manatt
manatt | phelps | phillips

# EMPLOYMENT & LABOR GROUP
# *BREAKFAST BRIEFING* SERIES

**November 2006**

## *Stop Thief! Go Recruiter!*
## *How To Stop Competitors From Stealing Your Trade Secrets And Employees, And What You Can Lawfully Poach In California*


**Los Angeles/Orange County**

**Andrew L. Satenberg, Esq.**

**Alison G. Sultan, Esq.**

**Palo Alto**

**John C. Fox, Esq.**

**Jay J. Wang, Esq.**


**THIS OUTLINE IS MEANT TO ASSIST IN A GENERAL UNDERSTANDING OF THE CURRENT LAW RELATING TO TRADE SECRET THEFT AND DEFENSE AND COVENANTS NOT TO COMPETE. IT IS NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.**

## TABLE OF CONTENTS

**Page**

## A. WHAT IS A TRADE SECRET? - WHAT IS MISAPPROPRIATION?

1. Definition of a trade secret.

a. Introduction.

(1) It is common to find even high-level employees who do not understand what a trade secret is.

(2) Purpose of Trade Secret Law.

The fundamental policy underlying trade secret law is "[t]he maintenance of standards of commercial ethics and the encouragement of invention." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481, 40 L. Ed. 2d 315, 325, 94 S. Ct. 1879, 1886 (1974); Uniform Laws Annotated, Commissioner's Comment, 14 U.L.A. at 438.

b. Definition of trade secret [under the Uniform Trade Secrets Act ("UTSA")].

(1) Where the UTSA has been adopted.

As of 2005, forty-five states, along with the District of Columbia and the U.S. Virgin Islands, have adopted the Act: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, and Wisconsin. See www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-utsa.asp. It should be noted that while Alabama and North Carolina have adopted some version of the UTSA, North Carolina accords broader trade secret protection and Alabama allows a much narrower protection than noted in the Act.

Additionally, during the 2004-2005 legislative session for each respective state, Massachusetts, New Jersey, and New York introduced bills regarding the adoption of the UTSA which, if they became legally effective, would leave

Wyoming and Texas as the only states that protect trade secrets under the common law or the Restatement.

(2) Common sense approach is to ask, initially: "Would I care if this were disclosed to my main competitor?" If you would, then think further about whether it could be a trade secret.

Conversely, "Would my main competitor care if this were disclosed to me?" If you think he/she would, then think carefully about whether it could be a trade secret.

(3) Under the UTSA definition, ALL of the following must be found for something to constitute a trade secret:

(a) Information - It must consist of information (UTSA, § 1(4)); and

(b) Economic value - The information must at least have potential economic value (UTSA, § 1(4)(i)); and

(c) Not generally known - The information cannot be generally known to other knowledgeable persons in the industry (UTSA, § 1(4)(i)); and

(d) Not readily ascertainable - The information cannot be readily ascertainable by proper means by other knowledgeable persons in the industry (this is a crucial limitation) (UTSA, § 1(4)(i)); and

(e) Treated as secret - The company claiming the trade secret must treat the information in question as a secret and must take reasonable steps to keep it secret (UTSA, § 1(4)(ii)).

(4) Loss of trade secret status over time: What is a secret or has economic value can change rapidly over time. New technology developed by Company A may only be six months ahead of Company B. So, after six months, it may no longer be a trade secret.

(5) Two categories of trade secret information - Technical and business.

The types of information that can be protected under trade secret law are virtually without limit. Trade secrets have been found in hundreds of different situations that are listed exhaustively in 1 Milgrim on Trade Secrets, § 1.09 at pp. 1-375 through 2–479.

(a) Technical Information

(i) Formulas - E.g., The formula for making Coca Cola is the classic example. (1 Milgrim, § 1.09 at pp. 1-376 through 1-380.)

(ii) Plans, Designs or Patterns - E.g., Plans or designs for specialized equipment or combinations of equipment. (1 Milgrim, § 1.09 at pp. 1-406 through 1-408.1)

(iii) Processes - E.g., Processes for manufacturing foods, drugs, chemicals, or other materials. (1 Milgrim, § 1.09 at pp. 1-380 through 1-383.)

(iv) Methods and techniques - E.g., Manufacturing methods, discovery tools - assays, substance libraries, expression systems, detection methods. (1 Milgrim, § 1.09 at pp. 1-386 through 1-393. )

(v) Negative information - What didn't work. The definition under the UTSA "includes information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor." Commissioner's Comment, 14 U.L.A. at 439.

(vi) Computer Software – Trade secret protection for software has been explicitly recognized. 2 Milgrim, § 9.03[3][b][ii][A] at pp. 9-132 through 9-134. Cybertek Computer Products, Inc. v. Whitfield, 203 U.S.P.Q. 1020, 1022 (Cal. Super. Ct. 1977); McCormack & Dodge Corp. v. ABC

Management Systems, Inc., 222 U.S.P.Q. 432, 444 (Wash. Super. Ct. 1983); Q-CO Industries, Inc. v. Hoffman, 625 F. Supp. 608, 617 (S.D.N.Y. 1985); Com-Share, Inc. v. Commuter Complex, Inc., 338 F. Supp. 1229, 1238-39 (E.D. Mich. 1971), aff'd, 458 F.2d 1341 (6th Cir. 1972).

Such protection may extend to software provided to an established client with knowledge that the information was confidential. In Hotsamba, Inc. v. Caterpillar, Inc., 2004 U.S. LEXIS 4882 (N.D.Ill., E.Div. 2004), the Court denied defendant's motion for summary judgment against plaintiff's claims of misappropriation of trade secrets and breach of a licensing agreement. The Court rejected defendant's argument that since the plaintiff software maker had disclosed the software to the defendant there was no trade secret protection. The Court emphasized that absolute secrecy is not required to maintain a trade secret, but rather that reasonable efforts were made to maintain the secret. The Court relied on Hotsamba, Inc.'s revelation occurring only to a long established customer, Caterpillar, Inc., and with the understanding that the information was confidential in nature.

(b) Business Information

(i) Financial information prior to public release. (1 Milgrim, § 1.09 at pp. 2-307 through 2-308.)

(ii) Cost and pricing. (1 Milgrim, § 1.09 at pp. 1461 through 1-468.)

(iii) Internal market analyses or forecasts. (1 Milgrim, § 1.09 at pp. 1-461.)

(iv) Customer lists. (1 Milgrim, § 1.09 at pp. 1-411 through 1-454.)

(v) Unannounced business relationships the company is negotiating or has entered into. (1 Milgrim, § 1.09 at pp. 1-472 through 1-475.)

(vi) Information about business opportunities, such as opportunities to acquire another company or product. (1 Milgrim, § 1.09 at pp. 1-472 through 1-475.)

(vii) Marketing or advertising plans both for existing or planned products. (1 Milgrim, § 2.09 at pp. 1-456.)

See generally, O'Grady v. Superior Court, 139 Cal. App. 4th 1423, 1436 (Cal. Ct. App. 2006) (denying discovery requests of Apple Computer after a leak of confidential information about an unreleased product to an internet magazine).

(viii) Personnel information:

a) Who key personnel are.

b) Compensation plans for key personnel.

c) Who would be good to try to hire away because of their special knowledge or experience and whether or not they might be receptive to a solicitation.

See generally, Bancroft-Whitney Co. v. Glen, 64 Cal.2d 327, 351 (1966)(unpublished list of desirable employees and their salaries is confidential information); Motorola, Inc. v. Fairfield Cameras and Instrument Corp., 366 F. Supp. 1173 (D. Ariz. 1973) (revealing other employees' salaries to competitor while still an officer of plaintiff was a breach of defendant's duty);

Eutectic Corp. v. Astralloy-Vulcan Corp., 510 F.2d 1111, 1112-13 (5th Cir. 1975) (breach of non-disclosure agreement found where employee disclosed to new employer which of his former co-workers were "good performers" and should be made job offers); Metropolitan Life Insurance Co. v. Usery, 426 F. Supp. 150 (D.D.C. 1976), cert. denied, 431 U.S. 924 (1977), aff'd, 736 F. 2d 727 (D.C. Cir. 1984) (insurance company's work force analysis, department lists, and promotion schedules were confidential information and were exempt from disclosure under FOIA); Surgidev Corp. v. Eye Technology, Inc., 648 F. Supp. 661, (D. Minn. 1986), aff'd, 828 F.2d 452 (8th Cir. 1987), (identity of a former employer's consultants found to be a trade secret under Minnesota and California law); GAB Business Services, Inc. v. Lindsey & Newsom.

(6) Meaning of "Economic Value."

Information has economic value if a potential competitor would have to expend time and money to develop it independently. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983). Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514 (1st App. Dist. 1997) (former employee's use of customer list to generate business for competing firm constituted misappropriation of trade secrets).

