

Protecting your trade secrets

*A brief guide
to preserving
intellectual
capital*

FISH & RICHARDSON P.C.

800 818-5070

www.fr.com

info@fr.com

©1994, 1997, 1998, 2000, 2002, 2005

FISH & RICHARDSON P.C. All rights reserved.

What is a trade secret?

A trade secret can be any useful information that is not generally known. A popular definition is “anything you don’t want the competition to know.” Other terms used for trade secrets are “confidential information,” “proprietary information,” and “know-how.”

Trade secrets are generally divided into two sorts: technical and business secrets. Technical trade secrets are found in research and development, secret formulas, designs, computer source code, manufacturing tools, and the like. Business trade secrets, a much broader category, cover the vast pool of marketing, sales, and financial and administrative data used to manage a business. Examples of business trade secrets include customer lists, marketing plans, financial and accounting data, and information about employees.

Trade secrets cannot cover information that is generally known to professionals in the field or generalized know-how (i.e., information necessary for a worker to complete a task efficiently and smoothly). For example, an experienced computer programmer’s ability to write efficient code cannot be classified as a trade secret; rather, it is part of the programmer’s “personal tool kit” – those skills belonging exclusively to the programmer and not to the employer. The programmer’s “personal tool kit,” however, cannot include specific code or specialized algorithms developed for previous employers. Drawing the line between what belongs to the employer and what is personal to the employee can be very difficult. In some states there are “inventor protection laws” that give employees rights to inventions made on their own time.

Why are trade secrets important?

In the past, a company's advantage might lie in its access to cheap labor or proximity to a railroad or quarry. In today's technology-driven markets, competitive advantage (and even survival) is a function of information. Even in "low-technology" industries, it is generally recognized that competitive advantage derives primarily from information, which often is referred to as "Intellectual Capital." Protection of that critical asset begins with trade secret law.

Employees move from job to job more freely than ever; and this is happening just as modern development and management techniques require that we trust more people, at lower levels of the organization, with access to the company's most valuable assets. Even customers and vendors are brought closely within the information circle by processes such as collaborative engineering. As we move closer to the global "virtual corporation," we find more information that is increasingly valuable and is being shared with more people, some of whom may be perceived to have less loyalty. Trade secret law protects your information from the actions of unscrupulous or careless employees.

Your company's intellectual capital is threatened not only by careless or unscrupulous employees and competitors, but also by governments around the world. For example, to manufacture or distribute your products, you may be required to trust agencies with secret formulas and other product information, or to license your trade secrets to a local (foreign) company. There is even evidence that some foreign governments commit industrial espionage to support their national industries. Knowing how to maintain the integrity of your information assets in this environment is critical.

Even good news carries with it a certain message of risk. The courts are more vigorous these days in protecting intellectual property. But this means that you may face expensive lawsuits from competitors who accuse your company of stealing their trade secrets and who seek restraining orders and massive damage awards. Also, criminal laws have recently been strengthened. Careless approaches to hiring employees or consultants, or to the development of new products or processes, can jeopardize your company's freedom of action in the market as well as expose you to criminal prosecution.

Creating trade secrets

No special procedure or government filing is necessary to create trade secrets. The law protects qualifying information that is shared in a confidential relationship, such as between employer and employee or between customer and vendor. Usually the relationship should include a written contract establishing that it is confidential.

Virtually all patents start out as trade secrets. Unlike patents, trade secret protection is potentially permanent. However, when you decide to use the trade secret form of protection for inventions, you take the risk that someone else may independently discover the same information and be able to use it without permission from you. Furthermore, if the later discoverer is able to get a patent, you may find yourself barred from using the very invention you first discovered. You may also lose your secret if it can be "reverse engineered" from your marketed product. See page 9.

Courts may refuse to recognize your claim of trade secret protection if they find you have failed to exercise reasonable efforts to keep your information from being disclosed. See page 5 for a list of appropriate safeguards.

Knowing what you have

The first step in protecting your property is to know what you have. You may be surprised at how much of your company's information will qualify for trade secret protection. Your goal in making any inventory of these assets is to identify the most critical areas of possible loss and opportunity. Ask: what do we have; who owns it; how is it being exploited; how might it be compromised or lost?

Define the team that will be involved in this process. Ideally, information security management should be handled at the executive staff level. You should include on the team those who have responsibility for physical and computer security as well as Human Resources. Develop a system for gathering information from managers involved in each phase of the company's business, including research and development, manufacturing, marketing, and administration.

Keep the process flexible. As you begin to review what you have, you may find that more (or fewer) people should be involved. As your company grows or moves into new markets or technologies, the procedure that worked before may no longer be appropriate.

Follow up regularly with efforts designed to update the data you have gathered and to generate feedback regarding the process. Remember that there is no single way to accomplish this important task. You must consider your company's unique features and environment.

