Protecting Trade Secrets from Employee Theft

Todd Presnell and Kara Shea

Todd Presnell and Kara Shea practice in the areas of employment and intellectual property law with the law firm of Miller & Martin LLP, a full service firm with offices in Atlanta, Nashville, and Chattanooga.

It is a problem many companies recognize only after it is too late—an employee with legitimate access to the intricacies of a company's software application or a company's technology-enhanced manufacturing process (for instance) abruptly leaves the company and accepts a job with a competitor. Many questions immediately arise: What property did the employee take? What software did the employee download? What trade secrets or other confidential or proprietary information will the employee provide to the new employer? What can we do to stop or slow the inevitable transfer of information?

Fears of misappropriation of confidential and proprietary information are further heightened when an employee has been terminated, since the negative feelings arising from the unpleasant end of the employment relationship could lead to a deliberate attempt to harm the former employer. In the current economic climate where periodic downsizing is an all too common occurrence, these fears are multiplied. Unfortunately, there are many ways that an entity's confidential information can be inadvertently disclosed, misappropriated, or outright stolen, including via improper disclosures by employees through customer or client relationships, through transmission of emails or Internet postings, or through corporate piracy such as computer hacking. Accordingly, before seeing these fears become a reality and finding itself asking the questions posed above, a primary question all companies should ask now is: What can we do as a proactive, front-end measure to prevent or at least limit the misappropriation of trade secrets or confidential or proprietary information by employees?

Fortunately, trade secret protection laws provide a remedy for misappropriation or disclosure of a company's secret, valuable business information. There are a variety of steps companies can implement to limit trade secret loss and secure legal remedies if an employee obtains and uses the company's trade secrets or discloses trade secrets to third parties.

What Are Trade Secrets?

As an initial matter, it is important for companies to understand the definition and scope of the term "trade secrets" as that term will ultimately be defined by courts or arbitrators determining whether actual misappropriation has occurred. Trade secret protection is a matter of state law; however, most states have a similar common law definition of what constitutes a "trade secret," typically defining this term to include "any information that can be used in the operation of a business or other enterprise that is sufficiently valuable and secret to afford an actual and potential economic advantage over others."[1] In addition, since 1979, the majority of states have adopted, in varying forms, the Uniform Trade Secrets Act, which defines "trade secrets" to include:

> Information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[2]

While this definition is admittedly convoluted, two themes may be derived for use in everyday business. First, trade secrets are broadly defined and global in scope; however, not every bit of information surrounding a product or process constitutes a protectable trade secret. For example, while the research and development information behind a software product generally constitute trade secrets, the method of implementing or using the finished product is generally not a trade secret. The key is whether the information if released would provide a competitive or economic advantage to the company's competitors. Assuming this criterion is met, there is no limitation on the scope of subject matter eligible for trade secret protection. Information need not qualify

for copyright or patent protection in order to constitute protectable trade secrets. Indeed, ideas, which are not protectable under any other theory of intellectual property law, may constitute protectable trade secrets.[3]

Companies should also know that not only scientific and technical information, but also financial, marketing, and other business information may constitute protectable trade secrets. For instance, a California appellate court recently held that information of a seller of locks related to pricing, profit margins, costs of production, pricing concessions, promotional discounts, advertising allowances, volume rebates, marketing concessions, payment terms, and rebate incentives had independent economic value and was useful to a competitor, and therefore could be classified as protectable trade secrets.[4] Other specific examples of materials held by courts to qualify as trade secrets include recipes[5] and preferred supplies for manufacturing a product,[6] as well as chemical formulas, manufacturing processes, product drawings and specifications, mechanical and electronic devices, instruction manuals, algorithms used in computer software, pending patent applications, results of quality control and product safety tests, projected capital investments, inventory, and (sometimes) customer lists.[7]

On the contrary, it is important to note that information that is easy to obtain, duplicate, or compile from sources available to the general public or competitors will not be entitled to protection. Customer lists are a good example of information that courts frequently find to be easily ascertainable from public sources and therefore nonprotectable. For instance, in *In re R & R Associates of Pinellas County, Inc.*,[8] a Florida bankruptcy court held that customer lists that could easily be compiled from telephone directories or other means are not protectable. Likewise, in *Lance Roof Inspection Service, Inc. v. Hardin*,[9] a Texas federal district court held that names of a roof inspection service's customers were either commonly known within the industry or easily ascertainable, and thus not entitled to protection against a former employee who had taken the company's customer list.

