9-1-1993

An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation

Derek P. Martin

Follow this and additional works at: https://digitalcommons.law.byu.edu/lawreview

Part of the Commercial Law Commons, Intellectual Property Law Commons, and the Torts Commons

Recommended Citation
Available at: https://digitalcommons.law.byu.edu/lawreview/vol1993/iss3/9

This Comment is brought to you for free and open access by the Brigham Young University Law Review at BYU Law Digital Commons. It has been accepted for inclusion in BYU Law Review by an authorized editor of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.
An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation

I. INTRODUCTION

As business and society become more dependent on technology, the importance of trade secrets increases. Today many companies depend on state trade secret law to protect their confidential information which provides them with advantages over their competitors. As competitive forces increase, so do the temptations to steal or misappropriate the trade secrets of a competitor. In 1984, the misappropriation of trade secrets was estimated to cost American firms close to twenty billion dollars annually.¹ In this intensely competitive business environment, it is critical that companies whose value depends on confidential information take affirmative, proactive steps to protect their trade secrets from misappropriation.

The scope of this comment is limited to misappropriation of a company’s trade secrets by the company’s current or former employees, and does not address issues that arise from theft of trade secrets by people outside the company. Employees typically have much easier access to an employer’s trade secrets than do outsiders. As a result, most measures taken to protect trade secrets from misappropriation by the company’s own employees should help protect those trade secrets from misappropriation by outsiders.

To analyze the threat of trade secret misappropriation by employees, legal issues such as which information can be protected as a trade secret and what constitutes misappropriation by an employee need to be addressed. These issues are analyzed herein by looking at the history and development of trade secret law. Special reference is made to the Uniform Trade Secrets Act (UTSA),² which has currently been adopted in thirty-seven states.³ The case law and the UTSA will allow a for-

². UNIF. TRADE SECRETS ACT, 14 U.L.A. 433 (1990) [hereinafter UTSA]. For the full text of the UTSA, see infra Appendix B.
³. See infra Appendix C for a list of states that have adopted the UTSA.
mulation of applicable standards for protecting an employer’s trade secrets.

Once the applicable rules and standards have been analyzed from the case law, a proactive strategy will be presented which will allow an employer to take affirmative steps to protect its vital trade secrets from employee misappropriation.

II. DEFINITION OF A TRADE SECRET

The definition of a “trade secret” has evolved over time, from its early common law origins, to a broadly accepted definition given in the Restatement of Torts, to a definition in the UTSA accepted by most states today.

A. Common Law Definition of a Trade Secret

Trade secret law has its origins in early common law, where one could be found liable in tort for disclosing confidential information in violation of a confidential employment relationship. Generally the decisions are framed in terms of protecting the property rights the employer has in its trade secrets.4

Legal scholars and case law agree that trade secrets still possess some attributes of property.5 The Supreme Court in Ruckelshaus v. Monsanto Co.6 held that confidential information recognized by state law as a trade secret is property protected by the Fifth Amendment.7 The Court compared trade secrets to other forms of property8 and concluded that trade secrets have sufficient property characteristics to warrant protection afforded to other forms of property. More recently, the Supreme Court in Carpenter v. United States9 reaffirmed that trade secrets have attributes of property that the law protects, stating that “[c]onfidential information acquired or compiled by a corporation in the course and conduct of its business is a species of property to which the corporation has the exclusive

---

5. ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01 (1986) (one can license, assign, or sell trade secrets; tax law treats trade secrets as property).
7. Id. at 1003-04.
8. Trade secrets have many characteristics of more tangible forms of property: they are assignable, can form the res of a trust, and can pass to a trustee in bankruptcy. Id. at 1002.
right and benefit."\(^\text{10}\)

While trade secrets do possess many of the attributes of property, they are also unique in many regards. Unlike other forms of property, the right to exclude others from using a trade secret depends on the owner's secrecy and the confidentiality she imposes on others. "[T]he value [of a trade secret] is in the information and the network of secrecy and confidentiality agreements created around it by its 'owner.'"\(^\text{11}\)

### B. Restatement of Torts Definition of a Trade Secret

The Restatement of Torts\(^\text{12}\) enunciates the most widely accepted definition of trade secrets in the common law. In summary, a trade secret is information which (1) is used in one's business, (2) provides a competitive advantage to its owner, and (3) is maintained in secrecy.\(^\text{13}\)

### C. Uniform Trade Secrets Act Definition of a Trade Secret

The UTSA was approved by the National Conference of Commissioners on Uniform State Laws in 1979, and amended in 1985.\(^\text{14}\) Since its approval it has been adopted by thirty-seven states,\(^\text{15}\) and its importance is therefore growing.\(^\text{16}\) In these states, the UTSA displaces any contrary provisions in the Restatement or the common law;\(^\text{17}\) however, the Restatement still provides guidance in interpreting the UTSA.\(^\text{18}\)

The UTSA definition of a trade secret is:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or poten-
tial, 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.19

An analysis of this definition shows that nearly any information can be characterized as a trade secret if it has independent economic value to its owner. The value of the information must derive from its secrecy, meaning that the information is neither generally known nor readily ascertainable.20 In addition, the owner must make reasonable efforts to keep the information secret.

D. Case Application of Trade Secret Law

Trade secret cases, whether they adopt the common law, Restatement, or UTSA definitions of trade secrets, are framed in terms of general concepts, not specific rules.21 These cases are highly fact-specific, and generally do not support a highly structured analysis. The court decisions in these cases flesh out the details of the applicable trade secret law, and the outcomes are heavily influenced by the underlying equities. For these reasons it is difficult to predict the outcome of a given case in a given circumstance. However, analyzing the body of case law does allow the extraction of certain principles which, if applied prudently by the owner of trade secrets, will more likely assure their protection from employee misappropriation.

III. WHAT INFORMATION CAN BE PROTECTED AS A TRADE SECRET?

"The threshold inquiry in every trade secrecy case is whether a legally protectable trade secret exists in fact."22 The existence of a trade secret is a question of law for the court.23

19. UTSA § 1(4), infra app. B.
20. The trier of fact has discretion to decide whether the information is generally known or readily ascertainable. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 900 (Minn. 1983).
21. See infra cases analyzed in parts III-VI.
To qualify as a trade secret, the information must (1) be the subject of a confidential relationship, and (2) have the requisite degree of secrecy.

