The cash rewards are tied to the proceeds of an audit. The reports are confidential and the associations refuse to disclose the names of their informants.

"In our experience, business owners targeted by the trade associations frequently believe that the person suspected of making the report was responsible for failing to maintain compliance or maliciously installed software without the owner's knowledge", said Robert J. Scott, Managing Partner, of Scott & Scott, LLP, an intellectual property and technology law firm, with a focus on software license compliance and software audit defense.

Because the BSA and SIIA reports are confidential, employers may suspect but usually cannot prove who the whistleblower was.

Scott & Scott, LLP recommends the following proactive measures to mitigate the risk of becoming a target of the BSA and SIIA:

1. Obtain signed confidentiality agreements from employees, IT vendors and consultants.
2. Implement a software asset management policy. Develop license compliance as a core competency.
3. Retain proofs of purchase and keep accurate records.
4. Negotiate license agreements with publishers to incorporate less one-sided terms into "standard" software license agreements.
5. Review software compliance regularly (at a minimum, once a year) with their licensing terms.

About Scott & Scott, LLP (www.scottandscottllp.com)(www.bsadefense.com) is a leading intellectual property

and technology law firm representing businesses in matters involving software licensing. Scott & Scott, LLP's legal and technology professionals provide software audit defense and software compliance solutions, all protected by attorney-client and work-product privileges.

Robert J. Scott, a recognized expert on software compliance and defense, is available for interviews.
-30-

Contact Information
Anita Scott
Scott and Scott, LLP
http://www.scottandscottllp.com
214.999.2915

Online Web 2.0 Version
You can read the online version of this press release here.