Information of "spiritual" but not economic value does not qualify as trade secret. Religious Technology Center v. Wollersheim, 796 F.2d 1076, 1091 (9th Cir. 1986), cert. denied, 479 U.S. 1103 (1987).

(7) Meaning of "Not Generally Known."

(a) Not a trade secret if known to relevant specialists.

It is not necessary that the information be known to the general public before trade secret protection is lost. "If the principal person who can obtain economic benefit from information is aware of it, there is no trade secret." Commissioner's Comment, 14 U.L.A. at 439.

(b) Can be a trade secret even if some other competitors know it.

"A trade secret need not be exclusive to confer a competitive advantage, different independent developers can acquire rights in the same trade secret." Commissioner's Comment, 14 U.L.A. at 439.

See, Electro-Craft, 332 N.W.2d 890, where the court rejected an argument that information had to confer an economic advantage over all other competitors. The court noted that information regarding servo motors used in computers could be a trade secret even if known to more than one company. "Several developers of the same information, for example, may have trade secret rights in that information." Id. at 900.

The standard applied in Electro-Craft is that information known to more than one company can still be a trade secret if "an outsider would obtain a valuable share of the market by gaining [that] information" and the information is not known to it or readily ascertainable. Id.

(c) Information disclosed to others pursuant to a confidentiality agreement is still a trade secret.

Information that is disclosed to employees, licensees or others pursuant to confidentiality or nondisclosure agreements retains its secret status because it imposes on them a duty not to disclose it.

(d) Unique combination of generally known concepts can be a trade secret.

In Cybertek, 203 U.S.P.Q. 1020, the court found that computer software was a trade secret even though it utilized some approaches that were "general concepts known to experts in the computer industry." Id., at 1024.

"[W]hile general concepts are not protectable, the specific implementation involving a particular combination of general concepts may well amount to a trade secret." Id.

See also, Q-CO Industries, 625 F. Supp. at 617 "It is a well settled principle 'that a trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process and operation of which, in unique combination, affords a competitive advantage and is a protectable secret'" (citation omitted); and Jostens, Inc. v. National Computer Systems, Inc., 214 U.S.P.Q. 918, 923 (Minn. 1982).

(e) Source code still secret even where object code is public.

Even if object code of a software package becomes public, the source code can remain secret. Q-CO Industries, 625 F. Supp. at 617.

(8) Meaning of "Not readily ascertainable by proper means."

(a) It is only "improper means" of discovering trade secrets that are prohibited. Thus, inquiry must be made into what is proper and improper as well as what is meant by "readily ascertainable."

(b) "Improper Means" certainly include:

(i) Theft; or

(ii) Bribery; or

(iii) Fraud or Misrepresentation; or

(iv) Espionage through electronic or other means; or

(v) Breach or inducement of a breach by another of a duty to maintain secrecy (UTSA, § 1(1)).

(c) Otherwise lawful conduct can constitute "improper means."

(i) Improper means are not limited to theft, bribery, misrepresentation, breach or inducement of breach of a duty to maintain secrecy. They can include espionage by means that are not, in themselves, illegal. Commissioner's Comment, 14 U.L.A. at 439.

See, e.g., E.I. Du Pont de Nemours & Co., Inc. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), cert. denied, 400 U.S. 1024 (1971) (improper means includes aerial reconnaissance over a competitor's plant to determine its layout during construction).

(d) Observation of the item in public use or display.

Proper means include observing the item as to which trade secret protection is claimed "in public use or on public display." Restatement, comment f; Commissioner's Comment, 14 U.L.A. at 438.

(e) Published information is readily ascertainable.

Where information can be obtained from published materials such as trade journals or reference books it loses trade secret protection for two reasons.

First, it is now "readily ascertainable." Commissioner's Comment, 14 U.L.A. at 439. See, Jostens, 214 U.S.P.Q. at 924 (plaintiff's claim of trade secret was seriously damaged by fact that an employee had been permitted to write an article and make a presentation explaining its software to other experts in the field).

Second, "[o]btaining the trade secret from published literature" is expressly defined as a "proper means"

Restatement, comment f; Commissioner's Comment, 14 U.L.A. at 439.

(f) Independent development is proper.

Proper means also includes "discovery by independent invention." Id.

The burden of proof shifts to defendant who had access to trade secrets to prove independent development. 3 Milgrim, § 15.01[2][a] at 15-115 through 15-117; Maxwell Alarm Screen Mfg. Co. v. Protective Service Corp., 218 U.S.P.Q. 580, 581 (C.D. Cal. 1982).

(g) Reverse engineering is proper.

(i) Definition of reverse engineering.

Reverse engineering is defined as "starting with the known product and working backward to find the method by which it was developed." Restatement, comment f; Commissioner's Comment, 14 U.L.A. at 438; Kewanee, 416 U.S. at 476; and Sinclair v. Actuarius Electronics, Inc., 42 Cal. App. 3d 216, 226 (1974).

(ii) Reverse engineering is specifically defined as one of the proper means of learning a trade secret. Restatement, comment f; Commissioner's Comment, 14 U.L.A. at 438.

See also, Kewanee, 416 U.S. at 476 and Sinclair, 42 Cal. App. 3d at 226 (noting that reverse engineering is proper).

This also applies to software. "Decompiling, disassembly, and reverse engineering are all proper means of discovering any trade secret which may be contained in [software]." Vault Corp. v. Quaid Software. Ltd., 655 F. Supp. 750, 763

(E.D. La. 1987), aff'd, 847 F.2d 225 (5th Cir. 1988).

(iii) Limits on reverse engineering.

Reverse engineering is only proper if the product which is reverse engineered is obtained "by fair and honest means." Restatement, comment f; Commissioner's Comment, 14 U.L.A. at 438.

(iv) Difficult reverse engineering can give rise to trade secret on behalf of company doing it.

If the reverse engineering is "lengthy and expensive," as is usually the case where it is done honestly, then the party discovering the trade secret this way can itself have a protectable trade secret in the information. Commissioner's Comment, 14 U.L.A. at 439.

c. Common law antecedents to UTSA definition (The Restatement).

(1) Definition of trade secret under common law.

(a) The definition of trade secrets that was widely adopted prior to the UTSA is set forth in the Restatement (First) of Torts, § 757, comment b ("Restatement").

(b) It defines a trade secret as "[A]ny 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."

(i) Information may take many forms.

"It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." Restatement, § 757, comment b.

(ii) Does not include "ephemeral events."

"It differs from other secret information in a business . . . in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like." Id.

(iii) Information must be in use.

"A trade secret is a process or device for continuous use in the operation of the business . . . ." Id.

(iv) Information must be secret.

"The subject matter of a trade secret must be secret . . . " Id.

Factors to consider re secrecy.

The Restatement notes that "An exact definition of a trade secret is not possible. Some factors to be considered . . . are:

i) the extent to which the information is known outside of his business;

ii) the extent to which it is known by employees and others involved in his business;

iii) the extent of measures taken by him to guard the secrecy of the information;

iv) the value of the information to him and to his competitors;

v) the amount of effort or money expended by him in developing the information;

vi) the ease or difficulty with which the information could be properly acquired or duplicated by others."

Comment b.

(2) Definition of misappropriation under common law.

The Restatement defines "misappropriation" as follows:

"One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if:

(i) he discovered the secret by improper means, or

(ii) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or

(iii) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to the other, or

(iv) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake."

d. Flaws in Restatement that the UTSA seeks to address.

(1) Failure to lead to uniform results.

The Restatement's definition, although widely adopted by state courts, failed to provide uniform results. Commissioner's Prefatory Note, 14 U.L.A. at 537. See,

Pooley, Better Protection for Trade Secrets, CAL. LAW. 51, at 51 (Aug. 1985) "in this melange of case law almost any abstract proposition can find support."

This lack of uniformity was due in part to the freedom courts had to adopt or reject whatever portions of the Restatement they chose. 20 Loyola Law Rev. 1167, 1170 (1987).

(2) Restatement poorly organized.

The Restatement was difficult to read. The essential elements of a trade secret are set forth in the comments rather than the text of § 757. Thus the comments have to be read in conjunction with the text.

(3) Restatement is antiquated.

The Restatement definition is antiquated (being based on pre-1939 cases) and fails to adequately protect the needs of modern employers for increased trade secret protection. 20 Loyola Law Rev. 1167, 1169 (1987), citing 69 Minn. L. Rev. 984, 991 (1985).

e. Principal Differences Between Restatement and the UTSA.

(1) Requirement of "continuous use" eliminated.

The Restatement defines a trade secret as "information which is used in one's business" and later as a "process or device for continuous use in the operation of the business." Restatement, comment b (emphasis added).

This requirement does not appear in the UTSA and is inconsistent with the definition of information with "potential" value as trade secret under the UTSA. UTSA, § 1(4)(i) It is also flatly rejected in the Commissioner's Comment. Commissioner's Comment, 14 U.L.A. at 543.

