

Intellectual Property

COMMENTARY

REPRINTED FROM VOLUME 13, ISSUE 21 / JANUARY 30, 2007

Trade Secrets: General Guidelines Every Employee Should Know

By Eric Faragi, Esq., and Todd Smith, Esq.*

Introduction

When most people think of trade secrets, they imagine Coca-Cola's famous recipe locked in a heavily secured vault or the names of Colonel Sanders' 11 herbs and spices dancing in the heads of a select few KFC executives.

The truth is that many companies — large and small — maintain their competitive advantage by using trade secrets that may be as mundane as source code and customer telephone lists. As technology continues to facilitate the rapid transfer of information, employees must be able to recognize when they are dealing with trade secrets and use strategies to avoid disseminating legally protected proprietary information.

Basic Principles

Each state has its own body of law governing trade secrets, but more than 40 of those states have passed versions of the Uniform Trade Secrets Act, the general provisions of which are discussed in this article. Under the UTSA a trade secret may include any formula, pattern, device or compilation of data used in a business that gives the business owner an advantage over competitors.

Because the law does not require trade secrets to be particularly inventive, they are rarely the subject matter of James Bond films. Trade secrets can be internal practices, business plans, marketing strategies, customer information, pending patent applications and financial data. An exact definition of a trade secret is impossible, but the following factors suggest that a given piece or collection of information may be protectable as a trade secret:

- The information is not known outside the business;
- The information is known by only a few employees in the business;
- Extensive measures have been taken to guard the secrecy of the information;
- The information is highly valuable to the business (and to its competitors);
- The business spent a great deal of time and/or money developing the information; and
- The information cannot be easily acquired or duplicated by others.

Secrecy, not surprisingly, is the foremost requirement for trade secret protection. The test for secrecy is whether the business has taken all proper and reasonable steps to protect the information, depending on the circumstances. The business might limit physical access to facilities, require agents or vendors to sign nondisclosure agreements, mark documents "confidential," require employees to sign noncompete agreements (restrictive covenants) or conduct exit interviews.

A trade secret may be protected indefinitely as long as it does not become publicly known. In some instances, trade secret protection may prove preferable over patent protection because a patent requires public disclosure of an invention and confers a limited-time monopoly lasting less than 20 years.

On the other hand, it is legal for a rival business to discover or derive, and then use, the trade secret information through independent development or reverse engineering. If a trade secret becomes "generally known," it ceases to be protectable, which is possible even through

inadvertent disclosure. In this respect, a patent affords broader protection than a trade secret.

What trade secret law protects against is misappropriation by improper means, such as theft, bribery, misrepresentation or espionage. In short, disclosure or use of a trade secret violates the law when there is a breach of confidence or an improper taking of the secret information. For example, a breach of confidence may occur when a business partner reveals or uses partnership information for personal purposes or when a business violates an express or implied agreement made with another business. A business person cannot use another company's trade secret if he or she knows the information was acquired in an illegal or immoral manner or that the trade secret was revealed by mistake.

When an express agreement between an employee and an employer is in effect, that agreement should be adhered to. Even in the absence of an express agreement limiting disclosure, an employee owes a duty of confidentiality to his employer with respect to the employer's trade secrets learned within the scope of employment. The employee is generally subject to varying obligations depending on his job responsibilities.

If an employee is hired to conduct research and development, there is an implied agreement that any trade secrets discovered by the employee within the scope of employment should not be disclosed or used without the employer's permission. If an employee is not hired principally to conduct research and development, he may have rights to a trade secret he discovers and may in the course of his employment disclose or use it, but the employer will also have the right to use it. (This doctrine is sometimes referred to as "shop rights.")

Penalties for Misappropriation of Trade Secrets

When trade secrets have been improperly acquired or used, a court may grant an injunction and/or monetary damages to the trade secret's owner. An injunction preventing the competitor's use of the information may last until the trade secret ceases to exist, or it may continue for a set period thereafter in order to eliminate any unfair lead time that was gained in the market because the competitor had knowledge of the information while it was still secret.

Monetary damages may include both the actual loss to the trade secret owner and the infringer's profit resulting from the misappropriation. Alternatively, damages may be calculated by determining a reasonable royalty. Damages may be enhanced in cases of willful and malicious misappropriation. Reasonable attorney fees may

also be granted against any party who took bad-faith positioning in the course of a trade secret dispute.

In addition to state law civil remedies, theft of trade secrets may also constitute a federal crime. The federal Economic Espionage Act, passed in 1996, makes certain instances of trade secret misappropriation a federal criminal offense. The EEA definition of a trade secret closely parallels the definition in the Uniform Trade Secrets Act. The EEA recognizes various categories of misappropriation of trade secrets, including theft, unauthorized duplication or transmission, and receipt, purchase, or possession.

