

Trade Secrets Revealed

By Christopher A. Sexton, Esq.

Businesses often invest substantial time and money developing specialized manufacturing processes, formulas, and customer lists. Moreover, such information may give them a competitive advantage and thus, the ability to protect it from unauthorized disclosure and use can be vital to the business' success. Fortunately, under California law, such information may receive protection as trade secrets. This article will provide an understanding of what trade secrets are and give strategies for their protection as well as for avoiding trade secret misappropriation claims by competitors.

What Are Trade Secrets?

In 1985, California adopted the Uniform Trade Secrets Act. It defines "trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Thus, whether a court will conclude particular information is a trade secret depends upon whether it believes the facts of that case meet the Act's requirements.

In essence, the definition of trade secret consists of four elements: (1) information; (2) not generally known to others; (3) which has independent economic value because it is unknown; and (4) which the owner has attempted to keep secret. An understanding of each element is necessary to determine whether a protect able trade secret exists.

1. Trade Secrets Are Information. In appropriate circumstances, courts have recognized the following types of information as trade secrets:

- **Customer lists and related information** are frequent subjects of trade secret litigation. When they are, value and secrecy are generally the focus of the court's inquiry. The most important questions are: Was the customer list compiled at substantial effort and expense (e.g., through years of marketing)? Are the users of the company's products easy to ascertain (e.g., which stores sell avocados)? Is the customer information sophisticated (key contacts, special requirements, which customers are most valuable)?

Most trade secret litigation involves former employees who use customer lists and information acquired during their employment in another competing business. Generally, the information is used to solicit customers (asking them for business) of their former employer. If the customer list is found to be a trade secret, the former employee and their new employer may be ordered to cease such solicitation and prohibited from doing business with the former employer's customers. However, if the information is only used to announce their new employment affiliation (and not solicit), a former employee my contact customers of their former employer even if their identities are trade secrets of the former employer.

- **Manufacturing processes and formulas** can be trade secrets. Even though certain tooling used in manufacturing may be patented, non-patented information related to the manufacturing process may be protect able as a trade secret. A formula, such as the ingredients used to manufacture a soft drink, can also be trade secret. Unlike patents, which are of limited duration, trade secret protection is available for as long as the information meets the requirements of the Uniform Trade Secrets Act.

- **Negative information**, knowing what not to do, may have substantial value and may have been

acquired through extensive research. Information related to which potential customers are not good prospects for a company's products or services, which suppliers' products are unsuitable for a particular manufacturing process, and which processes do not work have been held, in appropriate cases, to be trade secrets.

● **Computer software and source code** developed for in-house use can be a trade secret even if it consists of a combination of elements all of which are in the public domain.

2. The information cannot be generally known to others. Matters of public or general knowledge in an industry are not trade secrets. To be a trade secret, the information cannot be readily ascertainable through proper means such as directories, the internet, or technical journals. Moreover, if a trade secret misappropriation claim is based upon information disclosed by a former employee, it cannot consist of the employee's general knowledge and skills. An employee can use such information for the benefit of any new employer, even if it was acquired during former employment.

3. The information must have independent economic value because it is not generally known. A simple way to determine if this element is present is to compare the value of the information at issue to information that is generally known in a particular industry. If a business' customers buy its product or service for reasons unrelated to the secret, the value of the secret is questionable. In other words, does the owner derive a competitive advantage from the use of the secret?

4. A trade secret owner must take steps, reasonable under the circumstances, to keep the information secret. What may be reasonable for a small business may not be reasonable for a large company. Although extreme methods for preserving secrecy need not be used, to quote one court: "a substantial element of secrecy must exist so that, except by the use of improper means, there would be difficulty acquiring the information."

Reasonable efforts to maintain secrecy include advising employees of the trade secret's existence, limiting access to trade secrets on a "need to know" basis, controlling access to areas where trade secrets are being used, and requiring non-disclosure agreements from those who need access to or will be exposed to the company's trade secrets.