A. Confidential Relationship

Trade secret protection generally depends on the existence of a confidential relationship in which a third party receives the secret under restrictions implied by law or imposed by contract. For most employees the law presumes a confidential relationship between employer and employee for the purposes of protecting trade secrets.

B. Secrecy

The UTSA requires that the information be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Notice that the standard is reasonable efforts to protect the secrecy of the information, not absolute secrecy. Courts have been careful to require only reasonable efforts, to keep the information

25. Id. ch. 3, pt. A (¶ 3.03-.05); see also id. ¶ 3.02[2] ("[Trade secret] protection exists only if actual secrecy and the expectation of continued secrecy and confidentiality have in fact been established and enforced.").
26. See Continental Data Sys., Inc. v. Exxon Corp., 638 F. Supp. 432, 442 (E.D. Pa. 1986) (holding confidentiality is required in employer-former employee actions); Engineered Mechanical Servs., 464 So. 2d at 333. The employee has a duty to treat the information as confidential insofar as the employer has so treated it. This means that if the employer fails to take reasonable efforts to assure security, no confidential relationship as to that information exists. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983).
27. The "employment relationship is one of confidence and trust and places upon the employee a duty to use his best efforts on behalf of his employer." C-E-I-R, Inc. v. Computer Dynamics Corp., 183 A.2d 374, 379 (Md. 1962) (citations omitted). Contra Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102, 1111 (E.D. Mich. 1975) (citation omitted) (holding that, in the absence of a contractual obligation not to use or disclose, no duty arose from the employment relationship itself that would prevent a chemist from using and disclosing secret chemical formulae developed by him in the course of his former employment).
28. UTSA § 1(4)(ii), infra app. B.
30. "[S]ecrecy need not be absolute; the owner of a trade secret may, without losing protection, disclose it to a licensee, an employee, or a stranger, if the disclosure is made in confidence, expressed or implied." Avtec Sys., Inc. v. Peiffer, 805 F. Supp. 1312, 1319 (E.D. Va. 1992) (quoting Dionne v. Southeast Foam Converting, 397 S.E.2d 110, 113 (Va. 1990)).
31. See Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180
secret. Secrecy can be established by showing that the information is novel and protected by adequate security.32

1. Novelty

For information to be protectable as a trade secret, the information must be novel, which simply means that the information cannot already exist in the public domain. A lack of novelty implies that the information will give no commercial advantage to the owner of the information. The level of novelty required for trade secrets is not the same level of novelty required for patents.33 However, a trade secret “must possess at least that modicum of originality which will separate it from everyday knowledge.”34 The level of novelty for trade secrets does not require that the individual elements of a trade secret must be new; a trade secret can lie in a new combination of known elements.35

The question of novelty is closely tied to the question of value. According to the UTSA, a trade secret “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.”36 If information is novel, it is not in the public domain and would then derive value “from not being generally known to” others. By the same analysis, if information is in the public domain, it is not novel and would therefore be of little value to the company that would try to protect this information since it is already widely known.
2. Security

Security procedures are prima facie evidence of reasonable efforts to keep the information secret, thereby allowing the information to qualify as a trade secret under the UTSA. A company should implement both internal and external security procedures to assure adequate protection of its trade secrets.\(^38\)

a. Internal security procedures. Internal security procedures are used to control dissemination of trade secret information within the company. Without a minimum level of effort to protect confidential information, the information will not qualify as a trade secret.\(^39\) To be reasonable, the employer's actions in preserving the secrecy of its confidential information must be at least reasonably equivalent to security measures generally followed in the industry.\(^40\) An internal security program should provide physical security against misappropriation by storing the confidential information in locked files or rooms, limiting access to the confidential information to a "need-to-know" basis, using employee badges to indicate clearance to access confidential information, and having armed guards on duty.\(^41\) One of the primary purposes of an internal security program is to provide clear notice to employees of proprietary claims to confidential information by placing signs and proprietary notices on all manuals, files, computers, and the like that are deemed confidential.\(^42\) The internal security program

---

38. The basic idea is that "[a] business is not entitled to protect allegedly secret information unless it undertakes itself to build that protection through reasonable security procedures." Nimmer, supra note 11, ¶ 3.05.

39. See Medline Indus., Inc. v. Grubb, 670 F. Supp. 831, 838 (N.D. Ill. 1987) (declining to enforce a covenant not to compete when the employer took little effort to protect the information it claimed as a trade secret).


41. Computer Assocs. Int'l, Inc. v. Bryan, 784 F. Supp. 982, 1000 (E.D.N.Y. 1992) (holding that physical security measures such as employee identification badges with name and photograph, magnetic card entrance restrictions, keeping certain internal facilities locked, requiring visitors to sign in at front desk, requiring visitors to be escorted by employee, and having security guards on duty in evening hours show appropriate efforts to secure confidentiality of trade secrets); Sigma Chem. Co. v. Harris, 605 F. Supp. 1253, 1256 (E.D. Mo. 1985) (holding that restricted access, armed guard and employee badges were "reasonable efforts").

should condition the receipt of proprietary information upon certain restrictions on future disclosure.\textsuperscript{43} An effective internal security program is strong evidence of the employer's "reasonable efforts" to protect the secrecy of its trade secrets.

\textit{b. External security procedures.} In addition to the internal security procedures outlined above, a company must also have external security procedures in place. External security procedures assure that trade secret status is not lost by carelessly disclosing trade secrets to parties that do not have a confidential relationship with the company. These procedures address the sale of products containing trade secrets, the publishing of news releases, manuals or brochures, and the dissemination of information to customers and other outside parties, with the goal of assuring that trade secret status is maintained by properly guarding the dissemination of any information that might contain trade secrets.

There are no quantitative guidelines as to what type of information can be disclosed to what number of parties before trade secret status is threatened. In one case, publication in manuals to almost 6000 persons did not destroy trade secret status, since the distribution was controlled and receipt of the manual was conditioned on acceptance of restrictions through confidentiality agreements.\textsuperscript{44} In another case, distribution to six large customers without requiring confidentiality agreements relinquished trade secret status even though intermediate dealers had executed confidentiality agreements with the trade secret owner.\textsuperscript{45} A company desiring to protect its trade secrets should carefully screen all products and literature that leave the company to assure that no confidential information is being carelessly disclosed, and should condition the disclosure of confidential information upon the receiver's signing a confidentiality agreement.

\begin{footnotesize}

\textsuperscript{44} See Data Gen., 357 A.2d at 107-08, 111.

