



## TRADE SECRETS

In the area of Intellectual Property Law, trade secrets are an oddity. Unlike patents, trademarks and copyrights, they were not historically protected by any Federal law. Moreover, there is no procedure for examination, approval, or registration. Just as the name implies, “trade secrets” must be secret.

Trade secrets are vital to the livelihood of many companies and business entities.. Companies tend to invest significant time, energy, and money into restructuring various processes, techniques, and methods of operation that generate revenue. Without trade secret protection, competitors would have access to that same knowledge, which could potentially threaten a company’s survival in the marketplace. As such, trade secrets must be heavily guarded.

In this “Primer” on Trade Secrets, we explain what a trade secret is, what laws protect them, how to decide whether and when to rely on trade secret protection, and what to do when trade secrecy is violated...or you are facing claims of trade secret theft.

### Table of Contents

- A. What Is a “Trade Secret?”..... 2
- B. Trade Secret Laws ..... 2
  - 1. The Uniform Trade Secrets Act, and N.C.’s Standard for Trade Secrecy ..... 2
  - 2. The Minority Standard for Trade Secrecy..... 3
  - 3. The Federal Standard for Trade Secrecy..... 4
- C. Which Affords Better Protection—Trade Secrecy or Patents?..... 5
- D. Advantages of Trade Secrecy ..... 5
  - 1. Quick and Easy to Establish..... 5
  - 2. No Maintenance Fees ..... 5
  - 3. Perpetual Protection ..... 5
- E. Disadvantages of Trade Secrecy: Why Patenting or Registering Copyrights May Be the Better Option..... 6
  - 1. Reverse Engineering ..... 6
  - 2. Difficulty in Enforcement ..... 6
  - 3. Uncertainty ..... 6

F. Maximizing Trade Secret Protection .....	6
G. Enforcement of Trade Secrets.....	7
H. Defenses in Trade Secret Cases .....	8
I. Summary.....	8

## A. What Is a “Trade Secret?”

Trade secrecy is governed by federal law, state law, and the common law. Depending on the controlling law, the precise definition varies. However, there are three elements which are common to all definitions. Generally, a “trade secret” includes commercial information of any nature—including designs, devices, processes, compositions, techniques, or formulae—that:

- affords an economic benefit or competitive advantage to its owner;
- is not generally known to the relevant public; and
- is the subject of reasonable efforts to maintain its confidentiality.

Trade secrets include, for example, recipes (whether chemical formulae or recipes for soft drinks and fried chicken), manufacturing processes (from how to put thin films on semi-conductor chips to how to make the best “dimpled” honey-roasted peanuts), and business information (from customer lists, to names of suppliers, pricing data, and best ways to upfit data processing centers and offices for efficiency).

## B. Trade Secret Laws

Unlike patents, trademarks, and copyrights, trade secrets were not historically protected by any Federal law or specifically mentioned in the United States Constitution. This does not mean that a trade secret is without legal protection or status. Even in the early days, the common law recognized the right of a business to protect its confidential information, and common law still applies in those situations that have not been pre-empted by Federal or State laws.

Over the years, many states have enacted legislation to define a trade secret and outline the legal remedies for its misappropriation. Most of them now follow, at least in general terms, the format of the Uniform Trade Secrets Act. In 1996, additional protection was made available under Federal law to prosecute those who misappropriate trade secrets under the Federal criminal statutes.

### 1. The Uniform Trade Secrets Act, and N.C.’s Standard for Trade Secrecy

Like the laws in effect in most of the states and territories of the United States, North Carolina has a statute to protect trade secrets, based on the Uniform Trade Secrets Act with a few minor modifications. The statute first defines a trade secret as:

business or technical information, including but not limited to a formula, pattern, program, device, compilation of information, method, technique, or process that:

- a. Derives independent actual or potential commercial value from not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from its disclosure or use; and
- b. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The law goes further to state:

The existence of a trade secret shall not be negated merely because the information comprising the trade secret has also been developed, used, or owned independently by more than one person, or licensed to other persons.

As it sounds, the law is fairly broad, potentially covering a wide variety of valuable business information, from lists of customers to formulas for manufacturing the information, as long as the information is intentionally kept secret, is not generally known, and cannot be easily reverse engineered.