The second theme to derive from the definition of trade secrets set forth in the Uniform Trade Secrets Act is that information of whatever description will not be deemed a trade secret unless the company takes consistent steps to maintain the confidential nature of the information. It is difficult to argue that proprietary information of a company is a protectable trade secret when that company does not take measures to ensure that the information remains private. For instance, in *Gordan Employment, Inc. v. Jewell*,[10] a Minnesota appellate court ruled that business information did not constitute "trade secrets" when the company's customer list was kept in unlocked files in a public reception area without being labeled as "confidential," and when the company had not enacted a confidentiality policy. Similarly, an Alabama federal district court held that a pillow manufacturer could not limit the use of information by a former vice president when: (1) the information was kept in unlocked cabinets; (2) the information was not marked "confidential"; (3) the company did not communicate to its employees that proprietary information was to be kept confidential; and (4) the company did not require the vice president to execute confidentiality or non-compete agreements limiting the use of the information.[11] As these cases and myriad others make clear, it is in large part the company's actions that will deem information a trade secret worthy of protection.

Self-Protection

With these themes in mind, there are several steps a company can and should take in order to protect its trade secrets and proprietary information.

Employee Agreements

Probably the greatest fear is that a company's employees will gain access to and knowledge of its trade secret information, and subsequently leave to join a competitor and share those secrets. In the technology sector, many times a company's competitors are few and the loss of confidential information along with an important employee can be disastrous. As an Illinois federal district court recently observed when deciding whether to issue a preliminary injunction preventing a company's former employee from working for a competitor, "while [the former employee] may find another job, [the company] can never recoup the loss of their trade secrets."[12]

A comprehensive, written contract with the employee, however, can operate to prevent a damaging post-employment disclosure of a company's trade secrets, or at least limit the flow of confidential information, as well as provide for a legal remedy if the situation nevertheless occurs. In fact, the existence of employee agreements is often a critical factor in a court's determination of whether information is entitled to trade secret protection.[13] For instance, in *American Credit Indemnity Co. v. Sacks*,[14] a California court held that a customer list qualified as a trade secret when the company required employees to sign non-disclosure agreements. Similarly, in *Superior Flux & Manufacturing Co. v. H&S Industries, Inc.*,[15] an Ohio federal district court concluded that the fact that a company required its employees to sign "simple and understandable" confidentiality agreements favored trade secret protection for the company's proprietary information.

Important clauses in an employee agreement intended to protect trade secrets include the following:

Non-compete clause. These clauses, if carefully drafted, can prevent an employee from joining a com-

petitor for a certain period of time following termination of his or her employment with the company. Generally, these clauses should limit the employee's employment with a competitor for a certain period of time and/or within a certain geographical area. While clauses prohibiting an employee from ever working for a competitor are rarely enforceable, reasonable time and geographic limitations are. The scope of reasonable time and geographic limitations varies depending on the nature of the company's business. As a general rule, the longer the time period of the covenant, the more limited its geographic scope should be, and vice versa. For a company that provides Internet-based services, the issue of reasonable geographic scope of a non-compete is more complicated, as the geographic location of both the company and its customers may be irrelevant to the successful operation of the business. In certain situations, therefore, an agreement preventing the employee from working for any competitor for a limited period of time may be entirely reasonable.

If the company learns that an employee is contemplating joining a competitor, it is advisable to put the competitor on notice of the non-compete agreement. This is because, generally, a competitor must have actual or constructive knowledge of the employee's violation of duty to its former employer in order to be liable for use of the misappropriated trade secrets.[16] Accordingly, if the competitor has notice of the employer's non-compete agreement, but nevertheless disregards this notice and hires the employee, then a civil action may be maintained against the competitor.

