§ 201:67. Executive summary for clients regarding trade secret protection programs

Client Executive Summary on Trade Secret Protection Programs

§ 1. Introduction

For many companies, state trade secret laws have become a preferred form of intellectual property protection, even in cases where the subject matter might be an invention that is 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. This memorandum provides an introduction to some of the issues associated with trade secret protection programs by covering the legal requirements, situational factors in designing trade secret protection programs, elements of trade secret protection programs, administration of trade secret protection programs, steps for launching and maintaining the program, physical security measures, implementation of confidentiality procedures and review of public disclosures.

§ 2. Legal requirements

Where available, legal protection for trade secrets generally depends on an assessment of two critical factors: "commercial value" and "secrecy." Establishing the commercial value of a trade secret is relatively straightforward. However, structuring a trade secret protection program that will be considered by court to consist "of efforts that are reasonable under the circumstances to maintain its secrecy" is more difficult. In order to meet the "reasonable efforts" test, the law requires the trade secret owner to undertake actual efforts which are rigorous enough to force another to use improper, unethical or illegal means to discover the trade secret. In structuring a program to meet this standard, companies should keep several things in mind. First, the efforts to maintain secrecy need not consist of all conceivable means to maintain secrecy and prevent improper means of discovery or be so extensive as to make discovery impossible; however, the efforts must be steps actually taken, as opposed to mere intent, and must be a demonstrated and active course of conduct designed to prevent the unauthorized disclosure or use of the information. Second, the trade secret must be treated as secret by some combination of physical security measures and confidentiality procedures. Trade secret owners should adopt a variety of security procedures, since the courts focus upon the synergistic combination of measures in determining whether the program is adequate. Accordingly, owners must take a balanced approach in developing the protection program, since reliance on just one or two measures is insufficient. Finally, the efforts must be directed at the particular trade secrets opposed to general business security.

§ 3. Situational factors in designing trade secret protection programs

While there is an extensive list of measures that can be undertaken by a trade secret owner, the primary concern is to select and implement those efforts which are reasonable under the circumstances yet not so extensive as to make discovery impossible—one court observed that trade secret owners are not expected to "take heroic measures to preserve" secrecy. In choosing the particular measures, the trade secret owner must consider three situational factors: the nature of the trade secret and its economic value to the owner; the nature of the industry, including the prevalence of industrial espionage; and the nature of the company. In analyzing the nature of the trade secret, the owner must consider whether it is obviously something that should be kept secret or is non-intuitive in nature. The less obvious the secret, the greater the need to inform employees that it is a trade secret and must not be disclosed. Similarly, the value of the trade secret has an impact on what efforts are reasonable. The greater the value, the more extensive the efforts to protect it should be. For example, while customer lists and records might reasonably be protected by the use of a locked filing cabinet and non-disclosure agreements, a secret manufacturing process may require protection by guards, as well as separation of the process to two or more different venues. With respect to the nature of the industry, companies in industries that are extremely competitive, that have high levels of employee turnover or in which industrial espionage is prevalent, require more extensive efforts to maintain secrecy. Some courts have also used the standard practice in the relevant industry as a guide in determining whether specific security procedures were appropriate. For example, the failure to use a written non-disclosure agreement at the outset of discussions regarding a potential business relationship might be excused if such agreements are not typical in the industry. By contrast, the lack of a confidential legend may be a material defect in the security program where custom and practice within the industry dictate such legends. Finally, in analyzing the nature of the company, one must evaluate the size and financial strength of such company. A small company with few employees and limited resources need not undertake the extensive protective measures required by a Fortune 500 company in order to meet the "reasonableness" test.

§ 4. Elements of trade secret protection programs

Several factors should be considered when designing and implementing an effective program for identifying and protecting a company's trade secrets. First of all, those involved in the process should have 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. Second, it is essential to understand the company's organizational structure and the way in which information is distributed vertically and horizontally. Third, the groups and persons inside the company with ongoing access to the trade secret information need to be identified. Finally, the persons involved in setting up the trade secret protection program should understand and use intellectual property audit techniques to learn about the procedures that the company currently uses and has previously employed to protect its trade secrets.

With the information mentioned above, 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 five different types of 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 and implementing training programs to ensure that employees are aware of what is considered to be a "trade secret;"

- Developing a system to prevent inadvertent disclosure of the trade secrets to the public, such as through advertising or other publications; and

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

§ 5. Administration of trade secret protection programs

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. If such a committee is used, each 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, the internal auditing department would assist in the periodic review of the trade secret protection program. In addition, outside counsel should be available to assist in periodic audits and answer specific questions that come up on a day-to-day basis.

