TRADE SECRET PROTECTION PROGRAMS

By Alan S. Gutterman[1]

For many companies, state trade secret laws have become a preferred form of intellectual property protection, even in cases where the subject matter (i.e., invention) might otherwise be eligible for patent protection. A trade secret may include any formula, pattern, device, or compilation of information that is used in one's business and that gives the person in possession an opportunity to obtain an advantage over competitors who do not know or use it. One of the key elements of perfecting legal rights in trade secrets is the person's ability to establish and maintain a complete and effective trade secret protection program. Several factors must be considered in designing and implementing an effective program for identifying and protecting a company's trade secrets:

- Gaining a full understanding of the company's business including the intellectual property used by the company and other enterprises with which the company comes into contact (such as licensees, suppliers or competitors);
- Understanding the company's organizational structure and the way in which information is distributed vertically and horizontally;
- Becoming acquainted with those persons within the company that have ongoing access to the trade secret information; and
- Learning the procedures that the company currently uses and has previously employed to protect its trade secrets.

With this information, a trade secret program can be designed that will fit the particular needs of the company as well as provide for continuing education of employees and an ongoing review of the overall program. Most trade secret protection programs will consist of at least these procedures:

- Adoption of security measures to mark trade secrets, thus, identifying what is or is not considered to be confidential;
- Segregation of trade secret information and limitation of access to the trade secret owner or other authorized personnel;
- Placing employees on notice that the company maintains confidentiality of its trade secret information and that each employee has a duty to assist in protecting such items;
- Developing a system to prevent inadvertent disclosure of the trade secrets to the public (such as through advertising or other publications); and

---

[1] The material in this report will appear in *Business Counselor's Law and Compliance Manual* by Alan S. Gutterman to be published in the summer of 2010 and is presented with permission of Thomson Reuters/West. For more information or to order call 1-800-762-5272. Alan Gutterman is the Founder/Principal of Gutterman Law & Business (*www.alangutterman.com*), which publishes the Emerging Companies Blog and the Business Counselor Blog, and a Partner of The General Counsel LLC (*www.thegeneralcounsel.net*).

- Strictly controlling the legitimate disclosure of trade secret information to third parties so that recipients are obligated to protect any information which they might receive, not disclosing or using it in any unauthorized manner.

One person within the company should be given primary responsibility for implementing and supervising the trade secret protection program. Alternatively, a committee of two or more may regularly to determine what information is to be protected as a trade secret and the procedures to preserve the confidentiality of such information. Each committee member should have detailed knowledge of the company's technology, as well as its contractual relationships with third parties. In larger companies, responsibilities for the trade secret protection program may be allocated among several departments. For example, the company might organize a central protection committee with the primary responsibility for developing and implementing a trade secrets protection program. The committee might include representatives of each department within the company that might be called to ensure that the protection program is consistently implemented throughout the organization. The committee would report to senior management. While the legal department would have the responsibility of enforcing the company's rights to its trade secrets, internal auditing would assist in the periodic review of the trade secret protection program.

Whether the company uses a single security coordinator, or forms a committee of several persons, the following steps should be taken in order to properly launch and maintain an effective trade secret protection program:

(a) Conduct an investigation and legal compliance review covering the company's intellectual property rights, including its trade secrets and other confidential information;
(b) Based on the results of the compliance review, develop a set of recommendations which can be incorporated into a draft of trade secret protection program;
(c) Circulate the draft security program to the directors, officers, and key employees of the company, as well as persons who may have responsibility for handling confidential data and information;
(d) Prepare drafts of model documents and contracts necessary for effective trade secret protection, including confidentiality agreements, employee confidentiality and innovations assignment agreements, noncompetition agreements, and provisions for use in license agreements and other standard contracts;
(e) Obtain comments on all draft documents and prepare final versions for inclusion in employee handbooks, etc;
(f) Obtain authorization from board of directors to implement necessary physical security measures, including labeling and storage of trade secrets;
(g) Conduct one or more training seminars for employees regarding trade secrets and the trade secret protection program;
(h) If necessary, obtain executed employee confidentiality agreements from all employees; and
(i) Establish a schedule for periodic review of the protection program, including reports by the administrators of the program to senior management and the board of directors.