\end{footnotesize}
PROTECTING TRADE SECRETS

IV. WHAT CONSTITUTES A MISAPPROPRIATION OF TRADE SECRETS?

The UTSA definition of misappropriation applicable to employees states:

"Misappropriation" means:

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use. . . . 46

According to this definition, misappropriation of trade secrets by an employee implies that the employee appropriated the trade secret by improper means. But what constitutes "improper means"? According to section 1(1) of the UTSA, "[improper means' includes theft . . . or . . . breach of a duty to maintain secrecy . . . ."47 For an employee, the definitions above both hinge on a duty to maintain secrecy.

Therefore, according to these UTSA definitions, the elements of a prima facie case for employee misappropriation of trade secrets are (1) disclosure of a trade secret without the owner's consent; and (2) at the time of disclosure, the employee knew or had reason to know she had a duty to maintain secrecy.

The employer has the burden of proof to establish these two elements,48 which are questions of fact that must be established by a preponderance of the evidence.49 Assume that the relevant information meets the definition of a trade secret given in Part II, and that the employee has disclosed this trade

46. UTSA § 1(2), infra app. B.
47. Infra app. B.
49. Hutter, supra note 48, at 9 (citing Draeger v. Welsh Sporting Goods Corp., 541 F.2d 790 (9th Cir. 1976), and other cases).
secret to a third party without the employer's consent, satisfying the first element of the prima facie case. To establish the second element of the prima facie case, the employer must show that the employee knew or had reason to know she had a duty to maintain the secrecy of the trade secret.

If the employer has evidence that the employee acted wilfully and knew that the taking of the trade secret was improper, the employer has established the second element of the prima facie case of misappropriation under the UTSA. Absent evidence of intent to misappropriate, the employer must show that the employee should have known she had a duty to not disclose the trade secret to others. The employer makes this showing by providing evidence that the employee was put on reasonable notice concerning both the information the employer regards as a trade secret and the employee's duties to keep this information confidential.

While the internal security measures referenced above put all employees generally on notice, the employer makes a much stronger case by showing that the individual employee in question was specifically put on notice. This is easily shown if the employee signed a nondisclosure agreement.

The purpose of a nondisclosure agreement is to give specific notice to the employee of her duties in regards to trade secret information to which she is exposed during her employment, and to create a covenant that the employee will not disclose any of the employer's trade secrets in the future. Some courts may deny relief if no nondisclosure agreement exists.

The employee may have a strong defense if she was instrumental in developing the trade secrets in question. If the trade secret is brought into being through the initiative of the employee, no duty arises since the employee may then have an interest in the subject matter at least equal to that of her employer.

50. Supra notes 39-43 and accompanying text.
53. When developments are the product of an employee's own skill, without

Proving misappropriation by a former employee is generally more difficult than proving misappropriation by a current employee, because of the interest the employee has in working in her trade and the interest of society in assuring both the free flow of information and the mobility of employees. For former employees, in addition to the prima facie misappropriation elements listed above, the courts also consider whether the knowledge used is truly a trade secret or merely general knowledge and whether disclosure violates an agreement not to compete. These additional considerations are discussed in the following sections.

A. I s t h e F o r m e r E m p l o y e e U s i n g T r a d e S e c r e t s o r G e n e r a l K n o w l e d g e?

The first inquiry is whether the employee is using a trade secret from her former employer, or whether the employee is simply drawing on general knowledge gained through experience in her field. As a general rule, "an employee upon terminating [her] employment may carry away and use the general skill or knowledge acquired during the course of the employment."54 Relevant to this inquiry is whether the employer's trade secrets were pointed out with particularity and distinguished from general knowledge. Pointing out trade secrets with particularity allows protection of the employer's trade secret without preventing the employee from using her general skills and knowledge.55 If trade secrets are not specifically distinguished by the employer from general knowledge, the employee has reason to believe that any skill or knowledge appreciable assistance by her employer, she has an unqualified privilege to use and disclose the trade secrets so developed. Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102, 1112 (E.D. Mich. 1975). However, if the employer supported the development of the trade secret, asserted rights to the trade secret, and invested in the development with an intent to commercially exploit the trade secret, the employee is deemed to have reasonable notice that the information was a trade secret. See id.


55. See generally J & K Computer Sys., Inc. v. Parrish, 642 P.2d 732 (Utah 1982) (describing computer programs and methods as trade secrets and listing other precautions that entitled them to protection).
acquired becomes part of her general background. The internal security procedures referenced in Part III.B.2.a should be designed to give the employee reasonable notice of the specific information that the employer claims as a trade secret.

B. Does the Disclosure Violate a Covenant Not to Compete in the Employment Contract?

The next inquiry is whether the disclosure of confidential information by the former employee violates a noncompetition clause or covenant not to compete in the employment contract between the former employee and the employer. The general purpose of such covenants is to eliminate close questions of fact when an employee accepts employment from a competitor. A covenant not to compete is not strictly necessary, since a former employee can be prohibited from disclosing trade secrets belonging to her former employer whether or not there exists an employment contract with such a covenant. But the existence of a covenant with specific terms and conditions strengthens the employer's case. Under the terms of a reasonable covenant, the former employee is free to compete so long as the employee does not use any confidential information of her former employer.

It is critical to check the particular state law regarding the use of covenants not to compete, since many bar or restrict such covenants by statute. The most frequently permitted exception, however, is for trade secrets.

In some special circumstances the court will not enforce the covenant not to compete. For example, if the employee

56. See Dynamics Research, 400 N.E.2d at 1286-87; Jostens, Inc. v. National Computer Sys., Inc., 318 N.W.2d 691, 701-02 (Minn. 1982).

57. A former employee may be held liable for misappropriation even if she attempts to avoid using the trade secrets of her former employer and, in fact, may not have been consciously aware that she was misappropriating the secret information. Integrated Cash Management Servs., Inc. v. Digital Transactions, Inc., 732 F. Supp. 370, 377-78 (S.D.N.Y. 1989), aff'd, 920 F.2d 171 (2d Cir. 1990).


lacks bargaining power, the court may find the covenant to be a contract of adhesion. But a covenant not to compete is generally enforceable if consideration is given by the employer to the employee in return for the covenant and if the covenant is substantively reasonable, as discussed below.