(2) Exclusion of information relating to "ephemeral events" has no basis under the UTSA.

The Restatement excludes information concerning "ephemeral events" (i.e., events that occur only once) from its definition of trade secrets. Restatement, comment b. This limitation is not included in the UTSA definition.

(3) Accidental disclosure no longer fatal.

Under the Restatement, information that was disclosed by accident lost its trade secret status unless the person to whom it was disclosed had notice that the information was secret and that it had been disclosed by accident. Restatement, § 757 (d) .

The UTSA has greatly expanded the protection afforded trade secrets that are accidentally disclosed by providing that misappropriation includes use or disclosure of accidentally revealed information, where the user or discloser knew or had reason to know that the information was accidentally disclosed. UTSA, § 1(2)(ii).

However, there is no misappropriation under the UTSA where the user or discloser materially changed his position before learning of the accidental nature of the disclosure. Id.

(4) Consideration of cost of secret to the owner not a factor under the UTSA.

Under its discussion of the factors that are to be considered in determining whether information was secret the Restatement included consideration of the amount of effort or money expended in creating the trade secret. Restatement, § 757, comment b.

This is not a factor under the UTSA definition.

(5) Ease with which others might obtain (California).

The ease or difficulty with which the information claimed to be secret can be ascertained is a factor under both the Restatement (comment b) and the UTSA (trade secret information is "not being readily ascertainable by proper means . . . ." [§ 1(4)(i)]). However, California eliminated the requirement that the information not be "readily ascertainable" from its version of the UTSA. Cal. Civ. Code, § 3426.1(d)(1).

Note, however, that ready ascertainability by proper means remains a defense that the defendant can raise under the

California statute. Legislative Committee Comment - Senate (1984) to § 3426.1.

2. Misappropriation: How You Can Get into Trouble with Trade Secrets

a. Common sense approach.

"Misappropriation" is the legal term for doing something wrong with someone else's trade secret.

(1) "Is there something wrong with how I acquired this information"

(2) "Is there something wrong with using this information?"

(3) "Is there something wrong with disclosing this information to someone else?"

b. Definition of misappropriation [under the Uniform Trade Secrets Act ("UTSA")].

Under the UTSA definition, there are three separate potential trade secret violations.

(1) Wrongful acquisition;

(2) Wrongful use; or

(3) Wrongful disclosure.

c. Wrongful Acquisition of a Trade Secret (UTSA, § 1(2)(i)).

(1) "Is there something wrong with how I acquired this information?"

(2) Misappropriation by acquisition under the UTSA occurs where the following conditions are all met:

(a) The acquisition of a trade secret of another;

(b) By a person who knows or has reason to know;

(c) That the trade secret was acquired by someone by improper means;

(d) KEY: That "someone" can be you, or it can be anyone else who was involved in obtaining or passing along the information to you.

(3) Breach or inducement of a breach by another of a duty to maintain confidentiality.

(a) Have you asked someone to disclose another person's confidential information to you, even though he or she has an obligation not to disclose the information to you?

(b) If you have, AND you know or have reason to know, that he or she had a an obligation not to disclose the information, then you can be liable for misappropriation.

(c) KEY: The fact that this person willingly disclosed the information to you does not protect you.

(4) The key questions to ask before you know whether you have a problem or not are:

(a) How did I get the information? Was there something improper about how I got it?

(b) From whom did I get it? How did he/she get it? Was there something improper about how he/she got it?

(c) Does the person offering the information to me have the right to give it to me?

(5) Improper acquisition of a trade secret includes theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence, and other means either wrongful themselves or wrongful under the circumstances of the case. Elm City Cheese Co. v. Federico, 251 Conn. 59, 101 (1999).

d. Wrongful Use of a Trade Secret (UTSA, § 1(2)(ii)).

(1) "Is there something wrong with using this information?"

(2) The essence of an action for the wrongful use of trade secrets is the breach of the duty not to disclose or to use

without permission confidential information acquired from another. Philip Morris, Inc. v. Reilly 312 F.3d 24, 42 (1st Cir. 2002).

(3) Wrongful use of a trade secret takes place where:

(a) You use the trade secret of another person in your business; and

(b) You do so without the express or implied consent of the owner of the trade secret; and

(i) Obtained by you using improper means: Prior to use, you stole the information or employed other improper means to acquire it; or

(ii) Obtained from another person who used improper means: At the time of use, you knew or had reason to know, that you got the information from or through a person who stole it, or used other improper means to acquire it; or

(iii) Obtained from person who had obligation not to disclose it to you: At the time of use, you knew or had reason to know that you got the information from or through a person who had an obligation (whether by non-disclosure agreement or otherwise) not to disclose it to you; or

(iv) Obtained by you under agreement or obligation not to use the way you are using: At the time of use, you knew or had reason to know that you learned of the trade secret pursuant to a non-disclosure agreement or other similar agreement that prohibited the use you are making of the information; or

(v) Obtained by you knowing it was disclosed by accident: At the time of use, but before a material change in your position, you knew or had reason to know that it was a trade secret and that it was disclosed to you by

accident or mistake (e.g., because it was faxed or Emailed to the wrong address).

e. Wrongful Disclosure of a Trade Secret (UTSA, § 1(2) (ii)).

(1) "Is there something wrong with disclosing this information to someone else?"

(2) Wrongful disclosure analysis almost exactly the same as the wrongful use analysis.

(3) A single incident may be insufficient to show a wrongful disclosure. The circulation of a matter alone is not sufficient to preclude trade secret protection if the matter was circulated with at least an implied restriction. Highland Tank & Mfg. Co. v. PS International, Inc. 393 F. Supp.2d 348, 354 (W.D.Pa. 2005). The Court held that in order to maintain a trade secret action, one must take reasonable precautions...to insure secrecy, and that one wrongful disclosure of a trade secret should not preclude all future protection. There is a trade secret where the evidence does not prove that the process has in effect been thrown open to the public, or has been so negligently guarded that other persons have probably discovered it by means that were not unfair.

(4) Wrongful disclosure of a trade secret takes place where:

(a) You disclose the trade secret of another person to someone else; and

(b) You do so without the express or implied consent of the owner of the trade secret; and

(i) Obtained by you using improper means: Prior to disclosure, you stole the information or employed other improper means to acquire it; or

(ii) Obtained from another person who used improper means: At the time of disclosure by you, you knew or had reason to know, that you got the information from or through a person who stole it, or used other improper means to acquire it; or

(iii) Obtained from person who had obligation not to disclose it to you: At the time of disclosure by you, you knew or had reason to know that you got the information from or through a person who had an obligation (whether by nondisclosure agreement or otherwise) not to disclose it to you; or

(iv) Obtained by you under agreement or obligation not to use the way you are using: At the time of disclosure by you, you knew or had reason to know that you learned of the trade secret pursuant to a non-disclosure agreement or other similar agreement that prohibited you from disclosing the information to anyone else; or

(v) Obtained by you knowing it was disclosed by accident: At the time of disclosure by you, but before a material change in your position, you knew or had reason to know that it was a trade secret and that it was disclosed to you by accident or mistake (e.g., because it was faxed or E-mailed to the wrong address).

3. How trade secret protection compares to copyright and patent protection.

a. Differences between trade secret and copyright.

(1) Copyright protects only "expression" whereas trade secret protection is not limited.

(a) Copyright law protects original works of authorship, whether published or unpublished, that are fixed in a tangible medium of expression from copying, distribution and other acts. 17 U.S.C. §§ 102, 103, 106, & 302(a).

(b) Copyright law protects only expression. It does not protect ideas, procedures, processes, systems, methods of operation, concepts, principles, or discoveries contained in that expression. 17 U.S.C. § 102(b); Warrington Associates, Inc. v. Real-Time Engineering Systems, Inc., 522 F. Supp. 367, 368

(N.D. Ill. 1981); Q-CO Industries, 625 F. Supp. at 615.

(c) Trade secret law is not limited by the idea/expression dichotomy. It protects the ideas, procedures and concepts that copyright does not (Warrington, 522 F. Supp. at 368; Q-CO Industries, 625 F. Supp. at 615) as well as any other information that meets its test.

(2) Trade secret protection is burdensome and easily lost.

(a) As a review of the "reasonable efforts" cases makes clear, providing sufficient protection to procure trade secret protection for information can be quite burdensome. Copyright protection can be obtained far more easily.

(b) In addition, trade secret protection can easily be lost by failing to continue the reasonable efforts that are required to protect the information or through accidental disclosure. Copyright protection does not require secrecy and cannot be lost through disclosure.

(3) Trade secret protection lasts indefinitely.

(a) Trade secret protection, if properly maintained, can last indefinitely.

(b) Copyright protection lasts for the life of the author, plus 50 years (or, in the case of works for hire, 75 years after first publication or 100 years after creation of work, whichever occurs first). 17 U.S.C. § 302.

b. Differences between trade secret and patent.

