

Are You Prepared for a Software Audit? You Better Be

By Travis Crabtree, Looper Reed & McGraw



It is a little ironic that in the high tech software world, your liability sometimes comes down to whether you saved the receipt. If you face an audit and don't have the records to support all of the software on your system, you will have to pay the MSRP for the software (regardless of how much you paid originally), destroy it and buy another legitimate copy. You don't want to pay for software four times.

How it Works and Why You Need to Pay Attention?

Software companies have followed the music industry model and formed trade groups, such as the Software & Information Industry Association (SIIA) and the Business Software Alliance (BSA), to pursue claims for pirated software. These groups promise rewards for anonymous tips. So that disgruntled IT employee you let go may squeal to the industry group, even though he may have been the very one to download or copy an unauthorized program. As a result, you receive an audit demand letter.

The BSA publicized a settlement with a Texas company in excess of \$500,000 earlier this year and increases in the number of settlements in excess of \$100,000. Looper Reed has already assisted several clients who have paid more than \$100,000 in the aggregate.

The audit demand letter claims the BSA or SIIA has reason to believe you have pirated or unauthorized software and demands you run an audit of your system or face an expensive copyright infringement suit citing intimidating statutory copyright penalties ranging from \$750 to \$150,000 per work. You have two options: cooperate or ignore it.

Cooperating means you pay for an expensive software audit that reveals when and how many times each of the programs on your computers and your servers were installed. If you ignore it, you risk ending up in a federal copyright lawsuit and will have to go through the same audit as part of discovery.

If you chose cooperation, you usually agree to a process to audit your software, keep it confidential and provide the information. Along with the data, you should provide all of the documentation establishing you properly purchased the software. Without proper documentation, the trade groups assume the software is unlicensed.

What Documentation Do I Need?

The trade groups are very particular about the documentation they will accept. Generally, they do not accept photocopies of the packaging, photos of the CD or license keys. They prefer receipts or invoices from authorized vendors. When you buy a computer pre-loaded with software, you can often show the invoice from the manufacturer with the software listed.

What They Do With the Audit

The trade groups take all of the information and determine how many programs are not supported by proper documentation. They then make a demand for payment of the MSRP of the software, statutory penalties and attorneys' fees. It often includes inflated prices because industry groups unbundle the programs. For example, many companies will buy a suite or bundle of programs (like Microsoft Office or Adobe Creative Suite) that gives them ten software products for \$5,000. If you were to buy those same ten products independently, it would cost you \$10,000 or \$1,000 per program. If you have an unauthorized copy of the suite on someone's laptop or computer, then the demand starts at \$10,000 and not \$5,000. The statutory penalties often start at two or three times the MSRP. Now, the BSA or SIIA is demanding \$30,000 for the \$5,000 bundled suite.



Are You Prepared for a Software Audit

Usually, the parties can negotiate a settlement that includes a payment, an agreement to destroy the unauthorized copies and a requirement that the company implement software policies and do subsequent audits.

So What Can You Do To Avoid This Headache?

Unfortunately, it is very difficult to prevent the downloading of unauthorized software on all computers and networks. There are steps, however, you can take to greatly reduce the risk.

First, risk avoidance. It sounds simple, but keep the paperwork and audit yourself on occasion. Work with your IT personnel to prevent employees from downloading programs on your computers or systems without administrative authorization. If you are not up to that level technologically, at least educate your employees on the risks and have a policy in place that prohibits the employees from using or downloading unauthorized programs. Showing that you tried to act proactively can help in the negotiation process.

Second, risk shifting. If you outsource your IT functions, then make sure your consultant is responsible for maintaining the records and will indemnify, defend and hold you harmless for an audit and any fines. This assumes the consultants will be able to afford the costs of an audit, defend the claim and then pay the fines.

Third, risk mitigation. When the audit demand comes, find counsel and qualified IT personnel that can guide you through the process that can sometimes take between six and 18 months. Don't wait until the demand letter comes asking for three times the MSRP amount because qualified counsel can guide you along the way.

If you haven't received an audit demand yet, consider yourself fortunate. Now is the time to take steps to prevent this headache from ever even occurring.

About Looper Reed & McGraw

Founded in 1985, Looper Reed & McGraw is a full-service, Texas based law firm with more than 120 lawyers practicing in Dallas, Houston and Tyler. Looper Reed & McGraw offers a wide range of legal services including business litigation, corporate transactions, oil & gas, tax planning and litigation, real estate, healthcare, trusts and estates, employment law, family law, intellectual property, and bankruptcy. For more information, visit www.lrlm.com.

This Looper Reed & McGraw Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice.

Copyright © 2012 Looper Reed & McGraw, P.C. All rights reserved.