1. Consideration for a covenant not to compete

Consideration for a covenant not to compete is presumed if it is signed as part of an employment contract when the employee begins working for the employer. In return for the covenant, the employer is providing employment for the employee; the employment provides the necessary consideration to support the covenant. If the agreement not to compete arises after the employee is hired, the court may require additional consideration from the employer.

2. Substantive reasonableness of covenants not to compete

An enforceable covenant not to compete must reasonably balance the interest of the employer in protecting its trade secrets with the employee's interest in using her skills and training in future employment. The more specific the covenant is and the more narrowly it is tailored to the employer's needs, the more likely a court is to enforce it. A covenant not to compete is not enforceable if its purpose is to prevent competition rather than to protect the employer's confidential information. Courts will only enforce a covenant if it does not "impose upon the employee any greater restraint than is reasonably necessary to protect the business and good will of the employer." The reasonableness of the restraint is analyzed

---

62. See Modern Controls, Inc. v. Andreakis, 578 F.2d 1264, 1267 n.5 (8th Cir. 1978).
63. See, e.g., Stevenson v. Parsons, 384 S.E.2d 291 (N.C. Ct. App. 1989). See generally Fernando S. Tinio, Annotation, Sufficiency of Consideration for Employee's Covenant Not to Compete, Entered into After Inception of Employment, 51 A.L.R.3d 825 (1973) (Some courts hold that new consideration is required to make a noncompetition clause enforceable against existing employees.).
64. Nimmer, supra note 11, ¶ 3.10[3][a].
in terms of its scope of prohibited activity, geographic scope, and duration, as discussed more fully below.

a. Scope of the prohibited activity. A covenant not to compete is only enforced to the extent that the scope of the activity restrained is reasonable. If the employee can work for a competitor without disclosing trade secrets, the covenant will not be enforced. To ensure the enforceability of a covenant not to compete, the scope of the prohibited activity must be very narrowly limited to the activity the employee performs for the employer.

b. Geographic restrictions. The area in which the employee is restrained from working her trade must be reasonable, i.e., no broader than necessary to protect the employer. There is no consensus as to how broad or narrow the geographic restrictions must be to pass judicial review, but the reasonableness of the restriction may depend on many factors, including the nature of the business, the geographic scope of its operations, and the nature and scope of the competition. Illustrating the widely divergent views, one decision held that a restriction on competing within a fifty-mile radius of any city with a profit center of the former employer was too broad, while another decision enforced a nationwide restriction. While drawing bounds on enforceable geographic restrictions is very difficult, it is clear that restrictions in a covenant not to compete that are unlimited in geographic scope are generally considered "not necessary to protect any valid interest of the former employer and are unreasonable restraints of trade."

10 (Tex. Ct. App. 1988) (citing Weatherford Oil Tool Co. v. Campbell, 340 S.W.2d 950, 951 (Tex. 1960)).
68. See Trilog Assocs., Inc. v. Famularo, 314 A.2d 287, 294 (Pa. 1974) (invalidating a covenant not to compete covering employment unrelated to the work the employee performed for the employer as a "completely unreasonable restraint of trade").
70. NIMMER, supra note 11, § 3.10[3][b].
c. **Duration.** The duration of the covenant not to compete must be no longer than is necessary to protect the employer's interest. Failure to align the duration of the covenant to the valuable life of the information may lead to a voiding of the covenant.\(^{74}\)

VI. **REMEDIES FOR TRADE SECRET MISAPPROPRIATION**

The remedies at the disposal of an employer for employee misappropriation of trade secrets include criminal prosecution, injunctive relief, compensatory and punitive damages, and attorney's fees.

A. **Criminal Prosecution**

Misappropriation of trade secrets is generally thought of as a civil action, with criminal indictments for theft of trade secrets being "really unusual."\(^ {75}\) In recent years, however, many states have passed statutes that specifically provide for criminal penalties for trade secret misappropriation.\(^ {76}\) Recent cases indicate that the courts are increasingly willing to hand down indictments\(^ {77}\) and convictions\(^ {78}\) based on misappropriation of trade secrets. An employer may, therefore, be able to pursue criminal prosecution of an employee or former employee whose conduct falls within the scope of applicable criminal statutes.

B. **Injunctive Relief**

If the disclosure of the trade secret has been limited, injunctive relief is useful to stop the damage that widespread disclosure would cause. In addition, injunctions prevent compa-
nies using misappropriated trade secrets from profiting from their misappropriation. The UTSA provides for injunctive relief which encompasses both preliminary and post-judgment injunctions. Injunctive relief should be tailored to specifically address the harm that the plaintiff alleges.

1. Preliminary injunctions

Preliminary injunctions are considered extraordinary and drastic remedies. The criteria for granting a preliminary injunction for trade secret misappropriation is the same as for granting a preliminary injunction in any other civil action. The plaintiff must show "(1) . . . a clear right or interest needing protection; (2) . . . no adequate remedy at law; (3) irreparable harm . . . ; and (4) . . . reasonable likelihood of success on the merits." In addition, some courts also compare the irreparable harm to the plaintiff without the injunction to the harm to the defendant if the injunction is granted and consider the effect of the injunction on the public interest. A preliminary injunction may lead to a post-judgment injunction if the employer prevails on the merits at trial.

2. Post-judgment injunctions

The criteria for granting post-judgment injunctions are generally the same as for granting preliminary injunctions. The primary question is how long the post-judgment injunction should last. The predominant view limits the duration of the post-judgment injunction to the period that would be required to reverse-engineer the trade secret (known as the "head

79. UTSA § 2, infra app. B.
81. PCx Corp. v. Ross, 522 N.E.2d 1333, 1338 (Ill. App. Ct. 1988) (citing several cases). The element of irreparable harm is usually considered the most important element, and according to the Second Circuit, "the loss of 'trade secrets' is not measurable in terms of money damages . . . and is thus considered 'irreparable harm.' Computer Assocs., 784 F. Supp. at 986; see also Xerographics, Inc. v. Thomas, 537 So. 2d 140, 143 (Fla. Dist. Ct. App. 1989) ([I]rreparable injury is presumed where there is a violation of a noncompetition agreement.)" (citation omitted).
start” period), on the theory that the person who misappropriated the trade secret should be enjoined from using that secret only for the period of time before which the trade secret could have been fairly appropriated. An alternative view of post-judgment injunctions allows more extended, even permanent relief if the defendant’s conduct is egregious and willful.\(^{84}\)

The UTSA adopts an intermediate approach,\(^{85}\) favoring removal of the injunction after the “head start” period has expired, yet allowing the extension of the injunction for an additional reasonable period to eliminate any commercial advantage for the wrongdoer. If the employer can make the requisite showing to have a post-judgment injunction granted, the duration of the injunction may range from the “head start” period, at a minimum, all the way up to permanent relief, depending on the specific circumstances.