If a trade secret is discovered by a competitor without any wrongdoing, there is no legal recourse. If the discovery results from misappropriation, the law offers injunctions to prevent continued use of the information, possible royalty payments to the originator for continued use, and restitutionary or punitive damages.

## **2. The Minority Standard for Trade Secrecy**

Those few states and territories that have not adopted the Uniform Trade Secrets Act or (like North Carolina) a close variation of that Act have for the most part agreed on a standard of trade secrecy that typically is referred to as the “Restatement of Torts” definition. The principal difference between the Restatement standard and the standard followed by the other jurisdictions is one of breadth. Generally, less protection is afforded to secrets in the Restatement jurisdictions than is true in the majority of states.

Still, the protection is far better than nothing. While variations abound, most of the Restatement jurisdictions would agree on the following definition of a trade secret:

any formula, pattern, device or compilation of information which is used in one’s business, and which gives the business owner an opportunity to obtain an advantage over competitors who do not know or use it. . . . A trade secret is a process or device for continuous use in the operation of the business.

As a result, although the majority rule will protect “negative information”—that is, information about processes that do not work—those following the Restatement rule ordinarily

will protect only information that actually is used to operate a business.

### **3. The Federal Standard for Trade Secrecy**

Persons attempting to protect their trade secrets in the states and territories that follow the Restatement standard may be able to draw on other state remedies to protect their trade secrets—for example, laws prohibiting theft, or unfair competition. The differences in coverage across the United States, however, as well as in foreign nations (many of which have similar laws), emphasize the importance of knowing the specific requirements of the territory in which one is doing business and in which one's trade secrets may become known.

Partly because of the hodge-podge of laws, Congress stepped in and has passed two laws that give national teeth to trade secret protection,.

Under the Economic Espionage Act of 1996, theft of trade secrets became a Federal crime. In order to define what is punishable, Congress for the first time provided a Federal definition of “trade secret.” In general, the definition is similar to that set out in the North Carolina statute; if anything, it is broader:

The term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--

- a. the owner thereof has taken reasonable measures to keep such information secret; and
- b. the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public...

The Act defines “theft of trade secrets” as including outright theft of trade secrets, concealment of trade secret information, copying, photographing, uploading or downloading trade secret information, destroying trade secret information, knowingly receiving misappropriated trade secret information, and, in general, otherwise interfering or attempting to interfere with the trade secret owner's exclusive enjoyment of his property.

More recently, Congress adopted the “Defend Trade Secrets Act of 2016,” which substantially mirrors the Uniform Trade Secrets Act, uses a similar definition of trade secrets, has a three-year time period within which suit can be brought, and authorizes remedies similar to those found in current state laws. It adds protection for whistleblowers under certain circumstances, and failure to give notice of the protection can result in limitations on the damages an employer can recover if suit is brought. Essentially, the newest act gives trade secret owners one more option as to the location in which suit can be brought, with a few nuances that may assist them in proving their case and in obtaining rapid help when situations warrant.

## **C. Which Affords Better Protection—Trade Secrecy or Patents?**

The best method of protection depends upon the nature of the invention or information. In some cases, a patent is not the best way to protect an invention. The invention may be short-lived, for example, and might no longer be useful in two or three years; or it may be only marginally profitable, not justifying an investment in patent protection.

Other types of information simply don't qualify for patent protection. For example, business plans, customer lists, and financial data are not patentable inventions, and typically are protected by trade secrecy because there is no other viable protection for such information. (Copyright may protect outright copying, but in most cases it's the underlying information that needs protection—not the creative words in which the information has been put down on paper.)

In still other cases, patents and trade secrecy may be combined. For example, one aspect of a product might be patented, while the method of making other aspects, as well as sources of supply for the nonpatented components, are kept secret. (Remember, in order to get patent protection, one must disclose the best way known to the inventor of making the claimed invention—but it is not necessary to disclose the best way to make the parts for which protection is not sought.)