Employer or Employee, Who Owns Trade Secrets?

A threshold issue in any trade secret controversy, and one that should be resolved before trade secrets are developed (if possible), is who owns or will own the information. Disputes over trade secret ownership commonly occur in the context of employment relationships, with independent contractors, and between co-developers.

In a typical employment scenario, an employee may develop or participate in the development of trade secrets, inventions, or material protect able by copyright. In the absence of an agreement to the contrary, such developments usually belong to the employer. In fact, California Labor Code provides that: "Everything which an employee acquires by virtue of his employment, except the compensation which is due to him from his employer, belongs to the employer..." This includes inventions and trade secrets.

Only employee inventions (and presumably trade secrets) developed entirely on the employee's own time, without using the employer's equipment, supplies, facilities, or trade secrets that do not relate to the employer's business, its actual or demonstrably anticipated research or development, or result from any work performed by the employee for the employer, belong to the employee.

What is Trade Secret Misappropriation?

The Uniform Trade Secrets Act defines misappropriation as:

- “1. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
2. Disclosure or use of a trade secret of another without express or implied consent by a person who:
 - (A) Used improper means to acquire knowledge of the trade secret; or
 - (B) At the time of disclosure or use, knew or had reason to know that the his or her knowledge of the trade secret was:
 - (i) Derived from or through a person who had utilized improper means to acquire it; or
 - (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
 - (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
 - (C) Before material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge it had been acquired by accident or mistake.”

“Improper means” has been defined by the courts to encompass conduct that falls below an acceptable level of commercial morality and includes theft, bribery, misrepresentation, espionage, and breach of fiduciary duty or confidence. Thus, **misappropriation is the unauthorized acquisition, disclosure, or use of another’s trade secret if, at the time of acquisition, disclosure, or use it is known, or should be known, that the information was acquired by improper means, through a breach of confidence or duty, or by accident or mistake.**

In its most common form, the misappropriation results from copying and removing documents or data. However, even if the trade secret is retained in memory, through familiarity with the information or otherwise, its unauthorized disclosure or use is, nevertheless, misappropriation.

On the other hand, it is not misappropriation to perform independent research in an attempt to discover information that may be of value to a business, even if that information turns out to be the same or similar to a competitor’s trade secret. Reverse engineering, the process of analyzing an existing product and working backward to determine how it was developed, is also an acceptable form of research. Such means of obtaining information alone are not considered improper.

Protecting Trade Secrets

As discussed above, a trade secret must be the subject of reasonable efforts by its owner to maintain its secrecy. Disclosing the information to the public (those having no business relationship with the owner and thus, no “need to know”), even on a limited basis, destroys its secrecy and its status as a trade secret. Accordingly, care must be taken to disclose trade secrets only to persons with a “need to know.” Such persons might include employees, vendors, independent contractors, joint venturers, prospective licensees of the information, or prospective purchasers of the owner’s business. Although a duty of confidentiality is implied in most such relationships, it is best to create a contractual obligation to confirm the existence of the confidential relationship and provide notice of the obligations of confidentiality.

Because employees (or former employees) are the most common misappropriators of trade secrets

(intentionally and unintentionally), developing a protection program at that level should be the first line of defense. Protecting trade secrets should begin at the inception of the employment relationship and continue after its termination.

During the hiring process, prospective employees should be advised they will be working with company trade secrets and will be required to execute a confidentiality agreement. If trade secrets must be disclosed during the hiring process to, for example, determine an applicant's fitness for a particular position, a confidentiality agreement should be executed prior to any disclosure. Confidentiality provisions may also be included in the employee handbook and all employees required to read and agree not to disclose or use any proprietary information of the company.