§ 6. Steps for launching and maintaining a 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:

- Conduct an investigation and legal compliance review covering the company's intellectual property rights, including its trade secrets and other confidential information.

- Based on the results of the compliance review, develop a set of recommendations which can be incorporated into a draft of the trade secret protection program.

- 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. Review and participation by senior management is crucial given the importance and value of trade secrets.

- 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.

- Obtain comments on all draft documents and prepare final versions for inclusion in employee handbooks, etc. Comments are crucial to ensure that the documents are appropriately customized to the company's specific situation.

- Obtain authorization from board of directors to implement necessary physical security measures, including labeling and storage of trade secrets. Creating a culture of valuing and protecting trade secrets begins at the very top of the organizational hierarchy with the board.

- Conduct one or more training seminars for employees regarding trade secrets and the trade secret protection program, making sure that the presentation goes beyond reciting legal principles and addresses real questions that employees will have as they carry out their duties.

- If necessary, obtain executed employee confidentiality agreements from all employees.

- 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.

The company's trade secret protection program should be memorialized in a formal written statement. It can then be the basis for advising employees of their obligations with respect to the use and protection of such information. In addition, the existence of a written plan is persuasive documentary evidence that the company has taken affirmative steps to protect its trade secrets. The trade secret protection plan, which often takes the form of a security manual, generally includes a description and listing of the types of information considered to be a trade secret, along with a few examples of how protection might be lost for such items, and a detailed statement of the company's security procedures. The plan should also contain a clear statement of the "purpose" of the security program, which can be used as evidence of the company's diligence.

§ 7. Physical security measures

It is important for the trade secret owner to take a balanced approach to developing the protection program, since reliance on just one or two measures will generally not be sufficient. In some situations, the sufficiency of the measures taken will be analyzed with reference to the type of information and its economic value to the owner. Accordingly, while customer lists and records might reasonably be protected by the use of a locked filing cabinet and nondisclosure agreements, a secret manufacturing process may require protection by guards, as well as separation of the process to two or more different venues.

Companies should consider a variety of physical security measures calculated to limit access to trade secret information and to areas within the facility where such confidential information is housed. For example, to ensure that trade secret information is treated with the appropriate care, a company should physically separate the trade secret information, as well as any equipment used in a manufacturing process that is being protected as a trade secret, from other commonly used materials. Once the sensitive information has been placed in specified areas, the company must limit access to those who have a "need-to-know." Typical physical security measures include placing confidential information in locked cabinets and drawers, constructing fences and walls to prevent access to areas where trade secrets reside, marking trade secrets with an appropriate legend, and implementation of procedures to restrict the access of visitors to trade secrets within the facility.

Physical security measures should include procedures for the destruction of documents which contain confidential information which are no longer needed, as opposed to simply placing them in the garbage where they can easily be viewed, appropriated and copied. Access to trade secrets in the computer database should be restricted through passwords, changed regularly, and stored in locked cabinets with other confidential information. Special steps should be taken to erase such information whenever the computer is sold or a leased computer is returned to the lessor. Respect for the company's physical security measures must be impressed upon all employees. For example, employees should be reminded to store all notebooks and similar items in desks or filing cabinets, rather than leaving them in plain view of other employees or visitors. In addition, employees who have the right to inspect and use trade secret documents should be advised not to discuss the information outside of the restricted areas or with unauthorized personnel.

§ 8. Implementation of confidentiality procedures

Confidentiality procedures are central to protection of trade secrets and generally fall into four major categories: (1) document control; (2) procedures directed at computer use; (3) procedures directed at employees; (4) procedures directed at third parties outside of the company; and (5) protection of trade secrets obtained from third parties.

Beginning with "document control", it's important to recognize up front that the advent of photocopy machines, computers and mobile devices has made document control a difficult task. Nevertheless, measures can be taken to reduce the risk of misappropriation of trade secrets embodied in documents. The use of confidentiality legends is generally considered persuasive evidence that a company is taking the steps necessary to protect its trade secret information. Accordingly, the company should mark all documented trade secret information and records with prominent legends indicating that they contain sensitive information which must be maintained in confidence and instruct employees as to the meaning of that designation.

Another step that should be taken is to identify classes of documents that are important and then classify them according to the level of security required and mark them accordingly. For example, documents that may be shared with any company

employee may be classified and marked “Proprietary—Internal Use Only.” More sensitive documents may be classified and marked as “Proprietary—Need-To-Know.” These documents would consist of proprietary information that should be disclosed only to employees or others needing this information in order to carry out their jobs and respective tasks. Examples would include departmental budget information, organizational charts, performance reviews, market studies and market research. The most sensitive information may be classified and marked “Proprietary—Registered.” This information would include information that has the greatest value to the company, such as business plans, unreleased financial results of operations and information regarding new unreleased products. Information with this classification should be assigned a number for tracking purposes and not photocopied without the consent of the originator. Finally, the materials should be kept in locked cabinets when not in use.