Non-disclosure clause. Because a non-compete clause is necessarily limited, it is important for the company to also include in an employee agreement a non-disclosure clause. Such a clause should identify all categories of protected information and include the employee's contractual obligation never to disclose any such information to anyone outside the company—specifically competitors. The agreement should also require the employee to immediately report to the company all unauthorized uses or disclosures of the company's confidential and proprietary information. With this clause, an employee will be prevented from disclosing such trade secret information even after a non-compete time period expires. Moreover, such a clause prevents disclosure to non-competitors, which may not be covered by the non-compete clause.

While an employer may choose to limit non-compete agreements to top-level or highly compensated key employees, it should require all employees, from the CEO down to the lowest level clerical employees, to execute non-disclosure agreements. Similarly, while employers may choose (or be required, as a result of negotiation with a prospective employee) to include a clause in a non-compete agreement stating that it will not be enforced if the employee is laid off or terminated without cause, a non-disclosure agreement should clearly state that it will be strictly enforced throughout employment and thereafter, regardless of the reasons for termination.

Non-solicitation clause. If one fear is an employee leaving the company with proprietary information in tow, a greater fear is that a top-level employee will leave and then solicit other employees to join him or her either at a competitor or in a new entrepreneurial venture. Thus, it is important to provide a clause in an employee contract that prohibits an employee from soliciting other employees upon termination of his or her employment. Like non-compete clauses, non-solicitation clauses are generally enforceable for a certain period of time. Nevertheless, they should operate to prevent wholesale loss of employees.

Enforce All Agreements

Mistakes that employers commonly make are failing to enforce their employee agreements or engaging in selective enforcement of these agreements. The primary culprit in non-enforcement scenarios is overly broad agreements. That is, an agreement may cover information that is not really secret, confidential, or proprietary, and that would not harm the company if disclosed. Similarly, overzealous companies often require all employees, even low-level clerical workers, to execute extremely onerous non-compete agreements. In these situations, even when an employee leaves and goes to work for a competitor, in reality there will be no appreciable harm to the company. Thus, a company will simply ignore the breach rather than invest the time and significant financial resources necessary to enforce the agreement.

Another common scenario involves the departure of a long-term or well liked employee. In such cases, even when there is a real threat of harm to its protectable business interests, a company may ignore the breach of a non-compete or non-disclosure agreement simply out of sympathy for the employee. While arguably well-intentioned, such selective enforcement of employee agreements can have a negative impact on their long-term enforceability. For instance, the next time an agreement is breached, even if the company acts immediately to enforce the agreement, the departing employee will be permitted to discover how the company has handled past breaches. A company that has failed to enforce its agreements in the past may be deemed to have waived its protections. Even worse, the trade secrets that these agreements were designed to protect may be determined not to be trade secrets at all, due to the company's failure to treat them as such. For instance, in *Future Plastics, Inc. v. Ware Shoals Plastics, Inc.*,[17] a federal district court in South Carolina ruled that because a company did not object when its chief engineer left and started a competing company, it could not treat its processes as confidential and prevent other employees from going to work for competitors.

To guard against any claim that it has waived its ability to protect its trade secrets, a company should strictly scrutinize all employee agreements to make sure they cover only genuinely confidential and proprietary information that the company would be willing to go to court to protect. When preparing a non-compete clause, the company should ask itself whether this individual would truly pose a threat to the company if he or she went to work for a competitor. If the answer is "no," the company should skip the non-compete and simply require a non-disclosure agreement and, perhaps, a non-solicitation agreement. The bottom line is that a company should limit its employee agreements to terms that it is willing to consistently and vigorously enforce. And, most importantly, the company must follow up by taking appropriate action to address each and every breach of an employee agreement or other breach of confidence by its employees. The company must be willing to discipline, terminate, and litigate with employees over disclosure of trade secrets or other violations of employee agreements; otherwise, the execution of such agreements is, in the long run, a waste of time.