Moreover, the work environment should be a reminder that trade secrets are being used and conducive to their protection. Protective measures might include:

- Limiting access to areas where trade secrets are being used and to areas where trade secret information is stored, including file storage and computer networks, on a "need to know" basis.
- Placing proprietary information notices on trade secret documents and embedding such notices in documents stored electronically and/or use of color coding to remind employees such documents are confidential.
- Shredding or otherwise destroying confidential documents before disposal. Companies do not have a reasonable expectation of privacy in trash left for disposal in a public place. Thus, discovery of confidential information by culling through such discarded material is not misappropriation and may destroy its protection as a trade secret.
- Placing limits on the number of copies of confidential documents in existence.
- Developing a trade secrets protection plan incorporating the various protective measures to be utilized and including such plan in the employee handbook.

The employment termination process should also be addressed in the company's trade secrets protection plan. Among other measures, separating employees should be reminded of their continuing obligations of confidentiality. If possible, a signed statement from the employee acknowledging those obligations and representing that all company property has been returned, including copies of all confidential information in tangible or electronic form, should be obtained. Post termination, the company might consider sending polite letters to the former employee and the new employer, if known, regarding the existence of any confidentiality agreement and reminding them of the former employee's continuing duty of confidentiality.

Appropriate protective measures must also be maintained in the context of other relationships. Non-employee visitors to company facilities might be required to sign in, wear guest badges, be accompanied by an employee host and, in some cases, execute a confidentiality agreement. Trade secret information should only be disclosed to consultants, contractors, vendors, and others on a "need to know" basis and only after their written agreement to maintain the confidentiality of the information.

Although absolute secrecy is not required, the owner of a trade secret must make "efforts reasonable under the circumstances to maintain its secrecy." What a court will deem "reasonable" depends on the facts of a particular situation and has been the subject of many judicial opinions. Consequently, the assistance of counsel knowledgeable in trade secret law should be obtained to prepare a trade secret protection plan and to draft confidentiality agreements and other forms necessary to implement the plan.

Avoiding Misappropriation Claims

The consequences of misappropriating another's trade secret can be severe. Besides the costs of defending a misappropriation action (legal fees, wasted time, and aggravation), remedies provided by the Uniform Trade Secrets Act include orders prohibiting the use of the trade secret and monetary damages. If the misappropriation is wilful and malicious, the monetary damage award may be trebled and attorneys' fees may be awarded. In addition to civil liability, intentional misappropriators are subject to criminal prosecution under a panoply of state and federal laws. If convicted, penalties include imprisonment, fines, and restitution. Thus, in addition to protecting its own trade secrets, a business should guard against the misappropriation of another's trade secrets.

Because most misappropriation claims involve former employees of the plaintiff, particular care should be taken when hiring employees or former employees of a competitor. Before hiring a competitor's employee or former employee, enough information should be obtained by the company to weigh both the risks and benefits of hiring that person. Depending upon the industry and anticipated duties of the position to be filled, the company may want to determine:

- For which competitor(s) or potential competitor(s) has the prospective employee worked, their specific job duties, and, without the prospective employee's disclosure, the general nature of any trade secret information they possess.
- If the prospective employee is subject to any confidentiality, employment, or non-competition agreements.
 - What circumstances have led the person to seek new employment.
 - The nature and sources of knowledge and information to be utilized in the new position.
 - Any patents or patent able inventions of the prospective employee.
 - The company's motivation for hiring any employee possessing knowledge of trade secrets from which it may benefit.

If nothing else, the company should never encourage the disclosure of trade secrets or breach of any enforceable confidentiality, employment, or non-competition agreement. Moreover, the company should counsel the prospective employee not to disclose or use another's trade secrets during the hiring process or thereafter and obtain their written agreement not to do so.

In the area of trade secret law, there are few simple answers. The consequences of losing a trade secret by failing to adequately safeguard it or for the misappropriation of the trade secret of another can be devastating. As in many other areas of the law, "an ounce of prevention is worth a pound of cure."

Disclaimer

The information presented in this article is general in nature and should not be relied upon as legal advice. Any liability that might arise from the use of information presented here is expressly disclaimed. Please consult an attorney for advice on your particular situation.