Since computers have become common in the workplace procedures to protect the integrity and secrecy of the information stored on computers have taken on an added importance. Physical access to computers should be limited. Computer screens should have lock functions and employees should be instructed to log off if they will be out of their office for any length of time. Passwords and other data protection methods should be used as appropriate. Special caution should be taken with electronic mail. Unauthorized users can access electronic mail systems and it is easy to send electronic mail to the wrong address. Generally, more secure methods should be used when transmitting proprietary information.

With regard to “procedures directed at employees,” it is essential to alert employees to the necessity of protecting trade secrets and deterring inadvertent disclosure. Employees should be made aware of company policy regarding trade secret protection at the interview stage. Additionally, such policies should be made part of any company policy manual. Posters should be placed throughout the premises warning of the consequences to the company of disclosure of the company’s trade secrets. All employees should be required to sign confidentiality and assignment of invention agreements, a subject covered in detail in another program in this series, and when an employee terminates his/her employment, he/she should be required to turn over all company property including research, reports, drawings, blueprints, schematics, notebooks, and designs to his or her supervisor. The departing employee should also receive an exit interview during which the company should impress upon the departing employee his or her continuing obligations to the company.

“Procedures directed at persons outside of the company” follow from that fact that although “secrecy” is essential to demonstrate the existence of a trade secret, the owner of the trade secret must disclose the information to others—employees, customers, licensees, suppliers, and potential and actual joint venture partners—in order to obtain the maximum commercial benefit from the use of the trade secret. The reasonable use of a trade secret, including the controlled disclosure to employees and licensees, is consistent with the requirement of “relative” secrecy. There are several ways for a trade secret owner to disclose those secrets while preserving the right to prevent any subsequent unauthorized use and disclosure. Primarily, a disclosure must be pursuant to one of several “special relationships” which create an implied agreement on the part of the recipient not to disclose the information; secondarily, revelation of the trade secret may be pursuant to a written nondisclosure contract or agreement, which may be incorporated into a more comprehensive contract such as a license agreement covering the license of the trade secret to a third party. In order to bring an action for misappropriation, the trade secret owner must show the existence of a trade secret, proof of the unauthorized use or disclosure of the trade secret, and a confidential relationship between the parties.

Finally, a company may obtain the right to use valuable information which is being protected by a third party as its own trade secrets, such as under the terms of a license agreement. In such cases, the company is obligated to ensure that the third party’s trade secrets are not used or otherwise disclosed in an unauthorized manner. The duty of nondisclosure may be implied in certain cases; however, it is far more likely that a written nondisclosure agreement will be used. As a general rule, the company’s duties with respect to the protection of third party information will be limited to handling the information just as it would to protect its own trade secrets. However, since the forms of confidentiality agreements differ, a careful review of the actual requirements is required. Trade secrets obtained from third parties should be marked as confidential and treated with the same physical security measures as apply to the company’s own trade secrets.

§ 9. Review of public disclosures

It is important not to forget about the possibility of inadvertent public disclosure of trade secret information in repair manuals, customer handbooks, advertisements, trade shows, magazine articles, press releases, new product brochures, speeches and scientific publications. This documentation should be prepared well in advance of the proposed release or

publication date and reviewed to determine if it inadvertently discloses information to destroy the ability of the company to claim trade secret status. In addition, drawings, plans, or proposals prepared for prospective customers should be reviewed before delivery to ensure that they do not contain sensitive information such as tolerances of the steps to be followed in the manufacturing process.

Trade shows present particularly difficult issues, since competitors are likely to attend any presentation made by company personnel. Moreover, in many cases, sales personnel or public relations staffers are far more likely to make statements or create displays which inadvertently provide the information that an informed observer would need to fully understand a method or process which the company may have sought to maintain as confidential. Trade secret status can be surrendered when, for example, a competent engineer could reconstruct a manufacturing process using information that the trade secret owner disclosed to the public. Such public disclosures may appear in papers published by employees, films shown at engineering conferences, published photographs and in public speeches that included slides of the process. Accordingly, public presentations, including discussions by those staffing the company's trade show booth, should omit all references to trade secrets.

Employees who engage in sales and marketing activities have ongoing communications with third parties. These persons need to be diligent about the release of sensitive information. It is impossible for every employee to know whether or not the recipient has entered into an agreement with the company to maintaining the confidentiality of trade secrets. Information that is confidential or trade secret cannot be released without prior approval of appropriate company officials.