*****

MODEL STATEMENT OF TRADE SECRET SECURITY PROGRAM

Use of form: This form provides employees with a general description of the procedures that the company follows to protect its trade secrets and confidential information. It explains the reasons for the program, provides a mechanism for the company to inform its employees regarding the information eligible for trade secret protection, and sets out basic procedures for labeling, transmitting, and storing trade secrets. Normally, trade secret protection generally consists of these considerations: (i) security measures will be adopted to mark and segregate trade secret information and limit access by persons other than the trade secret owner and those who have a "need to know"' (ii) steps should be taken to put employees and certain contractors on notice that the company seeks to maintain the confidentiality of its trade secret information and that they, as employees, have a duty to assist in protecting such items; (iii) a system should be developed to prevent inadvertent disclosure of the trade secrets to the public through advertising or other publications; and (iv) legitimate disclosure of the trade secret information to third parties should be strictly controlled so that the recipients are obligated to protect information they receive and not disclose or use it in an unauthorized manner. The company's trade secret protection program should be memorialized in a formal written statement that can be used to advise employees of their obligations with respect to the use and protection of such information. The existence of a written plan is persuasive documentary evidence that the company has taken affirmative steps to protect its trade secrets.

1. The Program

Much of the information you develop or acquire as an employee of [~ Company ~] (Company) involves Trade Secrets. Trade Secrets are competitively sensitive because of their general importance, their limited availability, and the relative secrecy with which they are maintained. This Program helps to safeguard the Company's Trade Secrets.

Trade Secrets have a legal status different status than ordinary business information; for this reason, you must treat them with special care. What is a Trade Secret and how does it differ from other information? A Trade Secret may consist of any information used by the Company to gain an advantage over competitors who do not know about, or how to use, that same information. Trade Secrets include, without limitation, source code, algorithms, system documentation, user manuals, training instructions, data structures and modifications of all the Company's computer programs, systems design and architecture, and other technical developments. A Trade Secret differs from other information because of the special advantage the Company obtains by exclusively using such secrets.

The Company's Trade Secrets make its operations distinct from competitors and unique in the way it conducts business. To be recognized as such, Trade Secrets must be kept confidential. If disclosed without restriction to people outside the Company, the information may lose its protected status as a Trade Secret.

2. Reasons for This Program

Trade Secrets must be given special treatment by you and others working with the Company for several reasons:

(a) A Trade Secret, in some instances, is the essence of a particular company. For example, very few people know the formula for Coca-Cola. If the formula were widely known, The Coca-Cola Company would not be as successful as it now is, for others could formulate and produce an identical product without bearing any of the customary research and development expenses.

(b) Trade Secrets are assets of the Company. Skilled experts created these assets at great expense and only after painstaking research, development and testing. For example, the Company's proprietary software product known as [~ Name of Software Product ~] required over [~ Number ~] person years to develop. The Company is continuing to invest considerable resources in this product to enhance and modify its software. If one of the Company's trade secrets is disclosed to a competitor or to the public, a valuable asset will be diverted or diluted and could even be destroyed or rendered useless to the Company.

(c) Every person who works for the Company occupies a position of trust and loyalty. The Company has placed its confidence in its employees who owe a duty to the Company as a result of this trust.

3. Basic List of Company Trade Secrets

Although this list is not all-inclusive, the following information is considered confidential at all times: [~ List of Trade Secrets ~].

The following categories of information might also be deemed to be Trade Secrets [~ Categories of Trade Secrets ~]. Moreover, the following procedures are used to identify other possible trade secrets at the Company [~ Procedures to Identify Trade Secrets ~].

Portions of the above information may circulate through the Company along many avenues. It may be found in formalized embodiments (such as source code listings, system design documents, or magnetic computer tapes containing proprietary computer code). Some of this information will necessarily be contained in less formal documents. For instance, elements of a marketing program have to be broken down, analyzed separately from the overall marketing program, and sent to outside entities. Also, sales data may be set forth in financial documents and in memoranda.

Please remember that it is not the form the confidential information takes but, rather, its substance that is important. The fact that the confidential information is contained in a letter does not make the information any less confidential. In fact, some of the Company's most prized Trade Secrets may be kept only in the memories of various employees. The procedures for handling confidential information apply equally to all Trade Secrets, regardless of the form the Trade Secrets take.

4. Dissemination of Trade Secrets

In most instances, not all employees have access to the Company's Trade Secrets. Access is generally given only on a need-to-know basis. Employees who do have access to Company Trade Secrets, in essence, are "trustees" of that material. A most important element of the Company's Trade Secret Program is to limit access to Trade Secrets.

All employees must restrict access to the Company's Trade Secrets to authorized individuals who require access and who have a need-to-know. Employees who have no reason to obtain knowledge of Trade Secrets should not seek or be allowed access. To help employees determine which information constitutes Trade Secrets, the Company has adopted the special labeling program described in Section 5 below.