(1) Patent law protects inventions that are new, useful, and not obvious to one skilled in a particular subject matter. (35 U.S.C. § 101) Protection lasts for only 17 years (or 14 years in the case of design patents). 35 U.S.C. § 154.

(2) Trade secret protection lasts forever, or as long as the information continues to qualify as a trade secret.

(3) Patent protection is difficult to obtain. A patent can only be obtained from U.S. Patent and Trademark Office after application and examination. 35 U.S.C. §§ 111 & 131.

(4) Trade secret protection is easy to obtain. No formal steps to take or approval needed. Only have to make reasonable efforts to maintain secrecy.

(5) Patent protection is not fragile and is not lost by disclosure. In fact, to obtain patent protection, full and complete public disclosure of the invention must be made. 35 U.S.C. § 112.

## B. HOW CAN A COMPANY PROTECT ITS TRADE SECRETS?

1. "Reasonable efforts."

a. Trade secrecy is fragile.

A company will lose the protection of trade secret law for its confidential information if it does not take steps to protect that information.

Steps taken by the company must be "reasonable measures" designed to protect secrecy. 1 Milgrim, § 2.04, at 2-55. Ungar Elec. Tools, Inc. v. Sid Ungar Co., 192 Cal. App. 2d 398 (1961).

b. Extreme efforts not required.

Only efforts that are reasonable under the circumstances are required to protect trade secrets. "The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage." Commissioner's Comment, 14 U.L.A. at 439.

Example: "Reasonable efforts" do not include guarding against aerial reconnaissance during the construction of a plant because this form of espionage "could not have been reasonably anticipated" and would have been "enormously expens[ive]" to prevent. E.I. Du Pont de Nemours & Co., 431 F.2d at 1016-17.

Company must balance the cost of trade secret protection against value of trade secret and risks of not protecting it. (5 Santa Clara Computer and High Tech. L.J. (June, 1989), pp. 321-348). For this reason, at least some courts have taken the position that it is inappropriate to grant summary judgment for a defendant in a trade secret case based on a finding that efforts to protect the

information were not "reasonable." Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991).

In In re Innovative Constr. Systems, Inc., 793 F.2d 875, 884 (7th Cir. 1986), the Court determined that in asking whether particular efforts were reasonably adequate under the circumstances, the jury is called upon in part to exercise their common-sense judgment in determining whether additional measures were necessary to guard the secrecy of the formulas. In essence, this requires an assessment of the size and nature of the company's business, the cost to it of additional measures, and the degree to which such measures would decrease the risk of disclosure.

c. Mere intent to keep secret is not enough.

"The law requires more than a mere intent to keep [information] secret . . . ." Aries Information Systems, Inc. v. Pacific Management Systems Corp., 366 N.W.2d 366, 368 (Minn. Ct. App. 1985); Electro-Craft, 332 N.W.2d at 901.

The company claiming a trade secret must have made some tangible effort to keep the information secret. Electro-Craft, 332 N.W.2d at 901.

Example: Just setting forth procedures in an employee manual for protecting company confidential information is not enough. The company must actually enforce the procedures.

d. Employees must be given fair notice of what information is considered confidential.

A key part of exercising "reasonable efforts" is putting employees on reasonable notice of the existence of confidential information and their duty not to disclose it. Electro-Craft, 332 N.W.2d at 903; Jostens, 214 U.S.P.Q. at 924-25.

Example: Make sure your employees are given guidelines for what the company considers confidential. Make sure they all sign non-disclosure agreements. Make sure the company periodically issues reminders to employees re confidentiality.

e. Specific risks in industry must be considered.

In order to determine what steps are reasonable under the circumstances, the company with trade secrets must analyze the various risks that are specific to its situation.

See, e.g., Electro-Craft, 332 N.W.2d at 902 (employer's employee confidentiality procedures held "fatally lax" because "employees in the servo motor business frequently leave their employers in order to produce similar or identical devices for new employers").

KEY: In general, high-level industrial espionage is on the increase. Foreign governments are turning many of their "cold war" intelligence gathering capabilities to industrial espionage on behalf of their domestic industries.

France and Japan are among the most aggressive, with China and the U.K. also heavily involved.

f. What are the most important sources of risks for disclosure of confidential information in high technology companies?

(1) Mobility of the labor force. Key employees with knowledge of confidential business and technical information move to new employers.

(2) Physical security of labs and offices from outside intruders. Break-ins and attempted break-ins DO HAPPEN.

(3) In biotechnology companies: R&D "cowboys" with one foot in academia and one in company.

High level of informal, often uncontrolled, information exchanges between company's R&D personnel and their "colleagues" outside of the company.

Visiting scientist "colleagues" invited onto the premises without controls or non-disclosure agreements.

(4) Publishing of information in technical journals or at conferences.

(5) Proliferation of personal computers containing large quantities of important technical and business information - ability of employees to easily access, store and move large quantities of company information.

(6) E-mail systems allowing communication outside the company. Access of unauthorized users to company computer system.

(7) Company trash.

g. Specific cases re "reasonable efforts."

Although a determination of what constitutes "reasonable efforts" depends on the specific facts of each case, a review of several cases discussing reasonable efforts in the context of high technology companies is instructive.

(1) TouchPoint Solutions, Inc. v. Eastman Kodak Co. 345 F.Supp.2d 23, 29 (D.Md. 2004).

Plaintiff sought to prevent Defendant from using or disclosing Plaintiff's confidential information. Specifically, Plaintiff sought to enjoin Defendant from entering the "remote management software" field. Plaintiff's preliminary injunction seeking to enjoin Defendant from entering the field was denied, but was granted as to preventing Defendant from disclosing Plaintiff's trade secrets to third parties and from doing business with another entity.

The Court held that in the context of a misappropriation of a trade secret case, a plaintiff must show that it has taken reasonable measures to protect secrecy. Courts consider several factors in examining that prong, including: 1) the existence or absence of a confidential disclosure agreement, 2) the nature and extent of precautions taken, 3) the circumstances under which the information was disclosed and 4) the degree to which the information has been placed in the public domain or rendered readily ascertainable.

(2) Micro Lithography Inc. v. Inko Indus. Inc., 20 U.S.P.Q. 1347, 1349-51 (Cal.Ct.App. 6th Dist. 1991) (unpublished opinion).

Micro involved a misappropriation claim relating to the fabrication of optical pellicles. A jury verdict in plaintiff's favor on the claim was upheld.

In finding that Micro made reasonable efforts to protect its trade secret process, court took note of the following facts:

> All employees signed non-disclosure agreements (although the agreements did not specifically call out or define the alleged trade secret at issue here).

Visitors were never allowed in the pellicle fabrication area.

Visitors to other areas of plaintiff's plant were always escorted by an employee.

Employees were "constantly" reminded to keep the company's trade secrets confidential.

(3) Cybertek Computer Products, Inc. v. Whitfield, 203 U.S.P.Q. 1020 (Cal. Super. Ct. 1977).

Cybertek involved a misappropriation claim relating to a computer software system designed specifically for use by insurance companies. The software cost over $500,000 to develop and license fees for its use by customers cost between $100,000 and $200,000.

In finding that Cybertek made reasonable efforts to protect the secrecy of its software the court took note of the following facts:

Cybertek had the defendant/employee sign a non-disclosure agreement early in his employment;

Cybertek conducted an exit conference for the defendant/employee in which he acknowledged in writing that he understood his obligation not to disclose confidential information;

Cybertek had a corporate policy of requiring all employees to sign non-disclosure agreements;

Cybertek marked sensitive documents "Confidential;"

Cybertek used registration numbers in connection with copies of its documentation; and

Cybertek only permitted authorized personnel to have access to its software documentation.

(4) Schalk v. State, 767 S.W.2d 441, 443, 446-448 (Tex.App.Dallas 1988), aff'd, 823 S.W.2d 633, 21 U.S.P.Q.2d 1838 (Tex. Crim.App. 1991), cert. denied, 118 L.Ed.2d 425 (1992).

Schalk involved a criminal trade secret theft charge brought against two employees of Texas Instruments who took copies of TI's confidential speech-recognition software.

In finding that TI's efforts to protect the software were reasonable the court took note of the following facts:

> Non-disclosure agreements were signed by all new employees.
>
> Exit interviews with terminating employees reminded them of confidentiality obligations.
>
> Identification badges were required to prevent unauthorized personnel from entering certain areas.
>
> Security guards and closed-circuit television monitors were used.
>
> Entry to the speech-recognition lab was restricted and the lab was located in a separate wing or building.
>
> Print-outs and hard copy of data were not left in sight and nighttime security checks were made to look for data left on desks.
>
> Computer passwords or access codes were issued so that unauthorized personnel could not access key data.
>
> TI listed "speech processing" on its list of trade secrets.
>
> Lab employees were admonished to protect software developed in the lab.

