Misuse of Your Company's Software Volume License Keys Can Cause Big Headaches

(NAPSA)—It sounds harmless enough: An employee uses software at work and wants to continue using it at home. So he takes a copy of the software home, installs it and then validates it using his employer's volume license key (VLK)—a special code that software-makers issue to organizations with volume license agreements to allow activation of their software. But what happens when the employee shares that code with a friend? Or posts it to an Internet discussion board so all his friends can use it?

To those in the software industry, there are no shades of gray. Whether it's used by one person or 1 million people, a stolen VLK amounts to stolen software, and the ramifications can cause major problems for a business, a library, a university, or any organization that needs its software up and running.

Microsoft Corp. estimates that the majority of counterfeit software in use today employs VLKs that have been stolen, leaked or inadvertently misused. For the organization whose key is leaked and then used in piracy, remedying that situation can be time-consuming and a headache for IT administrators tasked to deal with it.

The software company must issue a replacement key, and then the organization must deploy the new product key again—across the entire enterprise. Of course, the amount of IT overhead involved depends on the size of the

> For unsuspecting users who receive counterfeit software through no fault of their own, some companies have services and promotional offers to help them obtain genuine software.
> Ⓣ

organization, but it can be expensive in terms of time and effort for the IT department.

So what can organizations do to better protect themselves from this problem? Most important, they should strictly control access to their VLKs. If new volume license agreements are issued, organizations should also use the new VLKs quickly. The better control they have over their VLKs, the less exposure they have to the risks of misuse.

For unsuspecting users who receive counterfeit software through no fault of their own, some companies have services and promotional offers to help them obtain genuine software, such as the Genuine Microsoft Software Web site at http://www.microsoft.com/genuine. According to those in the software industry, if you discover that your software is not genuine or that your VLK is no longer under your control, you should contact the licensing specialist or account manager who handled your software purchase.

For more information about genuine software, please visit http://www.microsoft.com/genuine.