5. Labels

The Company indicates to its employees that items are Trade Secrets and these shall be treated as confidential by conscientious labeling. This labeling program marks such sensitive material using rubber stamps, properly marked envelopes, and so forth. The following language, on a label or rubber stamp, should be applied to all materials containing Company Trade Secrets:

CONFIDENTIAL AND PROPRIETARY

This material is confidential and proprietary to the Company. Do not reproduce, publish, or disclose to others without express authorization of the Company.

6. Transmittal of Trade Secrets

Unavoidably, many of the Company's Trade Secrets must be sent via U.S. mail or through the direct mail channels of the Company. The following procedures should be followed in such event:

(a) Internal transmittal. Confidential materials disseminated within the Company through a direct mail channel should be placed inside an envelope marked "Confidential." This envelope must be (1) addressed, (2) marked "To Be Opened by Addressee Only" if appropriate, and (3) sealed. If the sender desires to avoid placing a legend on the outside envelope as "Confidential," then an envelope properly labeled as "Confidential" should be so marked and sealed, then it should be placed inside a separate envelope having no special legend. Of course, this precludes special handling of the enclosed "Confidential" envelope by mailroom personnel.

(b) External transmittal. Documents sent via normal postal channels are to be placed in an envelope addressed and sealed but not marked "Confidential." These documents will be forwarded as first class mail. In certain instances of extreme sensitivity, the nature of the information will warrant additional safeguards, in which case it should be sent as registered or certified mail, return receipt requested.

(c) Computer programming code and documentation. Whenever the Company makes a new release of a proprietary computer program with or without documentation, the distribution of such material is to be handled according to the procedures set forth in Section 6(a) and 6(b) above. In addition, all such materials are to be sent registered or certified mail, return receipt requested. An additional, form of a receipt should be placed in the envelope for the recipient to sign and return.

Company Trade Secrets should not be transmitted via e-mail since it is impractical to verify with certainty who has received a message and to limit the ability of recipients to forward a message that includes Company Trade Secrets to others who are not obligated to maintain the secrecy of the information included in the message. The only exception to this general rule would be under circumstances where the message is protected using Company-approved encryption devises or protective software and the message clearly notes that it includes Company Trade Secrets and that unauthorized recipients are required and requested to destroy the message and are prohibited from using or disclosing the contents thereof.

7. Storage of Company Trade Secrets

The Company policy mandates a "clean desk" and "locked file cabinets and desk drawers." Employees should take these steps in handling Trade Secrets:

(a) Confidential data should be secured at all times to prevent unauthorized disclosure of its contents.

(b) During non-working hours, this material shall be stored in a suitable, locked file cabinet or desk.

(c) During normal working hours, office doors should be closed and locked whenever the office is unattended, particularly if the confidential documentation is not stored securely (such as, open files kept in plain view on a desktop). This rule is particularly important during lunch hours.

(d) Access to confidential data through the use of network computer terminals and workstations or standalone desktop computers must be restricted under a security system that requires user identification codes and personal passwords. Various levels of security should be considered (including an actual lock and key where available, password protection to limit access to a particular program, directory tree structure, subdirectory or digital files). Similarly, backups of confidential data must be equally secure. No computer terminal or desktop computer is to be left unattended while logged in to a network or hard drive, or signed on to any database or program.

(e) Notebook computers that contain confidential data, whether located on a desk or carried in transit, are particularly vulnerable because of their portability. Such notebook or laptop computers never should be out of sight and reach, particularly when allowed to pass through photo-security screening (such as when entering in public buildings or at an airport terminal.

Backup diskettes, tapes or CD-ROMS containing confidential information must be equally guarded.

(f) Computer programs, when utilized by an authorized user on a Company computer, should be controlled by password access at all times and, when not installed in a Company computer, should be placed in the Company data center in the secured facility provided for such storage.

8. Destruction of Documents Containing Trade Secrets

At appropriate times, all confidential material should be systematically destroyed by shredding (with shredded material placed in burn bags where appropriate) or, where computer programming code is kept on magnetic tape, internal memory, or hard disk, by secure erasure and reformatting of the electronic media if appropriate. Under no circumstances should such material be thrown away in open waste containers as normal trash. When computers containing confidential material are replaced and the old computer is disposed of (whether by transfer to another user, sale, or destruction), all confidential material on the hard drive must be securely deleted as must the contents of all so-called backup, recycling and trash directories.

9. Intellectual Property Audit Procedures

Other procedures the Company uses to protect its Trade Secrets include: employee confidentiality agreements; assignments of inventions; non-competition agreements; entry and exit interviews; inspection of employee work stations; third party non-disclosure agreements; document managers who are responsible for administering the trade secret program; and intellectual property audit procedures.

10. Trade Secret Security Manager

The person responsible for administration of the Company's Trade Secret Security Program is [~ Program Manager ~].