Maintain Internal Confidentiality

As mentioned above, whether information is deemed a trade secret is largely dependent upon how that information is treated by the company. If measures are not implemented to maintain privacy, then trade secrets may not be protected even if an employee misappropriates the information for his or her or others' economic advantage. Indeed, even a detailed and strict non-disclosure agreement will not help a company attempting to prevent disclosure of information that it has not otherwise treated as confidential. For instance, in *Hickory Specialties, Inc. v. Forest Flavors Int'l*,[18] a Tennessee federal district court held that even when an employee signs a contract promising never to divulge confidential information, the contract is enforceable only if the information qualifies as a trade secret—"that is . . . is actually a secret, business related, and affords a competitive advantage."[19] Or, in the words of a Massachusetts federal district court, a non-disclosure agreement between an employer and employee "cannot make secret that which is not secret."[20]

Thus, it is extremely important for the company to institute any measure possible to protect the confidentiality of its trade secrets. In addition to implementing the employee agreements outlined above, a company should also require vendors, customers, independent contractors, temporary employees, and all other individuals or entities having access to its confidential and proprietary information to execute non-disclosure agreements. Such agreements should prohibit all non-authorized disclosure to third parties of the company's confidential and proprietary information. The importance of close monitoring of all disclosures of confidential information to third parties is reflected in *Schlage Lock Company v. Ingersoll Rand Company*,[21] a recent decision issued by a California appellate court. In *Schlage*, the court held that, while a lock manufacturer's proprietary business information regarding sales and marketing of its products generally constituted protectable trade secrets, the company lost the right to claim trade secret status for certain pricing and marketing information that it had disclosed in a proposal submitted to a potential customer, Home Depot, without requiring the customer to sign a non-disclosure agreement.[22]

Other precautionary measures include keeping confidential materials in locked rooms and cabinets with access limited to employees who need the information for a specific purpose, stamping such information with a "CONFIDENTIAL" label, limiting computer access to such information to certain employees, establishing password protection on confidential files, limiting access to the company's network, restricting access to certain areas of the company's property (such as the area housing a manufacturing process), posting signs or warnings of confidentiality in sensitive areas of the company, and posting the non-disclosure policy on bulletin boards or the company's intranet. In addition, regular reminders of the company's confidentiality policy should be printed in the company newsletter and attached at the end of each email containing confidential information. A company may also wish to require employees to periodically re-execute non-disclosure agreements in order to keep its confidentiality policy and attendant obligations, as well as the penalties for disclosure, at the forefront of employee awareness.

Courts consider a company's efforts to inform employees of its confidentiality obligations not only in determining whether information subject to disclosure constitutes trade secrets, but also in balancing the interests of the company and former employees in a post-employment enforcement proceeding. For instance, in *Barilla America, Inc. v. Wright*,[23] the court was asked to grant an injunction to a company preventing its former plant manager from continuing his employment with a competitor when the evidence showed the employee might have disclosed the company's trade secrets. If an injunction issued, the former employee would be fired from his new position. In deciding to issue the injunction despite the resulting harm to the former employee, the court in *Barilla* relied primarily on evidence showing the former employee was well aware of his duty not to disclose confidential information of his former employer. In particular, the court noted that the company required all employees to sign an acknowledgement of receipt of the company handbook, which contained a fairly detailed confidentiality policy,

including a description of the employee's post-employment obligations.[24]

A company should take additional precautions any time it decides to terminate an employee. The employee should be immediately required to return all company property, including all computers or other equipment used remotely or at the employee's home, as well as files, memoranda, and notes in any form, including the employee's personal notes relating to employment.[25] The employee should be given only a short time to clean out his or her work area and should be supervised during this process, in order to limit the employee's opportunity to remove proprietary information. In order to prevent unauthorized copying of files, the hard drive of any computer used by the employee should be impounded. All files downloaded by the employee should be carefully checked. In the case of both voluntary and involuntary terminations, the company should have a final meeting or exit interview with the employee, informing him or her once again of the company's confidentiality policies. The employee should be reminded of any non-compete or confidentiality agreements he or she has signed, and should be instructed to contact the company immediately if any question arises regarding his or her post-employment confidentiality responsibilities.