A good protection plan must consider all types of protection, and trade secrecy has a part in many situations. Business owners and others trying to protect business assets should consult an experienced intellectual property attorney to help determine when and how to rely on trade secrecy, keeping in mind the advantages and disadvantages discussed below.

## **D. Advantages of Trade Secrecy**

### **1. Quick and Easy to Establish**

Acquiring trade secret protection requires no application, no lengthy examination or registration process, nor any expensive fees. Unlike patents and trademarks, the details of a trade secret do not have to be revealed to a governmental agency. Trade secret protection exists as soon as the business entity takes reasonable precautions to keep the information confidential. Thus, where technology is rapidly changing, trade secrecy can keep pace with the changes.

### **2. No Maintenance Fees**

Unlike patents and trademarks, there are no intermittent fees that must be paid in order to maintain trade secret protection.

### **3. Perpetual Protection**

Protection can last indefinitely, so long as the trade secret is not discovered and made publicly know. One example, frequently discussed, is the formula for making Coca-Cola syrup. It has remained secret since its inception, and it is said to be known only by two people. Kentucky Fried Chicken's "secret formula" of herbs and spices is another example.

## **E. Disadvantages of Trade Secrecy: Why Patenting or Registering Copyrights May Be the Better Option**

### **1. Reverse Engineering**

Once a trade secret becomes known to the public, it is virtually lost and can never become a trade secret again. Both independent development and reverse engineering (analyzing a lawfully acquired product to discover its secret method of design or manufacture) are permitted under state law, although it remains to be seen whether at least some forms of reverse engineering will now be considered a Federal criminal offense. (The Federal Economic Espionage Act of 1996 defines downloading, uploading, and “replicating” trade secret information as types of wrongful conduct.) Thus, in many situations, if a product is available to the public, there is little that a company can do to prevent its analysis by others, and use of the analyzed information.

The unfortunate reality is that due to the vast array of scientific technology, almost anything can be broken down, analyzed, and copied. In spite of the fascinating history of the Coca Cola formula, statistics have been compiled which indicate that the average trade secret is secure for only about four to five years. This average life will decrease in the future, as technological advances make reverse engineering easier.

### **2. Difficulty in Enforcement**

As previously mentioned, if a trade secret is discovered, then protection is forever lost. It is irrelevant, in most cases, whether the trade secret is discovered through legitimate or illegal means. While a trade secret owner has the right to sue anyone who discovered your trade secret illegally, there typically is no protection against one who acquires the information by honest means. Both independent development and reverse engineering are permitted under state law, and may be permitted even under the more stringent Federal statute.

### **3. Uncertainty**

A trade secret holder cannot know when the secret will be lost, thus triggering the loss of all protection. Trade secrets do not have a fixed or known term like the seventeen years of a patent or ten years of a trademark. Thus, if a business relies on trade secrecy as a significant asset, it must face the reality that the asset has an uncertain life.

## **F. Maximizing Trade Secret Protection**

Because maintaining trade secret protection is entirely dependent on maintaining confidentiality, all reasonable steps which can be taken to maintain and enhance security should be taken. At a minimum, the trade secret owner should acquire and use a “CONFIDENTIAL” stamp or other means of putting “CONFIDENTIAL” notices prominently on documents that are to be kept secret. Employees should be told that they are not to discuss confidential information with anyone except those involved in the work, and not to discuss company business outside the place of employment.

It is safer to have written confidentiality agreements with those who will be exposed to

company secrets. Noncompetition agreements may be included in appropriate cases. Advice of counsel should be sought in drafting such agreements, and in obtaining employee signatures.

The agreements should be tailored to the specific requirements of the business owner, because the courts generally do not favor restrictions on use of information or on employment, and will invalidate overly broad contracts. Some states are stricter than others. In California, for instance, most restrictions are invalid, and California takes a very expansive view of the employment relationships it is entitled to govern.

In addition, unless the persons who are agreeing to maintain confidentiality receive something in return for their agreement, the contract will be invalid. Likewise, failure to mention whistleblower exemptions can prevent certain types of damage and attorney fee awards.

Counsel with experience in this field can advise, based on the particular circumstances of the business, what types of remuneration are likely to be sufficient and what terms should be included in the agreements.

