

Qualifying for Trade Secret Protection: Practical Steps for the Closely-Held Company

* * *

From vaccines to aircraft skins

By Dirk Bartram

Our article above explained why trade secret protection is important to closely-held companies. This article suggests three practical steps to qualify information for that protection.

When reviewing the steps outlined below, remember that trade secret protection only applies to information that: (i) gives your company a competitive advantage; (ii) is not generally known or ascertainable in the industry; and (iii) is subject to reasonable security measures.

Identify the information that might qualify for protection

Identify vital information used by your company which is not generally known or ascertainable by proper means, such as reverse engineering. This identification will help you to complete the other two steps outlined later in this article.

Don't be discouraged if some of your vital information is generally known. Nearly all trade secrets combine some public information with new and confidential information. The case of *Merck & Co., Inc. v. Smithkline Beecham Pharmaceuticals* gives an example. The plaintiff claimed trade secret protection for a process it developed for the production of a vaccine. The defendant claimed that the process was not a trade secret because its aspects were readily ascertainable in publications. The court rejected the defendant's argument, stating that "[T]he choice of individually known components and techniques to create a working manufacturing process is often, as here, a difficult undertaking. Where at individual steps of a process there are a variety of alternatives, the choice made through much effort of specific ingredients, materials, conditions and steps in an actual, working process constitutes a trade secret."

Make sure your company owns the information

After you identify the information you want to protect, ask yourself who owns it. Most closely-held companies mistakenly think they own the information they use. This problem usually arises when all or part of the trade secret information is developed by an employee. For example, say that your production manager develops a confidential, cost-effective, and unpatented method of manufacturing aircraft skin in your factory. If the production manager leaves the company, who owns the method, the company or the production manager?

We dealt with this question in our April edition of *Closely-Held*. The answer is that employees who are hired to invent a defined product or process (e.g., scientists or engineers) generally have a duty to assign their invention rights to their employer, even absent an agreement. This duty applies to inventions that are conceived during their employment and that relate to the employer's business.

The problem arises when the employee isn't hired to invent. These employees are free to market the invention and to seek patents for it absent an agreement otherwise. In the case of the employee not hired to invent, the employer may acquire a limited non-exclusive right to use the invention, known as a "shop right." However, this is little solace given that the invention can be licensed or sold for a competitor's use.

Don't put yourself in the position of having to prove that your production manager or other employee was hired to invent. Have each employee sign an enforceable agreement in which they automatically assign their company-related inventions. Washington law places some restrictions on such agreements with employees, but these agreements can be a valuable tool if drafted correctly.

Take reasonable security measures

Nondisclosure Agreements. Every employee should sign a nondisclosure agreement. The agreement should define the protected trade secrets as specifically as possible and make clear that they are owned by the company. It should obligate the employee to use your trade secrets only for company purposes and to make no unauthorized disclosures of the information. The agreement can be in a standalone agreement or a clause within a larger contract, such as an employment contract.

Document Security. Mark sensitive documents and software as "confidential." Keep confidential media in the company safe or other secure area when they are not under an authorized person's protection and control. Secure access to the sensitive areas of your company's facility. Secure all computers with appropriate passwords.

Exit Interviews. Have a conversation with each departing employee before he or she leaves the company. Remind them that the trade secrets belong to the company and may not be used or disclosed after departing the company. Follow up the conversation with a confirming letter.

Need to Know. Disclose trade secret information on only a need-to-know basis. Don't disclose a confidential process to the sales force if they don't need to know it to do their jobs.

© 2004 Henke Bartram PLLC

All articles are intended for general information purposes only and should not be construed as legal advice. You should contact us or your attorney to obtain advice on any particular issue or situation.