Such procedures will not only discourage employees and others from gaining unauthorized access, but also serve as proof that the company considered such information to be a protectable trade secret. For example, in *Surgidev Corp. v. Eye Technology, Inc.*,[26] a manufacturer's list of ophthalmologists who were high-volume implanters of its lenses were held to be "trade secrets" that could not be disclosed by former employees. The court in *Surgidev*, applying California law, made this determination based on evidence that the manufacturer required employees to sign non-disclosure agreements, restricted visitor access to its sales and administrative headquarters, kept customer information locked in files, and distributed customer information data only on a "need-to-know" basis."[27]

Finally, a company that finds itself involved in any kind of litigation, whether as plaintiff, defendant, or witness, should request that a protective order be entered before it produces or discloses any confidential or proprietary information. The protective order should outline how confidential information may be used and disseminated during the course of the litigation and should include penalties for inappropriate disclosure, and should cover oral testimony as well as documents and other materials produced during the discovery process. The order should also provide that all materials containing confidential and proprietary information must be returned to the owner within a short period after resolution of the litigation. A well drafted protective order will not only protect a company's trade secrets during the course of litigation, but will also demonstrate that the company has taken all reasonable measures to guard the secrecy of its confidential and proprietary information. For instance, a California court held that the fact that a customer list was subject to a protective order in unrelated litigation was a key factor in the determination of whether the company had utilized all reasonable efforts to maintain confidentiality of the list.[28]

Legal Remedies

Of course, despite implementing all of these agreements and procedures, an employee may nevertheless misappropriate or misuse a company's trade secrets. There are legal remedies available, however, when such improprieties occur.

Injunction

In most occurrences the first step is to obtain an injunction from a court prohibiting the employee from, depending upon the circumstances, (1) working with a competitor, (2) disclosing or using trade secret information, or (3) soliciting other employees. If the employee agreements outlined above are in place, the injunction remedy has a much greater chance of success. Even if no agreements exist, however, the Uniform Trade Secrets Act, as adopted in most states, allows for an injunction to prohibit the disclosure of trade secret information. The key again is that the company has previously taken steps to ensure that trade secrets have remained confidential.

Monetary Remedies

In addition to or instead of obtaining an injunction, a legal action may be available when an employee gains access to and uses trade secret information to his or her economic advantage and the company's economic disadvantage. For example, the company victimized by misappropriation of trade secrets may obtain relief for a breach of the employee agreements' non-competition or non-disclosure clauses. Even if no such contracts exist, however, a legal action may still lie for the person's misappropriation under both a state's trade secrets act and the common law. It is well established that, even in the absence of a separate contract, a departing employee has certain ongoing duties to his or her former employer:

> Unless otherwise agreed, after termination of the agency, the agent: . . . has a duty to the principal not to use or disclose to third persons on his own account or on account of others, in competition with the principal or to his injury, trade secrets, written lists of names, or other similar confidential matters given to him only for the principal's use or acquired by the agent in violation of duty.[29]

Moreover, state trade secrets acts provide additional disincentive for post-employment breaches of confidence, allowing for monetary remedies, including attorney fees if the misappropriation is deemed to have occurred in bad faith or through willful and malicious conduct.

Conclusion

A company's trade secrets are typically among its most valuable assets, providing a competitive edge, which would disappear if this information were disclosed to competitors by a former employee. Indeed, misappropriation and disclosure of trade secrets to competitors could have a fatal impact on many businesses, particularly in the current economic climate. While remedies exist when employees misappropriate and use a company's confidential trade secret information, the optimum avenue for protecting these valuable assets is to implement proactive steps to protect confidentiality and prevent disclosure. Implementing these protective measures along with an unwavering commitment to enforcement should allay the fears of employee trade secret theft that many companies realize only after the loss is irreversible.

