

September, 2005

# legal update



## Practical Advice on Protection of Proprietary Information

*By Helen A. Zamboni, Esq.*



You've developed a confidentiality and nondisclosure agreement (NDA) that you require all employees to sign as a condition of employment. The NDA states that the company owns this information, and that employees are only entitled to use it in furtherance of the company's business. The employees agree that upon termination of employment, they will return all company property, including intangible property such as customer lists, trade secrets, etc., and will not use it for any purpose whatsoever.

Under the NDA, the employees agree that they will sign any new agreement form the employer deems necessary to protect its confidential and proprietary information. Your NDA and all subsequent revisions make it clear that the version most recently signed revokes all prior agreements dealing with the same subject matter.

So far, so good. You've put your employees on notice that the company is serious about preventing disclosure, misappropriation and misuse of the company's intellectual property and competitively sensitive information. You can require employees to sign new forms so that you only have to administer one set of terms and conditions. The company should have the legal protections it needs.

But do you have gaps in your business processes that threaten to undo all that your documents have done? Have you trained your managers about "need to know"?

Too often, managers take for granted that employees at certain levels within a company have the right, by virtue of their positions, to know more than they need to know to perform their job duties. It's a matter of status. And knowledge is power. By spreading knowledge of proprietary information to subordinates, a manager is demonstrating her power and also building loyalty among the members of her staff.

Managers should evaluate carefully what company confidential information her employees truly need in order to perform their jobs before making any disclosures. This is especially true in sales management.

Salespeople generally have assigned "territories" (geographic, or based on customer size, or some other kind of segmentation). A salesperson needs to know about the customers in his territory. But he probably doesn't need to know about the customers in his colleagues' territories.

Here's a scenario to ponder: One of your best salespeople leaves your company, where he was assigned to the northeast, and joins one of your competitors. You are quite sure that he did not take any lists or computer files with him. After all, like many salespeople, he wasn't tech-savvy and relied on office support to handle his reports. He was also one of the most ethical salespeople you've ever worked with, and he left on good terms with your company.

Now his sales territory is the midwest. While he was working for you, did he have access to information about your midwestern customers?

Salespeople are the most mobile employees in any industry. Once they become familiar with the industry in which they are employed, they move from company to company with ease. Even if they don't take anything with them from your company -- a printed customer list, a computer file with customer information -- they have what is between their ears. It can be very difficult and expensive to prove that this former employee is misusing YOUR company's property under these circumstances. In fact, he may not even realize it himself.

It's best to try to avoid this altogether. Scrutinize your company's disclosure practices and tighten them up. An ounce of prevention is worth a pound of cure.