(5) Technicon Data Sys. Corp v. Curtis 1000, Inc., 224 U.S.P.Q. 286, 290 (Del.Ch. 1984).

Plaintiff developed a hospital medical record computer system whose communication interface was allegedly misappropriated by defendants.

In finding that the plaintiff had made reasonable efforts to protect the information, the court took note of the following facts:

> Employees were required to execute nondisclosure agreements.
>
> Customers using the computer system were also required to execute non-disclosure agreements.
>
> The manufacturer of the computer system was also required to execute a non-disclosure agreement.
>
> Manuals containing allegedly confidential information were marked "confidential."

(6) Com-Share Inc. v. Computer Complex, Inc. , 338 F. Supp. 1229 (E.D. Mich. 1971), aff'd, 458 F.2d 1341 (6th Cir. 1972).

Com-Share involved a dispute over the disclosure of software used for time sharing. Although the court's ruling was based upon a nondisclosure agreement rather than a trade secret analysis, it did find that reasonable efforts were made to protect the secrecy of the software.

In so doing the Court mentioned the following factors:

> Sensitive documents embodying Com-Share's system were marked "Confidential" on each page;
>
> Passwords were built into the software to prevent unauthorized access; and
>
> The magnetic tapes and symbolics containing the secrets were kept locked when not in use.

(7) Q-CO Industries. Inc. v. Hoffman, 625 F. Supp. 608 (S.D.N.Y. 1985).

Q-CO involved the alleged misappropriation of software designed to permit the use of personal computers as prompters for television and theater. Although the court did not expressly address the "reasonable efforts" issue, it did find that the plaintiff had a reasonable likelihood of prevailing on its trade secret claim.

The court did this despite noting that Q-CO did not have its employees enter into nondisclosure agreements. (See also, In Re Innovative Constr. Systems, Inc., 793 F.2d 875 (7th Cir. 1986) where the court held that a failure to have employees sign nondisclosure agreements or to conduct exit interviews would not automatically constitute a failure to take reasonable steps (not a computer case).)

(8) Aries Information Systems, Inc. v. Pacific Management Systems Corp., 366 N.W.2d 366 (Minn. Ct. App. 1985).

Aries involved a misappropriation claim relating to software specifically designed to meet financial accounting and reporting requirements of public bodies. The software claimed to be a trade secret (PHOBAS III) was the result of over eight to ten years of development (after an initial investment of $100,000 to come out with PHOBAS I).

In holding that Aries made reasonable efforts to maintain the secrecy of PHOBAS III the court noted the following:

> All of the source code listings and magnetic tapes incorporating the PHOBAS system bore proprietary notices;
>
> Aries' user manuals were copyrighted and stated that all system information was proprietary;
>
> Every "client contract" stated that PHOBAS was the exclusive proprietary property of Aries; and
>
> Key employees signed nondisclosure agreements.

(9) Electro-Craft Core. v. Controlled Motion, Inc., 332 N.W.2d 890 (Minn. 1983).

Electro-Craft involved a misappropriation claim relating to servo motors (motors that can start and stop at least 30 times per second). These motors are used in computer disc drives, among other things.

In finding that reasonable efforts had not been taken in Electro-Craft, the court carefully analyzed all of the steps that had been taken to protect security as well as those that had not.

Steps taken by Electro-Craft included:

Keeping some design notebooks locked;

Screening its handbook and publications for confidential information; and

Requiring some of its employees to sign nondisclosure agreements.

Steps not taken included:

Having good physical security in the plant (seven unlocked entrances to the plant existed without any signs warning of limited access);

Having the employees wear identification badges;

Destroying discarded drawings and plans instead of merely throwing them away;

Keeping motor drawings in a central and locked location.

The court specifically stated that the above, standing alone, would not necessarily be fatal to Electro-Craft because there was evidence that espionage was not a problem.

What was fatal for Electro-Craft was its failure to ensure that its employees were bound to keep the information in question confidential. This failure was deemed fatal because the evidence showed that employees in the servo motor industry often left their employers to produce similar products for their new employers.

In analyzing this failure the court noted the following:

The confidentiality agreements that were signed were too vague to put the employees on notice as to what was deemed confidential;

Sensitive documents were not marked "Confidential" even when they were being sent to customers or vendors;

No policy statement was issued by the company outlining what it considered to be confidential;

No informal warnings regarding confidentiality were given to vendors;

Two of Electro-Craft's plants even had open houses at which the public was invited to observe the manufacturing process.

(10) Jostens, Inc. v. National Computer Systems, Inc., 214 U.S.P.Q. 918 (Minn. 1982).

Jostens involved a misappropriation claim relating to software developed for use in designing class rings.

In finding that Jostens had not even intended to keep its software secret, the court took note of the following factors:

No consideration was ever given to developing a policy to keep information confidential;

Not until over a year after the software was developed did Jostens bar potential customers from the plant;

Jostens permitted a senior technical employee (one of the defendants) to write an article and give a presentation to industry experts explaining the software system; and

None of the sensitive computer tapes or documents were marked "Confidential" or "Secret" until after the litigation began.

(11) Vault Corp. v. Quaid Software, Ltd., 655 F. Supp. 750 (E.D. La. 1987), aff'd, 847 F.2d 225 (5th Cir. 1988).

Vault involved a misappropriation claim relating to software developed to prevent copies of programs from being made on floppy discs.

In finding that Vault had made reasonable efforts to protect its trade secrets the court noted the following factors:

The secret program was encrypted in four layers of code;

The programmers who developed it were kept separated;

All employees signed nondisclosure agreements;

All documents containing any portion of the program were shredded at the end of each day; and

The master program was kept locked in a safe.

h. Minimum practical "reasonable efforts."

(1) Locks on doors

(2) Employee I.D. badges

(3) Visitors

(a) Sign-in for visitors

(b) Badges

(c) No unescorted visitors

(4) Computer security - Passwords

(5) Policy statement - Employee handbook

(6) Confidentiality agreements

(a) Employees

(b) Third parties

2. While interviewing potential employees.

a. Do not disclose confidential information during interview.

(1) Disclosures of hot projects in interview.

(2) Tours of the facility.

b. If planning to disclose, use non-disclosure agreement.

3. On hiring employees.

   a. Explain trade secrets policies.

   b. Review company policy.

   c. Explain types of information that company considers confidential.

   d. Confidentiality/Invention Assignment agreement.

      (1) Confidentiality Agreements.

         (a) Contracts containing confidentiality clauses provide a powerful means of protecting trade secrets. They do this in several ways.

         (b) Contracts establish a duty of nondisclosure.

         While a duty to keep the trade secrets that are disclosed to a person can arise in the absence of a contract, most parties prefer to establish this duty in an express contract because it eliminates any ambiguity.

         Contractual confidentiality agreements can create a duty not to disclose trade secrets. Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102, 1113 (E.D. Mich. 1975); Cybertek, 203 U.S.P.Q. at 1022; Winston Research Corp. v. Minnesota Mining & Mfg. Co., 350 F.2d 134, 140 (9th Cir. 1965); 1 Milgrim, § 3.01 at 3-2.

         (c) Persons learning trade secret information are put on notice.

         An element of many trade secret cases is that the misappropriator knew or had reason to know that the information at issue was confidential. Where no notice is given of the confidential nature of the information, trade secret protection may be lost. Electro-Craft, 332 N.W.2d at 903.

         One way to give such notice is via a confidentiality agreement which informs the employee or licensee that the information being disclosed is confidential.

Such agreements should be as specific as possible. If they are too vague as to what information is confidential, they may be ineffective. Id.

(d) Contracts tend to show "reasonable efforts."

Another advantage of confidentiality agreements is that courts are more likely to find that reasonable efforts were made to protect the information at issue when they are used than if they are not. See, Cybertek, 203 U.S.P.Q. at 1021; Aries, 366 N.W.2d 366; Electro-Craft, 332 N.W.2d 890.

(e) All employees should sign one.

(2) Audit personnel files to make sure no one has been overlooked in the past.

e. Non-Competition/Non-Solicitation Agreements (California and elsewhere).

(1) "Non-competition" agreements -- Generally.

(a) Covenants not to compete provide a valuable supplement to confidentiality agreements because they permit an employer to prevent an employee who has had access to trade secrets from using them in competition with it for a reasonable period of time without having to make any showing of actual misappropriation.

(b) Generally enforceable.

Agreements not to compete will be enforced in most states if they are reasonable and limited as to time and geographical scope. E.g., Raimonde v. Van Vlerah, 325 N.E.2d 544 (1975). See generally, Blake, Employee Agreements Not to Compete, 73 Harv. L. Rev. 625 (1960). (Note: non-competition agreements companies try to enforce are generally unenforceable in California. Cal. Bus. & Prof. Code § 16600.)

(c) Must be balanced against employee's interest in engaging in his/her trade.