C. Damages

Compensatory damages can generally be recovered in cases where trade secret misappropriation by employees is shown. Punitive damages may also be available depending on the employee’s conduct and the conduct of her new employer, both of whom are generally defendants in the misappropriation action.

1. Compensatory damages

Compensatory damages are intended to compensate the trade secret owner for the loss sustained as a result of the misappropriation of the trade secret by the defendant. In measuring compensatory damages, the court may consider the trade secret owner’s loss, the defendant’s gain, or both.\(^{86}\) Using the loss to the trade secret owner as the appropriate measure emphasizes the compensatory character of this remedy.\(^{87}\)


\(^{85}\) See UTSA § 2, infra app. B. The UTSA formulation for injunctions is similar to that used in Analogic Corp. v. Data Translation, Inc., 358 N.E.2d 804, 808 (Mass. 1976).

\(^{86}\) UTSA § 3(a), infra app. B, states “a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss.”

\(^{87}\) See Sperry Rand, 311 F. Supp. at 923; Computer Print Sys., Inc. v. Lew-
In many situations, however, the loss to the trade secret owner is difficult to quantify or estimate. As a result, some courts look to the defendant’s gain to calculate damages. This gain to the defendant can be measured by either the defendant's profits from the misappropriation or the estimation of a fair price for a license to use the trade secret at the time the misappropriation occurred.

Each of the methods outlined above for calculating the amount of compensatory damages involves some measure of uncertainty which is often substantial. The lack of certainty, however, is not grounds for denying compensatory damages. "[I]t is the fact of damages, rather than the amount of damages, which must be proven with reasonable certainty." A trade secret owner, therefore, may still be awarded damages that are somewhat speculative and uncertain provided it makes a clear showing that it has suffered some damage.

2. Punitive damages

Punitive damages are available in trade secret misappropriation cases only if the defendant acted "wantonly, wilfully, or in reckless disregard of the plaintiff's rights," if the defendant's conduct was flagrant, or if the defendant's conduct was malicious. While punitive damages may be allowed in these circumstances, they cannot be excessive. If the employee's conduct in misappropriating the trade secret was willful, the employer should seek punitive damages in addition to compensatory damages.

92. Telex, 510 F.2d at 933.
D. Attorney’s Fees

The UTSA allows payment of attorney's fees to the prevailing party “[i]f . . . a claim of misappropriation is made in bad faith, . . . a motion to terminate an injunction is made or resisted in bad faith, or . . . willful and malicious misappropriation exists.” If the employer can show bad faith on the part of the defendant, the employer should move for the payment of attorney’s fees.

VII. PROACTIVE EMPLOYER ACTIONS TO ASSURE TRADE SECRET PROTECTION

Once an employer discovers that its trade secrets have been misappropriated by an employee or a former employee, history has locked in the events of the past, and the only remedy for the employer is to secure good counsel and litigate the matter. Many employers learn harsh lessons through expensive and unsuccessful litigation which could be avoided by implementing a proactive plan for protecting trade secrets before misappropriation occurs.

The objectives of a proactive plan to protect trade secrets are (1) to establish and provide evidence of a confidential relationship with employees, and (2) to establish and provide evidence of security over trade secrets through “reasonable efforts.”

The employer should embark on a two-phase process to prove the requisite level of confidentiality and security. The first phase is an initial trade secret review, where the employer evaluates the present need to protect trade secrets and institutes procedures to protect trade secrets from misappropriation. These procedures are drawn from the case law dealing with trade secret misappropriation, discussed in Parts II-VI above, to assure that the employer has a solid legal position should misappropriation occur. The second phase is to hold periodic trade secret audits to adapt the system for protecting trade secrets according to changing needs.

95. UTSA § 4, infra app. B.
96. See supra parts III.A-B.
A. Initial Trade Secret Review

1. Identifying and classifying confidential information

The first step in the initial trade secret review is to form a committee to protect the company's confidential information by selecting one or more individuals to coordinate and control the trade secret protection program. The company's legal counsel should be included as a member of this committee to assure that the committee is apprised of new developments in the applicable state trade secret law.

Once this committee is formed, its first task is to identify and list what company information deserves protection as confidential or proprietary. A strong sense of company pride may tempt the committee to be overinclusive, identifying more information as confidential than is necessary. Being overinclusive is risky, since this may put the status of the actual trade secrets in jeopardy if they are mixed with information that is not truly confidential. As a result, the committee should be very careful to limit the classification of confidential information to information that is truly confidential or proprietary.

Once the list of confidential and proprietary information has been compiled, the committee must then determine what level of security should be applied to each item on the list. Some suggested levels of security are indicated below, according to the impact on the employer if the information were disclosed outside of the company:

1. Critical—disclosure would be devastating
2. Top Secret—disclosure would be damaging
3. Secret—should be considered a trade secret

98. Epstein & Levi, supra note 1, at 902; see Motorola, Inc. v. Fairchild Camera & Instrument Corp., 366 F. Supp. 1173, 1185 (D. Ariz. 1973) (holding that employees were under no duty not to disclose alleged trade secrets when the employer did not specifically identify which information was considered secret).
99. Epstein & Levi, supra note 1, at 902-03 (if a corporation fails to implement an over-ambitious plan, the court may find that none of the protected information are trade secrets).
100. "Marking everything as 'secret' may be construed by the courts as lack of guidelines for employees using the data." Mills, supra note 97, at 104.
101. Id.
4. Confidential—secrecy is preferred\textsuperscript{102}

Once the information to be protected is identified with the appropriate level of security, the committee must implement security procedures to protect this information.\textsuperscript{103}

2. \textit{Implementation of security procedures}

Security procedures as discussed in Part III.B.2 must be implemented by the committee to assure that the employees have a confidential relationship with the employer with regards to the employer's confidential information, and to assure that adequate security measures are in place to protect the secrecy of that information.