Plan to protect trade secrets

A good trade secret protection program should have these goals:

- **Prevent loss** *(by inadvertence or theft)*
- **Discourage theft and encourage care**
- **Demonstrate the importance of the company's information assets**

Your plan should contain these elements:

- **Inventory** *This is covered on page 4.*
- **Simplicity** *Overly complex procedures won't be followed and can cause more harm than good.*
- **Responsibility** *Management commitment and ownership of this function must be clear.*
- **Review** *The plan should be regularly reviewed for compliance and possible changes.*

Specifics of any program will of course vary, but should address at least these areas:

- **Document and records control** *Protection from improper disclosure or use; retention/destruction policies*
- **Facilities control** *Visitor access and escort*
- **Equipment control** *Computers (including laptops), photocopiers, fax machines*
- **Contracts** *With employees, consultants, vendors, customers and others (see page 7)*
- **Employees** *Hiring, education, and termination (see page 6)*

See also page 12 about programs to limit criminal exposure.

Dealing with employees

Use care in hiring. Claims may result from your being seen as hiring in order to obtain the trade secrets of a competitor, or to destroy a competitor's ability to compete. Investigate your candidates carefully. You will want to know if someone has a contract restricting his or her right to compete, or if the applicant has been exposed to particularly sensitive information in previous employment. Watch out for those who imply that they can bring useful information to the company; in fact, you may want to have applicants sign a statement that they will not infect the company with trade secrets belonging to anyone else.

Educate your employees (all of them) about the importance of trade secrets. Studies have shown that the vast majority of information losses occur through employee inadvertence. The education process should begin with the signing of an individual non-disclosure agreement. It should continue with a variety of techniques, including memos, handbooks, and training sessions, designed to communicate the company's policy that its valuable trade secrets need the active concern of everyone in the organization and that the trade secret rights of other companies are also to be respected. You may want to consider incentive programs that encourage employees to disclose their ideas and inventions to the company.

Require that records be kept of all research and development activities. Review papers, articles, and speeches before they are published. And be sure that sales personnel know what they can and cannot say regarding unreleased products.

With particularly valuable employees who will have ready access to important trade secrets, consider requiring a promise not to compete against the company for a period of time after the employment ends. The

advantage of such an agreement is that you don't have to prove in litigation that the former employee might misuse specified trade secrets. However, noncompete contracts with employees are closely examined by the courts for fairness and in some states they are not allowed.

Be especially attentive to trade secret concerns when an employee terminates employment. Use a standard procedure for exit interviews that confirms the employee's continuing obligations to protect the company's information. Learn where the employee is going and the level of risk indicated. Consider sending a warning letter to the former employee and the new employer.

Using contracts to protect and exploit secrets

Contracts are the key to protecting your trade secrets outside the company, as well as to avoiding trade secret disputes. You should consider these principles when you are dealing with your vendors, customers, business partners, and the government.

First, be sure that your relationship is well-defined. If you plan to trust someone else with your most important property, you want to be clear about the confidential nature of the disclosure. In most cases, this requires only a simple statement that the person receiving the information acknowledges its confidentiality.

Second, be clear about what information is covered, and the process that you will follow in identifying information that is considered confidential. This is especially important for the person that receives the information, so that there is no misunderstanding about the scope of what is to be maintained as secret. If the contract covers useful information developed during the

course of the relationship, you need to define who will own what.

Third, define how each side's information will be protected during the contract period, and how it will be returned or destroyed at the end of the relationship.

Fourth, if you intend to grant a license to use the secret information and related patents, be careful to distinguish between the two types of property. You can be compensated for the trade secrets (a "know-how" license) indefinitely, but if this is mixed with patent rights which expire on a set date, you could have serious problems.

Finally, be sure that you have established policies and procedures for dealing with the trade secrets of others. If you have taken on the burden willingly, you should take care to control access and use so that you comply with your contract. In addition, you should make clear to your workforce that no unauthorized disclosure to the company of the trade secrets of others will be tolerated. See also page 10 about avoiding criminal exposure.

Competitive intelligence

A wealth of useful information about your competitors is freely available. The challenge is to gather it in a way that is ethically—and therefore legally—proper. Courts usually regard as acceptable using public sources, such as databases and government filings, but draw the line at what might appear to be espionage or behavior that induces someone to breach a duty of confidence. For example, in one case, a competitor's aerial photography of a factory under construction was held illegal. You expose yourself to civil and criminal liability when you try to trick someone (such as an unsuspecting employee) into giving you information that you know is supposed to be confidential.

Because the boundary defining unlawful activity is not bright and clear, it is important that you manage this activity within your company. Consider centralizing the function under one or more persons who are trained professionals. Periodically review the methods used. Avoid the temptation to gather information from disaffected employees of your competitors in the course of (or worse, under the guise of) job interviews.

To protect against effective competitor intelligence, make extensive use of nondisclosure agreements with all vendors. Require that raw materials be delivered in unmarked or color-coded containers. Train and warn all those who attend trade shows and conventions to be wary. Qualify your potential customers and know to whom you're talking. When you discover a breach of security, treat it seriously and swiftly. The best defense against this sort of attack is to be known as intolerant of trade secret theft.