1. Restatement (Third) of Unfair Competition, § 39 (1995).
2. Unif. Trade Secrets Act, § 1(4).
3. *See, e.g.*, Timely Products Corp. v. Arron, 523 F.2d 288, 303 (2d Cir. 1975) (concepts related to construction of electrically heated socks, while not patentable, are subject to protection as trade secrets).
4. *See* Schlage Lock Co. v. Ingersoll-Rand Co., 101 Cal. App. 4th 1443, 1455–1456 (Ct. App. 2002).
5. *See* Mason v. Jack Daniel Distillery, 518 So. 2d 130, 133 (Ala. Civ. App. 1987) (recipe for "Lynchburg Lemonade" is a protected trade secret).
6. *See* Valco Cincinnati, Inc. v. N & D Machining Service, Inc., 492 N.E.2d 814, 818–819 (1986) (identity of materials used to manufacture glue applicator heads is a trade secret).
7. *See generally* Jay Dratler, Jr., Intellectual Property Law, Trade Secrets, § 4:02[3], pp. 4-25–4-26 (11th ed. 2001).
8. In re R & R Associates of Pinellas County, Inc., 119 B.R. 302, 304 (M.D. Fla. 1990).
9. Lance Roof Inspection Serv., Inc. v. Hardin, 653 F. Supp. 1097, 1103 (S.D. Tex. 1986).
10. Gordan Employment, Inc. v. Jewell, 356 N.W.2d 738, 740–741 (Minn. Ct. App. 1984).
11. *See* Alagold Corp. v. Freeman, 20 F. Supp. 2d 1305, 1315–1316 (M.D. Ala. 1998).
12. Barilla Am., Inc. v. Wright, 2002 U.S. Dist. LEXIS 12773 *14 (S.D. Ill. July 5, 2002).
13. *See, e.g.*, Schlage, 101 Cal. App. 4th at 1454 ("requiring employees to sign confidentiality agreements is a reasonable step to insure secrecy").
14. American Credit Indemnity Co. v. Sacks, 262 Cal. Rptr. 92, 97 (Ct. App. 1989).
15. Superior Flux & Mfg. Co. v. H&S Indus., Inc., 210 U.S.P.Q. (BNA) 669, 670 (N.D. Ohio 1980).
16. *See* Uniform Trade Secrets Act, §§ 1(2)(ii)(B) (II) & (III).
17. Future Plastics, Inc. v. Ware Shoals Plastics, Inc., 340 F. Supp. 1376, 1382 (D.S.C. 1972).
18. Hickory Specialties, Inc. v. Forest Flavors Int'l 26 F. Supp. 2d 1029, 1032–1033 (M.D. Tenn. 1998) (applying Tennessee law).
19. *Id.*
20. Lanier Prof'l Servs., Inc. v. Ricci, 192 F.3d 1, 5 (1st Cir. 1999) (applying Massachusetts law).
21. Schlage, 101 Cal. App. 4th at 1447, 1454–1455.
22. *Id.* at 1454–1455.
23. Barilla Am., Inc. v. Wright, 2002 U.S. Dist. LEXIS 12773 at * 15.
24. *Id.*
25. *See* Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc., 86 F. Supp. 2d 1102, 1106–1107 (D. Kan. 2000) (employee's personal logbook regarding his customer contacts that he kept while working for company was property of his employer, for purposes of determining if logbook was entitled to trade secret protection under Kansas Uniform Trade Secrets Act).
26. Surgidev Corp. v. Eye Tech., Inc, 828 F.2d 452 (8th Cir. 1987).
27. *Id.* at 455–456.
28. *See* Am. Credit, 262 Cal. Rptr. at 97.
29. Restatement (Second) of the Law of Agency, § 396(b) (1958). *See also* Eaton Corp. v Giere, 971 F.2d 136 (8th Cir. 1992) (Even where there is no contractual duty, employees have a common-law duty under Minnesota law not to use trade secrets or confidential information.).