\textit{a. Employee awareness program.} The committee should implement an employee awareness program—based on the information from the case law\textsuperscript{104}—to inform employees of their duties regarding trade secrets and other confidential information. The first step is to require entry interviews for all new employees that may have access to trade secrets or other confidential information during their employment.

During the entry interview, the interviewer (a committee member) should inform the employee that she will have access to trade secrets, and specifically give notice of her obligations toward the employer in regard to those trade secrets. The interviewer should inform the employee that her employment and exposure to confidential information are conditioned on her acceptance of restrictions in disclosing the information to others. In addition, the interviewer should inform the employee that she has a duty not to disclose any trade secrets she may have learned at previous employers during her employment with this company. This will strengthen the employer's case should the company be sued for misappropriation of trade secrets after hiring an employee of a competitor. The final step in the entry interview is to have the employee sign a nondisclosure agreement which memorializes all the information given in the entry interview and reaffirms the employee's duty and agreement to not disclose the employer's confidential information. The nondisclosure agreement should be carefully drafted

\begin{itemize}
\item \textsuperscript{102} \textit{Id.}
\item \textsuperscript{103} Epstein & Levi, \textit{supra} note 1, at 902.
\item \textsuperscript{104} \textit{See supra} part III.B.2.
\end{itemize}
so its provisions are "reasonable in the industry, both as to
duration and geographic application."^{105}

The entry interview process works well for giving notice to
new employees of their duties regarding the company's confi-
dential information, but measures also need to be taken to give
notice to existing employees of their duties as well. All existing
employees that have access to trade secrets should sign the same
nondisclosure agreement used for new employees. The
advantage of having an existing employee sign a nondisclosure
agreement is that it may specifically identify the projects the
employee has worked on which contain trade secrets. However,
one problem with having existing employees sign a nondisclo-
sure agreement is that some courts hold that, absent separate
consideration, these types of employee agreements are not
binding.^{106} The sure solution to this problem is to give the
existing employee new consideration at the time she signs the
nondisclosure agreement. This new consideration could be a
promotion, a raise, stock options, or various other forms of non-
ominal consideration.^{107}

The employee nondisclosure agreement should have specific
elements and provisions whereby the employee acknowledges
the following:

1. She has access to trade secrets^{108}
2. The company is sufficiently protecting these trade se-
crets^{109}
3. She has not and will not disclose or misappropriate the
trade secrets^{110}
4. She will report to the company all unauthorized disclo-
sures or uses of the trade secrets^{111}
5. Employment with the company creates a relationship of

^{105} Micro Plus, Inc. v. Forte Data Sys., Inc., 484 So. 2d 1340, 1342 (Fla.
Dist. Ct. App. 1986). For more detailed treatment of drafting nondisclosure agree-
ments and covenants not to compete, see Christopher H. Mills, Drafting Employ-
ment Agreements: Practical and Legal Considerations, in HANDLING CORPORATE

^{106} See Jostens v. National Computer Sys., 318 N.W.2d 691, 703-04 (Minn.
1982). Nondisclosure agreements are similar to noncompetition clauses, which are
discussed in Tinio, supra note 63, at 829-39.

^{107} Accord Tinio, supra note 63, at 829-39.

^{108} Epstein & Levi, supra note 1, at 905.

^{109} Id.

^{110} Id.

^{111} Id.
confidence and trust between the employee and the company with respect to any confidential information.\textsuperscript{112}

6. She understands the definition of proprietary or confidential information, which includes examples of the confidential information to which the company is claiming rights, including trade secrets, processes, formulas, computer programs, data, know-how, inventions, improvements, techniques, marketing plans, product plans, strategies, forecasts and customer lists.\textsuperscript{113}

7. She expressly assigns all rights to the company's confidential information to the company.\textsuperscript{114}

8. She covenants not to disclose any of the company's confidential information.\textsuperscript{115}

9. She covenants to deliver any materials, documents and data of any nature containing or pertaining to confidential information when her employment terminates, and covenants not to take any such information with her when she leaves.\textsuperscript{116}

Rather than being a separate agreement, the nondisclosure agreement could be included in an overall "Employment Contract," which could include other clauses and provisions, such as covenants not to compete.\textsuperscript{117} In this manner all employees that have access to confidential information would be required to sign a covenant not to compete as a portion of their employment contract. As explained in Part V.B.2, the covenant not to compete needs to be narrowly tailored in the scope of activity, the geographic restriction, and the duration of the restraint. A covenant not to compete that is narrowly tailored to protect an employer's legitimate interests will be enforced by the courts, while covenants that are overbroad are routinely deemed unenforceable.\textsuperscript{118}

The company should also clearly assert its rights in its


\textsuperscript{113} Id.

\textsuperscript{114} Id.

\textsuperscript{115} Id.

\textsuperscript{116} Id.

\textsuperscript{117} Nondisclosure agreements and covenants not to compete are appropriate ways of protecting proprietary information in an industry that cannot use patents and trademarks to protect research and development because they take considerable time to obtain. Id.

\textsuperscript{118} See supra notes 65-74 and accompanying text.
confidential information. A good first step is to publish a written statement of the company's security policy towards trade secrets in a company security manual.119 This statement should include a general definition of what the company considers confidential information,120 an assertion of the company's rights to its confidential information, examples of how trade secrets may be lost,121 and an overview of the company's policy for maintaining secrecy of confidential information.122 In addition, clear markings on all confidential information will give notice to employees of the employer's asserted rights in this information.123 The company should also document an intent to exploit a market when developing any product or process that may involve trade secrets, since this tends to prove that the trade secrets have value to the company.

The committee should also limit access to confidential information to those who have a "need to know",124 this provides further notice to employees regarding which information is confidential. Limiting access can be accomplished by monitoring all employees that are given access to confidential information,125 and by numbering copies of secret documents and logging their locations.126

A final procedure in the employee awareness program is to institute exit interviews.127 During the exit interview the interviewer (a committee member) should identify in writing all trade secrets that the employee has worked with, and reaffirm the employee’s duty of confidentiality by having the employee sign a copy of the original nondisclosure agreement and covenant not to compete which she signed previously. This does not require any consideration since the employee is simply reaffirming covenants and promises made at an earlier date.128 A

120. Id.
121. Id.
122. Id.
123. The company should assure that the information marked confidential is treated as confidential; otherwise, the information may lose its trade secret status. See Combustion Eng'g, Inc. v. Murray Tube Works, 222 U.S.P.Q. (BNA) 239 (E.D. Tenn. 1984).
126. Mills, supra note 97, at 104.
128. Some employers require employees to sign a "Termination Agreement"
final precaution at the exit interview is to procure the name and address of the employee's new employer (if known), and follow up with a letter to the new employer asserting rights to the company's confidential information the employee learned during her employment.\textsuperscript{129} This puts the new employer on notice of the company's rights to its trade secrets and other confidential information.

