SOFTWARE POLICE OFFER REWARDS TO INFORMANTS

Brought to you by WOOD HERRON & EVANS LLP

Both of the two predominant software industry trade associations, the Software & Information Industry Association (SIIA) and the Business Software Alliance (BSA), offer rewards to an employee-informant who reports software piracy at his/her company (or, as often as not, his/her former company). The offer of what amounts to a bounty for tips on corporate piracy has added impetus to enforcement efforts that were already vigorous.

Through its toll free tip line and web site, the SIIA has generated an average of 150 reports per month, mostly from current or former employees of the target companies. Upon receiving these initial reports, the SIIA conducts a preliminary review of the credibility of the informant and the reliability of his/her information and, after vetting the initial calls, generally settles on about 25 cases per month for further investigation and pursuit.

The reward programs of both BSA and SIIA offer up to $1,000,000 to informants with first hand knowledge of corporate end-user piracy. The SIIA advises that the quality and level of detail provided by its informants has been substantially increased as a result of the reward program.

While both of the BSA and SIIA do a good bit of work behind the scenes, a target's first inkling that something is amiss is typically a letter from association outside counsel to the president or general counsel of the target advising that the trade association has information leading it to believe that the target has pirated copies of certain software applications. The letter typically advises of statutory remedies of up to $150,000 per copy for willful violations and offers participation in a voluntary self audit in lieu of litigation.

By the time a target gets one of these letters, the opportunity to avoid a disruptive, expensive, and embarrassing investigation has been lost. While cooperation in the audit will forestall no-win litigation, the target will be in the unenviable position of attempting to produce dated proofs of purchase for each and every copy of software installed on all of its PCs, laptops, and servers. Targets of BSA/SIIA investigations invariably find this process, with its upside down burden of proof, to be a frustrating distraction from the press of ordinary business.

The terms of settlement typically offered at the conclusion of the audit generally require the target to agree to destroy all copies of software for which proof of purchase could not be produced, repurchase replacement copies for the software destroyed, pay a settlement sum amounting to three times the manufacturer's full suggested retail price of the individual applications destroyed (not discounted suite or bundle prices), and make certain additional certifications. Although it is possible, under appropriate circumstances, to negotiate for much more favorable settlement terms, the better approach is for companies to get their IT house in order before they become a target. Consider conducting a self-audit under the supervision of your own lawyer before a disgruntled employee nominates your company for a program it may find most unrewarding. And if it's too late for that now, give us a call.

For more information, contact:

Steve Gillen
Wood Herron & Evans LLP
2700 Carew Tower
441 Vine Street
Cincinnati, Ohio 45202-2917

sgillen@whe-law.com
Direct Dial (513) 707-0470