Reverse engineering

Reverse engineering is defined as starting with a known product and working backward to learn the process which aided in its development or manufacture. So long as you do this without violating some other right (such as patent, copyright, or trademark) or obligation (such as a contract that prohibits it), you are acting within the law.

Why engage in reverse engineering? You may want to know what others are up to, in order to keep abreast of the "state of the art" in your field. You may also want to understand another's product so that you can develop a product or service that is compatible or complementary. These are considered appropriate objectives by the courts.

In order to avoid trouble, start with a product or information that you acquired legally and honestly. Do not make unauthorized copies, which could violate the Copyright Act or (as to semiconductors) the Mask Work Act. You may talk to knowledgeable people, so long as they do not reveal confidential information about the product. Finally, conduct a review of the literature and issued patents not only to learn about the technology, but also to lessen (if not eliminate) the risk that you will be investing your resources in making something that is covered by a valid patent. Also, consider contracts or licenses that might apply to the product or information you are using. Sometimes these include a promise not to reverse engineer. Enforceability of these contracts may be unclear; nonetheless, only after carefully analyzing the contract should you take on the risk.

In the process of reverse engineering, use only personnel who have not had previous access to the information you are trying to discover. Keep thorough records, since this is key to showing that you spent your own resources in deriving the information. And if you plan to produce a product with similar functionality, avoid any unnecessary similarities in appearance.

Trade secret disputes and criminal cases

Litigation over trade secrets is expensive, time consuming, and distracting. Avoid it if you can; if you cannot, seek a practical and effective solution early in the process.

If you believe that your trade secrets are compromised, first be sure of the facts through investigation. Of course it is important to pursue vigorously clear cases of theft, but you stand a better chance of getting what you want if you have a clear idea of what happened and of the secrets

that are at risk. A thoroughly prepared plaintiff is much more likely to convince a judge to issue an immediate injunction, which often leads to a quick resolution of the case.

As a plaintiff, your primary objectives are to stop the misappropriation of your trade secrets and perhaps to recover compensation. As a defendant, your goal is to resolve the litigation in your favor. More frequently than you might think, both sides' goals can be accomplished without carrying lawsuits through to trial and appeal. Working through competent counsel with experience in this sort of litigation, trade secret claims are often diverted from the courts into private mediation and arbitration. This method generally produces results more swiftly and less expensively than litigation does and helps to preserve potential business relationships.

In fact, early and clear communication between potential combatants can avoid litigation completely. Again, chances of success depend on being prepared, but high-level communication between executives should be the preferred avenue of confrontation.

In many states, trade secret theft is a crime. Theft of trade secrets affecting interstate commerce may also be covered under the federal trade secrets law, (called the "Economic Espionage Act") which imposes severe fines and jail terms. If the case warrants it, the authorities may assist you by investigating and prosecuting the wrongdoers. This method is arguably the best solution because the behavior is treated seriously and without substantial cost to you. However, keep in mind that once you hand-over the matter to the criminal justice system, its ultimate resolution is out of your hands.

It is also important to control your own exposure to criminal prosecution for the

actions of an employee, agent, or affiliate. A “compliance plan” designed to meet federal requirements should define standards of conduct and disciplinary consequences, provide for training of employees, be managed from a high level of authority, and be subject to regular monitoring and audits.

Foreign protection of trade secrets

The world community is coming to recognize the importance of all forms of intellectual property, including trade secrets, as necessary foundations of a global economy. However, few foreign countries provide effective remedies against trade secret misappropriation. Despite recent success in establishing international trade secret standards through mechanisms such as the GATT agreement and the NAFTA treaty, enforcement in most foreign countries is spotty. Efforts at harmonization of international laws and enforcement mechanisms are ongoing, but unlikely to produce substantial improvement in the near term. Nevertheless, by coordinated action in the relevant foreign country and in the U.S. (which is often the offending company’s biggest market), satisfactory results can be achieved in court.

Self-help measures are of utmost importance in protecting your trade secrets abroad. Confidentiality agreements are critical, especially in civil law countries (i.e., most outside of the U.K. and the former Commonwealth). In general, exercise increased vigilance in connection with foreign travel by executives; guard sensitive papers and laptops closely, and suspect eavesdropping. Limit the information provided to overseas managers, and consider rotating foreign nationals who occupy sensitive positions at foreign facilities. ♦

This material is for general informational purposes and is not legal advice. It is not a substitute for professional legal advice regarding a specific transaction or the laws for a particular jurisdiction. This information is not intended to create, and receipt of it does not create, an attorney-client relationship.



FISH & RICHARDSON P.C.

Intellectual property | Litigation | Corporate

Austin

512 391-4930

Boston

617 542-5070

Dallas

214 747-5070

Delaware

302 652-5070

New York

212 765-5070

San Diego

858 678-5070

Silicon Valley

650 839-5070

Twin Cities

612 335-5070

Washington, DC

202 783-5070