If the steps outlined above are followed, the employees will be well informed of their duties and the employer's rights to confidential information. These combined efforts will tend to strongly establish a confidential relationship between the employer and the employee. The remaining task is to prove that the employer took reasonable efforts to keep the information secret by taking reasonable security measures.

\textit{b. Security program.} The security procedures outlined in Part III.B.2 tend to show that the employer is taking reasonable efforts to protect its trade secrets. Security procedures which will influence the court to find that the employer has expended reasonable efforts include physical separation of confidential information from nonconfidential information\textsuperscript{130} and restricted access to confidential information. Access may be restricted by the following:

1. Locked gates
2. Locked cabinets
3. Security guards\textsuperscript{131}
4. Procedures for checking safeguards before going home\textsuperscript{132}
5. Employee identification badges\textsuperscript{133}
6. Proper disposal of confidential information\textsuperscript{134}

\textsuperscript{129} See Cybertek Computer Prods., Inc. v. Whitfield, 203 U.S.P.Q. (BNA) 1020, 1025 (Cal. App. Dep't Super. Ct. 1977) (employee received letter from former employer, of which current employer was informed).

\textsuperscript{130} Epstein & Levi, \textit{supra} note 1, at 906.


\textsuperscript{132} Epstein & Levi, \textit{supra} note 1, at 908.

\textsuperscript{133} \textit{E.g.}, Mills, \textit{supra} note 97, at 104.

\textsuperscript{134} Documents containing confidential information should be shredded when
7. Appropriate computer security\textsuperscript{135}
8. Restricted access to visitors\textsuperscript{136}

These procedures should be tailored according to the appropriate level of security identified in the initial trade secret review—i.e, critical, top secret, secret, or confidential.\textsuperscript{137} In addition, the company should also take steps to assure that confidential information is not inadvertently disclosed, thereby destroying the trade secret status of that information. This can be accomplished by instituting a procedure for screening the content of all speeches, press releases, and other publications\textsuperscript{138} before releasing them to sources outside of the company. One committee member should be appointed to screen all external communications to assure that no confidential information is being disclosed.

B. \textit{Trade Secret Audits}

A trade secret audit is defined as "a periodic, formal review of trade secret information and materials and the procedures that are being used to protect them."\textsuperscript{139} Such an audit should be carried out at least once per year.

1. \textit{Benefits}

The benefits of holding trade secret audits include the following:

1. Reducing the cost of trade secret litigation by encouraging potential defendants to settle and by preventing further

\textsuperscript{136} The company should restrict plant tours that might reveal confidential information, Epstein & Levi, \textit{supra} note 1, at 909, and should require an employee escort for all visitors, Sigma Chem. Co. v. Harris, 605 F. Supp. 1253, 1256 (E.D. Mo. 1985).
\textsuperscript{137} \textit{See supra} notes 101-103 and accompanying text.
\textsuperscript{138} \textit{See} Epstein & Levi, \textit{supra} note 1, at 910-11.
\textsuperscript{139} \textit{Id.} at 898.
breaches of security during trial

2. Strengthening the company's litigation posture by proving that the company took affirmative security steps to establish the trade secret

3. Promoting cost efficiency by reducing or preventing trade secret leaks

4. Demonstrating to employees leadership and control at the management level

5. Increasing employee morale by demonstrating that the company values the employee's work and is willing to take appropriate steps to protect it

2. *Trade secret audit procedure*

The primary purpose of the trade secret audit is to reevaluate the system for protecting confidential information and to determine if changes are needed. The trade secret audit should specifically evaluate whether the geographical scope of operations for the company has changed; this may require modifications to the employee nondisclosure agreements and covenants not to compete to assure they will be effective and enforceable in court. The trade secret audit should also assure that the company's security measures are well balanced and specifically aimed at protecting the employer's legitimate interests in its confidential information. The trade secret audit should also assure that periodic employee meetings are held to review the employee obligations in regards to confidential information.

In addition, the trade secret audit should attempt to anticipate new business developments which the company is exploring to ensure that any new developments are adequately protected. Trade secrets that are no longer valuable should be terminated, meaning that they should be moved from the area where confidential information is stored and placed with the nonconfidential information. While this may seem relatively unimportant, the proper termination of trade secrets demonstrates the company's commitment to tailoring its programs for the purpose of carefully guarding its trade secrets and other confidential information.

The company counsel should come to the trade secret audit

140. *Id.* at 899-900.
141. *Id.* at 902.
prepared to discuss any relevant changes in the state trade secret laws or precedents which might affect the company, along with suggested modifications to the company’s procedures to assure continued compliance with state law requirements for the preservation of trade secret rights. In accordance with these potential changes, the scope of the company’s nondisclosure agreements and covenants not to compete should be carefully scrutinized to assure that the restrictions therein comply with the current state of the law and the current operations of the company. It would even be desirable to have the employees involved on new projects sign new nondisclosure agreements at the time of the trade secret audit. The agreements should specifically identify the new project and reaffirm the employee’s duty to not disclose any confidential information relating to the new project.

VIII. CONCLUSION

Companies in the United States lose billions of dollars each year through the misappropriation of trade secrets. Although the applicable trade secret law in the various states is becoming more uniform with the widespread acceptance of the Uniform Trade Secrets Act, the case law interpreting state trade secret laws is highly fact-specific. If an employer fails to take proactive steps to protect its trade secrets, the employer is gambling that it can construct a strong after-the-fact case which will provide the desired protection of its trade secrets. This belated approach to trade secret protection may prove to be very costly to the employer if the court holds that the pertinent information is not a trade secret. A much safer and surer approach is to take affirmative, proactive steps which strengthen the employer’s legal posture through lessons learned in the applicable case law.

