Adobe Audit Demands Can Be Burdensome

By Christopher Barnett

Businesses contacted by Adobe for software audits can be lulled into thinking that those investigations entail less exposure risk than audits by other publishers, like Microsoft or IBM. Adobe audits typically are conducted directly by Adobe representatives, rather than by a third-party auditor like Deloitte or KPMG, and the inventory data usually is provided by the audited business using its own toolsets. In addition, Adobe's audit team is generally quite genial in its approach, at least at the outset of an engagement. However, like all software audits, companies need to be aware of the pitfalls associated with Adobe reviews, notably including the following:

- **Scope Creep.**
  The biggest trap for many businesses facing Adobe audits is the demand for data that the relevant licensing agreements do not require an audited business to create or maintain. Adobe's agreements typically vaguely require licensees to provide an "unedited accurate report of all Software installed" on their computers and "records useful to determine whether installations…have…been serialized." However, the agreements do not specify what kinds of data must be maintained, nor do they expressly require licensees to generate reports, run scripts, or take any other actions outside the ordinary course of business. Adobe's auditors often are very specific win their requests with regard to scripts, toolsets and report outputs, but audited companies must determine for themselves whether those requests are consistent with the terms of the agreements that define the scope of Adobe's audits.

- **Hacked Installs.**
  Unlike many publishers, Adobe takes a special interest in gathering data that it believes points to the installation of "cracked" or "portable" installations of Adobe software on an audited company's computers, and it typically presses companies to provide the file path and executable filename information for the software deployments captured in audit inventories (information that, again, is not identified as something that licensees are required to produce during an audit). For those products, instead of a simple license purchase, Adobe often will demand a penalty payment based on some measure of the damages available under U.S. copyright law. All companies need to make it clear to employees that the use of invalid serial numbers or other technical work-arounds for copy-protection measures are not allowed on company computers.

- **Inflated Demands.**
  Where "cracked" or "portable" Adobe installations are discovered during an audit, companies need to work closely with legal counsel to ensure that Adobe's penalty demands are consistent with the audit data and with the damages allowable under U.S. copyright law. Like those of many publishers and software industry groups, Adobe's allegedly copyright-based settlement demands often are tainted by either an incomplete or overly optimistic understanding of applicable legal principles. An audited business' legal team should be prepared to attack those calculations (or to negotiate an alternative approach to resolving the audit).

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

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333