The EEA applies to theft of a trade secret related to or included in a product in interstate or foreign commerce. In such cases individuals are subject to fines and imprisonment for up to 10 years, and organizations are subject to fines of up to \$5 million. There is no private right of action under the EEA, so the prosecution of a case is at the discretion of the federal government. Thus, if a company wishes to be sure of a hearing on its claims of trade secret misappropriation, a civil suit is the best remedy.

Practical Strategies for Employees Dealing With Trade Secrets

There are several practical strategies employees should keep in mind when dealing with trade secrets. The cardinal rule to remember is that trade secrets must always be protected by efforts that are "reasonable under the circumstances." What is reasonable can vary from one situation to the next. As a result, there are no hard-and-fast rules for protecting trade secrets, but there are some best practices to keep in mind.

Whenever dealing with trade secrets or any proprietary and confidential company information, an employee should always follow his company's policies. These policies may limit how and where trade secret information may be stored, both in terms of physical locations for files and equipment as well as virtual locations for digital materials.

In general, confidential information should be disclosed only to those employees who need access for business purposes, and a company's policies should limit access to this information accordingly. Policies may also include how documents and files containing trade secrets should be labeled. At a minimum, confidential documents should be labeled as "confidential."

Some trade secrets may be easily ascertained by observing operating machinery or manufacturing processes. If this is the case, those areas containing the machinery or manufacturing should be cordoned off and marked as restricted. Only those employees who need to take part in the process should be allowed access.

In many circumstances, to properly take advantage of trade secrets and utilize them in the course of business, they may need to be disclosed to third parties, such as outside contractors, suppliers or even customers. When dealing with outside parties, employees should avoid disclosing trade secrets unless doing so is necessary for business purposes.

Depending on company policies, authorization from a manager may be required prior to disclosure of trade secrets to outside parties. Without a signed nondisclosure agreement with the outside party, there may be a risk that the trade secret could lose its protected status. The third party should be made aware of any trade secrets being disclosed and notified that the information should not be further disseminated.

Confidential information of other companies should be treated with the same level of care as internal information. Employees should be careful to follow protocols and provisions in any confidentiality agreement with the counterpart company, which will contain limits on how information may be used. Employees should never seek to obtain the trade secrets of other companies improperly.

Employees should also refrain from bringing trade secret information from their prior employment to their new jobs. If an employee receives information from an outside source that he believes is an unauthorized disclosure of another's trade secret, he should immediately report the situation to a manager or the legal department.

Trade secrets should never be posted on a publicly accessible Web site because the law may deem the secrets "publicly known" by virtue of such posting. Confidential information should be sent via e-mail only when necessary, and the message, along with any attachments that contain trade secrets, should be marked as confidential. All parties addressed in an e-mail concerning confidential information should be authorized to have access to the trade secrets contained therein.

Employees should be aware that the duty to maintain the confidentiality of trade secrets continues after they leave a job. Some companies will have express confidentiality and nondisclosure agreements, but even without an express agreement an employee has an implied duty of loyalty to maintain the confidentiality of an employer's trade secrets.

Summary Of Do's And Don'ts for Employees

- Make your manager aware of existing or new trade secret information that is used or generated in your duties;
- Do not disclose your company's trade secrets without clear authority from your manager;
- If you need to disclose or send trade secret information by e-mail and you have authorization to do so, mark the e-mail "confidential";
- If you need to copy trade secret material, protect and mark the copies;
- If you need to disclose trade secrets to someone outside the business and you have authorization to do so, check with the legal department to confirm whether the person needs to sign a nondisclosure agreement and explain to the recipient that the information is confidential and not to be further discussed;
- Do not violate any nondisclosure or employee agreement;
- If you are not sure whether information is a trade secret, do not disclose it without first consulting with your legal team; and
- Respect trade secrets of other companies.

Conclusion

Trade secrets are a common, but potentially powerful, form of intellectual property. Businesses must be particularly careful when dealing with trade secrets because, unlike the case with patents or trademarks, for example, failure to maintain the confidentiality required for trade secret protection can result in a complete loss of rights. Those who improperly acquire or use trade secrets may face injunctions and may be forced to pay substantial monetary damages.

Employees must learn to identify information that qualifies for trade secret protection and must adopt strategies to prevent its inadvertent dissemination. Employees should always become familiar with their companies' policies governing confidential information and should consult with their managers when not sure whether a particular piece of information is a trade secret.

Trade secrets present many risks and opportunities, and the most prudent approach to managing them is to consult with intellectual property counsel on a regular basis.

** Eric Faragi and Todd Smith are associates in the intellectual property practice group at Baker Botts in New York.*