Covenants not to compete are limited by the strong public policy favoring the rights of employees to freely engage in their trade. 20 Loyola Law Review 1167, at 1184 (1987).

(d) Access to trade secrets.

Courts will enforce reasonable covenants not to compete in order to protect the trade secrets or confidential information of a former employer. See, e.g., Modern Controls, Inc. v. Andreadakis, 578 F.2d 1264 (8th Cir. 1978); and Sigma Chemical Co. v. Harris, 605 F. Supp. 1253 (E.D. Mo. 1985), aff'd in part and rev'd in part, 794 F.2d 371 (8th Cir. 1986).

(2) "Non-competition" agreements -- the California rule.

(a) California Business and Professions Code § 16600 provides: "Except as provided in this Chapter, every contract by which any one is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."

Thus, non-competition agreements are generally not enforceable in California.

(b) California Business and Professions Code § 16600 does not apply to partnerships, only corporations.

(c) Moreover, section 16601 creates several exceptions, one of which is found where the person agreeing to be bound by the non-competition agreement sells "all" of his/her shares in the corporation to the other party. This is deemed to be akin to the sale of the goodwill of the corporation. (See, Radiant Industries, Inc. v. Skirvin, 33 Cal. App. 3d 401 (1973) for a strict interpretation of "all.")

(d) At least one court has refused to apply this exception to a three year non-competition agreement where an employee was required to buy 9% of the employer's stock upon joining it and agree that he had to sell it back upon termination. Bosley Medical Group v. Abramson, 161 Cal. App.

3d 284 (1984). The court characterized the agreement as a "sham devised to circumvent our state policy against agreements which prevent the practice of a business or profession" and refused to find the exception in section 16601 applicable. It held that section 16601 was "intended to permit noncompetition agreements only in situations in which the transfer of 'all' of the owner's shares involves a substantial interest in the corporation so that the owner, in transferring "all" of his shares, can be said to transfer the goodwill of the corporation."

(e) Vacco Indus., Inc. v. Van Den Berg, 5 Cal. App. 4th 34 (1992),

In Vacco, a California Court of Appeal expanded the enforceability of non-competition agreements between former minority shareholders of acquired corporations and the acquiring corporations under Business and Professions Code § 16601. The court enforced a five year noncompetition agreement covering the entire country between a former officer of the acquired corporation and the acquiring entity even though he held only 3% of the acquired corporation's stock. The court distinguished Bosley on the ground that it involved a "sham" agreement forcing the selling party to sell his stock upon termination of his employment solely as a means to evade the noncompetition proscriptions in Section 16600. The court found that, where there is no element of sham and the selling shareholder had been a "principal officer" and ninth largest shareholder of the acquired corporation, a non-competition agreement would be enforceable.

f. The Application Group, Inc. v. The Hunter Group, Inc., 61 Cal. App. 4th 881 (1998), review denied, 1998 Cal. LEXIS 2968 (May 13, 1998).

In The Application Group, a California Court of Appeal concluded that a noncompetition clause, in an employment agreement between a Maryland company (Company A), and the company's employee who did not work in California, was unenforceable against the employee and a California company (Company B) with

whom she sought employment after leaving Company A. The employment agreement (including the noncompetition clause) provided that it would be governed by Maryland law. The clause prohibited plaintiff from working for direct competitors, which included Company B. Following Company B's recruitment of the employee, and Company A's objection, Company B and the employee filed an action in a California court for declaratory relief, requesting that the court find that California law (specifically, § 16600) applied and rendered the noncompete unenforceable. Following a detailed choice of law analysis, the trial court concluded that, despite the express language in the employment agreement that it would be governed by Maryland law (which recognizes and enforces noncompetition clauses), California law would be applied and the clause deemed unenforceable, based, in part, on the conclusion that California has a "materially greater interest than [Maryland] in the determination of the particular issue, based on the strong policy which underlies 16600, and its interest in protecting the freedom of movement of all persons who California employers wish to employ.

g. Kolani v. Gluska,
64 Cal. App. 4th 402 (1998)

In Kolani, a California Court of Appeal addressed the issue of "blue penciling," or judicial rewriting, of covenants not to compete. The case involved a breach of contract claim in which the employment agreement contained a broad covenant not to compete—providing for a duration of one year after termination of employment and extending within forty miles of the city where the employer was located. The agreement also contained a "savings" clause authorizing a court to narrow or revise the noncompetition clause. The Court of Appeal affirmed the trial court's holding that the covenant not to compete was void and unenforceable and refused the employer's request that the court rewrite the noncompete clause as a mere bar on misappropriation of confidential customer lists and trade secrets. The court held that, despite the "savings" clause, an illegal contract—such as a broad covenant not to compete—cannot be saved from illegality by narrowed construction. The court also emphasized that if employers were permitted to rewrite otherwise unlawful agreements in the event of litigation, they would have no disincentive to use broad, illegal non-compete clauses that, in most instances, with which most employees would uncritically comply.

h. Latona v. Aetna,
82 F. Supp. 2d 1089 (C.D. Cal. 1999)

In Latona, the plaintiff-employee sued her former employer for violation of § 16600 after the employer discharged her for refusing to sign a noncompetition and confidentiality agreement. The court held that the agreement's broad noncompetition provision was void as against public policy, rejecting the employer's argument that the noncompetition agreement—even if unenforceable—was simply a nullity and thus could not violate public policy. More importantly, the Latona decision helped to flesh out the law regarding "blue penciling" of agreements containing noncompetition provisions. The noncompetition agreement at issue in Latona contained a severability clause designed to save the remainder of the agreement in the event that any of the provisions were found unenforceable. The employer argued that the presence of the severability clause should rescue the agreement as a whole—allowing for the extrication of the illegal noncompetition provision and retention of the remainder of the agreement. The court disagreed, citing the California Court of Appeal's Kolani opinion, and held that that an employer may not fire an employee for refusing to sign an agreement that is against public policy and then escape liability for wrongful termination on the ground that the rest of the provisions were inoffensive.

i. Walia v. Aetna,
93 Cal. App. 4th 1213 (2001), *depublished*, 41 P.3d 548 (Feb. 27 2002)

In Walia, a companion case to Latona, Aetna fired the plaintiff-employee for refusing to sign a noncompetition agreement and subsequently sued her former employer for wrongful termination in violation of public policy. The trial court ruled that the agreement violated § 16600 as a matter of law, and a jury awarded the employee $54,312 in compensatory damages, $125,000 in emotional distress damages and $1,080,000 in punitive damages. The employer appealed, challenging the propriety of the damage awards. The Court of Appeal rejected the employer's challenges, holding that the employee had a Tameny claim for wrongful termination because she had been discharged for refusing to do something that public policy condemned—i.e., to sign a noncompetition agreement. On February 27, 2002, the California Supreme Court granted review of Walia and depublished the Court of Appeal's opinion, so Walia is not currently citable authority.

j. D'Sa v. Playhut,
85 Cal. App. 4th 927 (2000)

In Playhut, a California Court of Appeal found that the fact that an unlawful non-competition clause was, by its terms, severable from the overall employment agreement does not make the firing of an employee for refusing to sign the agreement lawful. The plaintiff employee sued his former employer and its human resources, payroll, and administrative services provider for wrongful termination, alleging that they had violated public policy when they fired him because he refused to sign a confidentiality agreement containing an illegal covenant not to compete. The Court of Appeal reversed the trial court's grant of summary judgment for the defendants, holding that an employee may not be terminated for an unlawful reason or a purpose that contravened fundamental public policy. The court found that, because the employment agreement in question contained a non-competition clause that was unlawful under § 16600, the employer could not lawfully make the signing of the agreement a condition of continued employment—even if the covenant not to compete was severable from the rest of the agreement. The court found, therefore, that the employer's termination of the employee for refusing to sign the agreement constituted a wrongful termination in violation of public policy.

k. Hill Medical v. Wycoff,
86 Cal. App. 4th 895 (2001)

In Hill Medical, the employee had entered into a stock redemption agreement with the employer whereby the employer would repurchase the employee's common stock upon the termination of the employee's employment. Under the agreement, the repurchase price would be measured by net book value—i.e., assets minus liabilities—and the employer did not carry goodwill as an asset on its books. The stock redemption agreement contained a covenant not to compete, barring the employee from similar employment within a 7 ½ mile radius of any of the employer's facilities for three years. In a lawsuit brought by the employer to enforce the covenant not to compete, the trial court found that the noncompetition provision was invalid under § 16600. On appeal, the plaintiff-employer argued that the covenant fell within the exception set forth in § 16601, as it was part of an agreement for sale of the employee's common stock in the company.