To protect its trade secrets, an employer must prove that the information was indeed a trade secret, which requires a dual showing that (1) the employer had a confidential relationship with the employee, and (2) the employer made reasonable efforts to keep the information secret. A proactive program to protect an employer’s trade secrets specifically addresses these two prongs required to establish a trade secret. An effective proactive program will therefore consist of an employee awareness program to put employees on notice and to affirmatively establish the confidential relationship, and a security program to assure the continued secrecy of the trade secret.
The proactive program for assuring the protection of trade secrets should be implemented in two phases. The first phase is the initial trade secret review, which determines which information should be protected, determines what level of security is required for each, and puts in place the required procedures to assure their protection. The second phase is the trade secret audit, which is a periodic review held at least once per year to determine what changes need to be made in the procedures to assure continued legal protection of the trade secrets as the scope of the business changes and as the state laws governing trade secrets evolve.

This proactive program for protecting trade secrets will discourage employee misappropriation of trade secrets, encourage prompt settlement when a misappropriation does occur, and strengthen the employer's legal posture by showing regular and consistent efforts to protect its trade secrets.

*Derek P. Martin*

APPENDIX A

RESTATEMENT (FIRST) OF TORTS § 757, COMMENT B (1939)

*Definition of trade secret.* A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.

*Secrecy.* The subject matter of a trade secret must be secret. Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret. Matters which are completely disclosed by the goods which one markets cannot be his secret. Nevertheless, a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information. An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.
APPENDIX B

UNIFORM TRADE SECRETS ACT, 14 U.L.A. 433 (1990)

§ 1. Definitions.
As used in this [Act], unless the context requires otherwise:
(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;
(2) "Misappropriation" means:
   (i) 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
   (ii) 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 his knowledge of the trade secret was
           (I) derived from or through a person who had utilized improper means to acquire it;
           (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 a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.
(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.
(4) "Trade secret" means 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. Injunctive Relief.
(a) Actual or threatened misappropriation may be enjoined. Upon application to the court, an injunction shall be terminated when the
trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.

(b) In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

§ 3. Damages.

(a) Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (a).

§ 4. Attorney's Fees.

If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party.

§ 5. Preservation of Secrecy.

In an action under this [Act], a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.


An action for misappropriation must be brought within 3 years after the misappropriation is discovered or by the exercise of reason-
able diligence should have been discovered. For the purposes of this section, a continuing misappropriation constitutes a single claim.

§ 7. Effect on Other Law.
   (a) Except as provided in subsection (b), this [Act] displaces conflicting tort, restitutory, and other law of this State providing civil remedies for misappropriation of a trade secret.
   (b) This [Act] does not affect:
      (1) contractual remedies, whether or not based upon misappropriation of a trade secret;
      (2) other civil remedies that are not based upon misappropriation of a trade secret; or
      (3) criminal remedies, whether or not based upon misappropriation of a trade secret.

§ 8. Uniformity of Application and Construction.
   This [Act] shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among states enacting it.

§ 9. Short Title.
   This [Act] may be cited as the Uniform Trade Secrets Act.

§ 10. Severability.
   If any provision of this [Act] or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

§ 11. Time of Taking Effect.
   This [Act] takes effect on______, and does not apply to misappropriation occurring prior to the effective date. With respect to a continuing misappropriation that began prior to the effective date, the [Act] also does not apply to the continuing misappropriation that occurs after the effective date.

APPENDIX C

States that have adopted a form of the Uniform Trade Secrets Act, with effective dates. 14 U.L.A. 78 (Supp. 1993).

<table>
<thead>
<tr>
<th>State</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>8-12-1987</td>
</tr>
<tr>
<td>Alaska</td>
<td>9-2-1988</td>
</tr>
<tr>
<td>Arizona</td>
<td>4-11-1990*</td>
</tr>
<tr>
<td>Arkansas</td>
<td>3-12-1981*</td>
</tr>
<tr>
<td>State</td>
<td>Effective Date</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>California</td>
<td>1-1-1985</td>
</tr>
<tr>
<td>Colorado</td>
<td>7-1-1986</td>
</tr>
<tr>
<td>Connecticut</td>
<td>6-23-1983*</td>
</tr>
<tr>
<td>Delaware</td>
<td>4-15-1982</td>
</tr>
<tr>
<td>Dist. of Columbia</td>
<td>3-16-1989*</td>
</tr>
<tr>
<td>Florida</td>
<td>10-1-1988</td>
</tr>
<tr>
<td>Hawaii</td>
<td>7-1-1989</td>
</tr>
<tr>
<td>Idaho</td>
<td>1-1-1988</td>
</tr>
<tr>
<td>Illinois</td>
<td>2-25-1982*</td>
</tr>
<tr>
<td>Indiana</td>
<td>4-27-1990*</td>
</tr>
<tr>
<td>Iowa</td>
<td>7-1-1981</td>
</tr>
<tr>
<td>Kansas</td>
<td>4-6-1990*</td>
</tr>
<tr>
<td>Kentucky</td>
<td>7-19-1981*</td>
</tr>
<tr>
<td>Louisiana</td>
<td>5-22-1987</td>
</tr>
<tr>
<td>Maine</td>
<td>7-1-1989</td>
</tr>
<tr>
<td>Maryland</td>
<td>1-1-1981</td>
</tr>
<tr>
<td>Minnesota</td>
<td>7-1-1990</td>
</tr>
<tr>
<td>Mississippi</td>
<td>7-9-1988</td>
</tr>
<tr>
<td>Montana</td>
<td>3-5-1987</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>1-1-1990</td>
</tr>
<tr>
<td>New Mexico</td>
<td>4-3-1989*</td>
</tr>
<tr>
<td>North Dakota</td>
<td>7-1-1983</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>1-1-1986</td>
</tr>
<tr>
<td>Oregon</td>
<td>1-1-1988</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>7-1-1986</td>
</tr>
<tr>
<td>South Dakota</td>
<td>7-1-1988</td>
</tr>
<tr>
<td>Utah</td>
<td>5-1-1989</td>
</tr>
<tr>
<td>Virginia</td>
<td>7-1-1986</td>
</tr>
<tr>
<td>Washington</td>
<td>1-1-1982</td>
</tr>
<tr>
<td>West Virginia</td>
<td>7-1-1986</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>4-24-1986</td>
</tr>
</tbody>
</table>

* Date of Approval