## **G. Enforcement of Trade Secrets**

Lawsuits can be brought in state court to enforce trade secrets and to enforce confidentiality and noncompetition agreements. Suit may also be appropriate in Federal Court in some circumstances, such as when the parties are from different states, or when patent, trademark, Federal unfair competition, or copyright claims are also included—or when suit is brought under the federal Defend Trade Secrets Act. In addition, under the Federal Economic Espionage Act of 1996, the United States Attorney is authorized to bring criminal charges against those who have misappropriated trade secrets.

The disadvantage of litigation is that the defendant normally has a right to know what is alleged to be secret, so that he can prepare a defense. The secret may thus be exposed to a potential direct competitor, as well as to expert witnesses who become involved. Although judges can issue orders that the alleged secret be kept confidential by all parties while the suit is pending, the risk of inadvertent exposure increases as the number of people with knowledge increases. If the suit is lost, the secrecy order will often be lifted, and a competitor has thus probably been given more information than it had to begin with.

Successful litigation, however, can deter employees from setting up competitive businesses based on stolen corporate information. In addition, a victory can enforce ethical business practices by competitors who, without such deterrence, would thrive on stolen data.

Theft of trade secrets is usually coupled with unfair trade practices. As a result, the trade secret owner, if successful, can usually not only recover his actual, provable damages (or the misappropriator's profits), but also can have these damages trebled; or receive an additional award of punitive damages. The defendant may also be required to pay the trade secret owner's attorneys' fees.

In criminal cases, a guilty defendant can be imprisoned up to ten years as well as fined; and corporations can be fined up to \$5 million (or, if greater, three times the value of the trade

secret). If the trade secret was stolen for the benefit of a foreign government or foreign instrumentality or agent, then the potential term of imprisonment becomes fifteen years, and the potential fine is also increased (\$500,000 for an individual; \$10 million for a corporation). The guilty defendant will also forfeit to the United States government any profits earned from use of the trade secret and any property purchased with the money that was earned; and may also forfeit any property that was used in stealing the trade secret (computers or automobiles, for example).

## **H. Defenses in Trade Secret Cases**

Misappropriation of trade secrets is most often alleged against former employees and their new employers. The interests of the defendants are not always identical. The employee is caught in a real bind. He often has little money to defend against a suit, but his future employability may depend on a successful defense. While his new employer may assist, it is often strategically best for the new employer to take the position that even if the employee did take information to which he was not entitled, the data has not been passed on to the new employer, and the new employer is not at fault in any way.

Success in defense of trade secret cases often depends on thorough investigation. It is important to have a clear statement of the material alleged to be trade secret, and then to intensively investigate the extent of public knowledge of that information. Any glitches in the trade secret owner's methods of maintaining confidentiality should be explored. Are outside salesmen taken into areas where the allegedly secret process is being used? Are family members allowed inside the plant? Is confidential data stamped "confidential" and kept in locked file cabinets, or strewn about on desks where anyone could see it? Has the company obtained patents, which of course are public documents, on aspects of the supposedly secret apparatus or method? Have other companies used the same technology, showing that it is "generally known" and thus does not qualify as a trade secret. How easy would it be to compile the same data? If "secret" customer lists are merely a listing of all companies that appear under certain headings in the phone book, or in trade directories such as the Thomas Register, then the same data would be "readily ascertainable through independent development" and does not qualify as trade secret.

Even where a contract was signed, promising confidentiality and noncompetition, it may be invalid. For instance, the trade secret owner may have failed to give adequate compensation for the agreement.

Thus, the mere accusation of trade secret misappropriation, although traumatic, is not grounds for despair. Nonetheless, trade secret litigation is expensive, and should be avoided whenever possible.

## **I. Summary**

While trade secrecy is an inexpensive form of protection in many ways, maintaining confidentiality requires constant vigilance. Without such vigilance, however, the trade secret and all its value to the company will be lost. Use of confidentiality agreements, "CONFIDENTIAL" stamps, and similar steps will help maintain trade secrecy. If litigation must be brought,



consultation with experienced counsel as early as possible will help in planning a strategy to enforce the secrets without unduly risking their disclosure and loss.

\* \* \*