The Court of Appeal upheld the trial court's finding that the noncompetition provision was void and unenforceable, rejecting the employer's § 16601 argument on the ground that there had been no compensation for goodwill under the repurchase agreement. The court held that, in order to uphold a covenant not to compete pursuant to § 16601, a contract for the sale of corporate shares must clearly establish that the parties valued or considered goodwill as a component of the sales price—thus, the share purchasers would be entitled to protect themselves from competition from the seller. The Court of Appeal also denied the employer's request that the court restructure the covenant to make it enforceable, finding that this was not a situation in which an otherwise valid covenant covered an unreasonably large geographical area or was unreasonably long in duration. Rather, because there had been no compensation for goodwill, the covenant was void and could not be rewritten. Citing Kolani, the court held that to rewrite a void covenant would undermine § 16600 and California's public policy of open competition.

l. Edwards II v. Arthur Andersen LLP,
142 Cal. App. 4th 603 (2006)

The Court of Appeal held invalid under California Business & Professions Code section 16600 a non-competition agreement prohibiting the plaintiff from performing professional services, for an 18–month period, for any client on whose account on which he had worked. The court emphasized Section 16600's bright line rule which voids contractual restraints on trade or business unless used to protect trade secrets or confidential proprietary information. Id. at 803. The Court of Appeal disagreed with the trial court's application of the so-called "narrow restraint" exception to Section 16600, which the Ninth Circuit had adopted many years ago, which provides that a non-competition agreement does not violate Section 16600 as long as the restriction imposed is limited and leaves a substantial portion of the market available to the employee—(e.g. restrictions limited in time, geography or scope). Id. Though Andersen's non-competition agreement placed only a limited restriction on Edward's ability to engage in his profession, the Court of Appeal held that the agreement nonetheless restricted his ability to practice his profession and was therefore void under California law. Id. According to this court, non-competition agreements forbidding work on a departing employee's former accounts, even if narrowly drawn, are unenforceable, unless they fall within the statutory or trade secrets exception.

4. Non-Solicitation Agreements -- Generally.

   Enforceability will vary from state to state. However, the analysis of enforceability will generally be the same as that of non-competition agreements.

5. Non-Solicitation Agreements -- the California rule.

   a. Solicitation of former employer's customers.

      "Anti-solicitation covenants are void as unlawful business restraints except where their enforcement is necessary to protect trade secrets." Moss, Adams & Co. v. Shilling, 179 Cal. App.3d 124 (1986); see alsoCourtesy Temporary Service, Inc. v. Camacho, 222 Cal. App.3d 1278.

   b. Solicitation of former employer's employees.

      California law is unsettled on the enforceability of such clauses. The outcome in any given case will probably turn on the specific facts of each case, including perception of extent to which clause impinges on ability to compete. At least one court has upheld a clause prohibiting solicitation of employees. Loral Corporation v. Moyes, 174 Cal. App. 3d 268 (1985).

6. During the employment period.

   a. Have a trade secret policy and enforce it.

   b. Screen employee speeches and publications in advance.

   c. E-Mail

      There are four primary features of e-mail's communication capability that make it a threat to the company's ability to protect confidential information.

      (1) Scope of addressees;

      (2) Easy to send message to wrong addressee;

      (3) Forwarding messages; and

      (4) Remote access.

7. On terminating employees.

a. Exit interviews.

b. Reaffirmation of confidentiality agreements.

c. Carrying out searches.

Consider searching the following areas:

(1) Laptop or computer returned from home;

(2) Office PC;

(3) E-mail messages; and

(4) Hard copy files.

d. Demand letters.

(1) To former employee

(2) To new employer

e. The "Inevitable Disclosure" Theory.

(1) Where an employee who had access to trade secrets goes to work for a competing company on a project similar to what he/she did for the former employer, some courts are sympathetic to claims based on a theory of "inevitable disclosure."

(2) The theory is that, even an employee acting in good faith cannot help but use or disclose confidential information learned with the prior employer on that project. Accordingly, the former employer claims the right to a preliminary injunction prohibiting the employee from working for the competitor in that capacity, at least for some "reasonable" period of time.

(3) The concept of inevitable disclosure dates back at least eighty years to Eastman Kodak Co. v. Powers Film Products, 189 A.D. 556, 179 N.Y.S. 325 (4th Dep't 1919) (employee of Kodak with detailed knowledge of technical aspects of film development enjoined from working for direct competitor where the "mere rendition of the service [for the defendant company] would almost necessarily

impart such knowledge to some degree. [The employee] cannot be loyal . . . .").

(4) This interest in preventing "inevitable disclosure" clashes with the strong public policy in favor of the free movement of labor. This policy is especially strong in California. (California Bus. & Prof. Code, § 16600.). One California appellate court adopted the inevitable disclosure doctrine in a 1999 decision, despite the doctrine's clear conflict with the terms of, and policies behind, § 16600. Electro Optical is discussed below.

(5) Cases Supporting "Inevitable Disclosure" Argument

(a) Pepsico, Inc. v. Redmond,
54 F.3d 1262 (7th Cir. 1995).

The seminal decision on the inevitable disclosure doctrine comes from the Seventh Circuit. In Pepsico, defendant William Redmond, who served as a high level manager for over ten years, left the company and attempted to join a direct competitor, Quaker Oats, Co. Quaker and Pepsico competed in the sale of sports drinks (Gatorade and All Sport) as well as new age soft drinks. Redmond had "extensive and intimate knowledge" of Pepsico's marketing, distribution, pricing and overall strategic plans for the sale of Allsport (Pepsico's sports drink).

When Pepsico learned that Redmond was preparing to leave and join Quaker in the development and marketing of Gatorade and other competitive products, it sought and obtained a preliminary injunction preventing him from assuming the position of Vice President of Field Operations. The Court of Appeals for the Seventh Circuit, construing Illinois Trade Secrets Act (ITSA) affirmed the district court's issuance of a preliminary injunction.

The court of appeals determined that Redmond held "extensive knowledge about [Pepsico's] strategic goals for the sports drinks and new age drinks." The court concluded that "unless Redmond possessed an uncanny ability to compartmentalize

information, he would necessarily be making decisions about [Quaker's] Gatorade and Snapple by relying on his knowledge of [Pepsico's] trade secrets." In light of the fierce competition between Pepsico and Quaker as to these products, and the sensitive nature of the information to which Redmond had been exposed over ten years at Pepsico, the court held that the district court properly found a threat of misappropriation.

Pepsico is repeatedly cited by courts and scholars on the issue of inevitable disclosure.

(b) Electro Optical Industries, Inc. v. Stephen White, 76 Cal. App. 4th 653 (1999) (depublished; in California, this means that this case cannot be relied on as support for the inevitable disclosure doctrine).

In Electro Optical, defendant Stephen White worked for the plaintiff as a sales manager for fifteen years, selling test equipment to military and defense contractors. White was not an engineer, but, Electro Optical argued, he possessed technical information about design and manufacturing aspects of the company's current and future products. When White informed Electro Optical that he was leaving the company to join a direct competitor, Santa Barbara Infrared, Inc., Electro Optical instructed White to sign a termination statement, wherein he agreed not to use or disclose the company's trade secrets following his departure. Immediately after White signed the statement, Electro Optical served on him a complaint alleging misappropriation of trade secrets by way of inevitable disclosure, and seeking a temporary restraining order.

The trial court denied Electro Optical's requests for injunctive relief, finding no actual or threatened misappropriation of trade secrets. The Court of Appeal for the Second Appellate District affirmed. However, in affirming the lower court's ruling, the court of appeal addressed the inevitable disclosure doctrine (which California courts did not recognize at that time) and stated: "Although no California

court has yet adopted it, the inevitable disclosure rule is rooted in common sense and calls for a fact-specific inquiry. We adopt the rule here."

Two aspects of Electro Optical merit discussion. First, given that the court's adoption of the inevitable disclosure rule was not necessary to its holding that the plaintiff failed to make a showing of actual or threatened misappropriation, adoption of the rule is dicta.

Second, the court neither discussed nor even mentioned in passing California Business & Professions Code § 16600. As discussed above, this statute prohibits non-competition agreements in California, and is rooted in a strong policy in favor of the free movement of labor. The court's adoption of the inevitable disclosure doctrine necessarily conflicts with this statute, and the court's failure to address this conflict is troubling.

In April 2000, however, the California Supreme Court depublished the Electro Optical opinion. Thus, at this writing, inevitable disclosure doctrine continues not to be recognized in California and Electro Optical is no longer citable authority.

(c) Novell, Inc. v. Timpanogos Research Group, Inc., 46 U.S.P.Q.2D 1997 (1998).

Novell, an industry leader in computer networking software, sued Timpanogos, a software development company started by former Novell employees, claiming that the former employees misappropriated Novell's "clustering" technology (the "Wolf Mountain Project"). The employees left Novell because of the difficulty they experienced in developing the project. Novell and the employees entered into an agreement upon their departure, by which the employees would form a new corporation to engage in software development, but would respect Novell's intellectual property, and if they developed any products which would compete with Novell products, the employees would obtain required licenses for Novell technologies.

Moreover, although not bound by non-competition agreements, the employees entered into confidentiality agreements with Novell regarding the Wolf Mountain technology. After starting Timpanogos, the defendants began developing a new project, "Tapestry," which was "lifted verbatim from the Wolf Mountain Architecture."

After finding that the former employees violated the confidentiality and licensing agreements they entered with Novell, and misappropriated Novell's trade secrets (based in part upon disclosure of the Wolf Mountain technology, disguised as Tapestry, to Microsoft Corporation), the court addressed inevitable disclosure.

Although no Utah court had previously addressed the doctrine, the trial court concluded that the Novell dispute constituted an "excellent example of why it should." The court found that the defendants were the principal inventors of the Wolf Mountain Technology. Moreover, because of their long association with the Wolf Mountain project, the employees were sufficiently educated as to what worked, and what did not, on the project, and it would be "inconceivable to believe that if they are designing a product similar to Wolf Mountain that they ever would start down any of the blind alleys that they already know won't work . . . it is inevitable that [the defendants] will not use any of the negative knowledge which they learned while at Novell . . . ." The court concluded "there is no question that there is a high probability that defendants will use or disclose Novell's trade secrets."

(d) Weed Eater, Inc. v. Dowling,
562 S.W.2d 898, 902 (Tex. Ct. App. 1978).

Lower court found to have abused discretion in refusing to enjoin defendant, who had signed a non-competition agreement, from working for direct competitor of former employee in same capacity as he held for former employer. Court of Appeal found that, "Even in the best of good faith,

[defendant] can hardly prevent his knowledge of his former employer's confidential methods from showing up in his work. The only effective relief for [plaintiff] is to restrain [defendant] from working for [new employer] in any capacity related to the manufacture by [the new employer] of a flexible line trimming device." (emphasis added) (citations omitted)

(e) Electronic Data Systems Corp. v. Powell, 524 S.W.2d 393, 398 (Tex. Ct. App. 1975).

Non-competition agreement enforced and injunction broadened by Court of Appeal to prohibit defendant from working in same capacity for competitor of former employer.

"It was clearly established that the methods and techniques developed by EDS have resulted from a significant investment of time and money. Even in best good faith, a former technical or `creative' employee such as Powell working for a competitor such as SRI can hardly prevent his knowledge or his former employer's confidential methods from showing up in his work. If Powell is permitted to work for SRI in the same area as that in which he was trained by EDS, injunctive relief limited to restraint of imparting such special knowledge as prepayment utilization review [PPUR], is likely to prove insufficient. The mere rendition of service in the same area would almost necessarily impart such knowledge to some degree in his subsequent employment. Powell cannot be loyal both to his promise to his former employer, EDS, and to his new obligation to his present employer." (emphasis added) (citations omitted)

(f) But see, Hart v. McCormack, 746 S.W.2d 330 (Tex. App. Beaumont 1988).

Court states that Texas law provided no authority to permit a court to issue an injunction to restrain competitive employment absent a restrictive covenant.

(g) Air Products & Chemicals, Inc. v. Johnson, 215 U.S.P.Q. 547, 555-56, 442 A.2d 1114 (1982).

Even in absence of restrictive covenant, former sales VP could be enjoined from engaging in certain kinds of sales activities for competitor of former employer, by reason of perceived inevitability of disclosure of both technological and confidential business trade secrets.

Trial court granted injunction against disclosure and against employee working in certain of defendant's operations for one year even though the employee had not executed a restrictive covenant.

(h) But see, Oberg Indus. Inc. v. Finney, 382 Pa. Super. 525, 555 A.2d 1324 (1989).

The result in Air Products has been described by the same court as being limited to situations involving employees with significant technical knowledge.

(i) Gillette Co. v. Williams, 360 F. Supp. 1171, 1177 (D. Conn. 1973).

Case involved restrictive covenant and was decided under English law. The parties stipulated that it was the same as Connecticut law. The court denied defendant's motion to dismiss the plaintiff's application for a preliminary injunction restraining defendant from going to work for a competitor ("Schick").

The court engaged in a lengthy analysis of confidential information the defendant was exposed to and concluded that Gillette acted reasonably in seeking a restrictive covenant from key employees such as plaintiff.

"At the time the parties entered into the contract containing the restrictive covenant, it was reasonable to assume that a key employee might be familiar with valuable confidential information if he subsequently left Gillette's employment to work for a competitor. Recognizing that it would be virtually

impossible to avoid or detect his divulging such information to a competitor, Gillette understandably required [plaintiff] to sign the agreement as a condition of employment to protect its competitive position in the market." (Emphasis added).

(j) Emery Industries. Inc. v. Cottier, 202 U.S.P.Q. 829, 835-37 (S.D. Ohio 1978).

In light of former employee's pervasive knowledge of plaintiff's trade secrets, the court found that his duty not to use or disclose could be enforced only by court ordered noncompetition for one year, even though there was no non-competition agreement.

The court concluded that an injunction merely prohibiting disclosure would not be effective, and it cited approvingly to the "inevitable disclosure" language in Allis-Chalmers Mfg. Co. v. Continental, 255 F. Supp. 645 (E.D. Mich. 1966).

(k) A.B. Chance Co. v. Schmidt, 719 S.W.2d 854 (Mo. Ct. App. 1986).

Plaintiff was the sole company practicing a particular high tech process for the manufacture of certain epoxy resin rods. Defendant employee was about to enter into the employ of a would-be competitor which had attempted to develop the same type of rod and it appeared that the job interviews and placement had been based upon defendant's experience with plaintiff.

Despite the absence of a restrictive covenant, the court found that an injunction was properly entered to prevent the employee from working on certain types of projects for his new employer.

(l) Allis-Chalmers Mfg. Co. v. Continental, 255 F. Supp. 645, 654 (E.D. Mich. 1966).

Defendant employee was enjoined from working for defendant employer in connection with design and development of distributor pumps in light of "inevitable and imminent danger of disclosure of

[plaintiff's] trade secrets" and the "virtual impossibility" of defendant working for employer "to the best of his ability," without in effect giving it the benefit of [plaintiff's] confidential information."

(m) IBM v. Seagate,
1991 U.S. Dist. LEXIS 20406 (D. Minn. 1991), *reversed and remanded*, 962 F.2d 12, 1992 U.S. App. LEXIS 19849 (8th Cir. Minn. 1992)

District Court granted preliminary injunction to IBM prohibiting former high-level IBM employee with knowledge of confidential information regarding its MR head design from taking a position with Seagate where he would be responsible for developing its competing MR head design.

Based on a three part test, the court found that IBM made out a claim for "inevitable disclosure."

The court looked to: (1) the level of competition between the former employer and the new employer; (2) whether the employee's position with the new employer is comparable to the position he or she held with the former employer; and (3) the actions the new employer has taken to prevent the former employee from using or disclosing trade secrets of the former employer.

On Appeal - 8th Circuit dissolves the injunction for technical deficiencies and remanded.

(n) FMC v. Varco International. Inc.,
677 F.2d 500, 501, 505 (5th Cir. 1982).

The plaintiff was an innovator in certain oilfield equipment and the defendant corporation was an avowed copier of plaintiff's parts. Defendant was unable to copy one particular part, despite repeated efforts, and accordingly attempted to hire one of plaintiff's knowledgeable employees and place him in charge of that development. The Court of Appeal found that the trial court erred in denying a preliminary injunction. It determined that the

appropriate injunction would prohibit both disclosure and placing the employee in any position at defendant in which there would be an inherent risk of disclosure.

(o) See also, 1 Milgrim, § 5.02[3][d], at 5-42 through 5-48.1, and cases cited at fn. 46. "Where, [however, trade secrets] are proven, and there is a high degree of probability that competitive employment will lead to their wrongful use or disclosure, an injunction against such competitive employment might be had despite the absence of a covenant not to compete."

(6) Cases To Cite Arguing Against Injunction based on "Inevitable Disclosure"

(a) Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443 (2002).

In Whyte, respondent J. Douglas Whyte had served as appellant Schlage Lock Co.'s Vice-President of Sales. During his employment, Whyte had signed a confidentiality agreement to protect Schlage's proprietary information. Subsequently, Whyte was offered a position with Kwikset, a competitor of Schlage, which he accepted. Schlage contended that Whyte disavowed his confidentiality agreement at the time of his departure, in addition to stealing confidential, trade secret information.

Schlage sought an injunction against Whyte in Colorado state court under the doctrine of inevitable disclosure. Such request was denied, and Whyte subsequently filed a lawsuit in California against Schlage alleging interference with contract and seeking declaratory relief allowing him to continue working with Kwikset. Schlage countersued, alleging misappropriation of trade secrets, among other claims, and brought an ex parte application for an order temporarily restraining Whyte from using or disclosing trade secrets. After granting the temporary restraining order, the trial court denied Schlage's request for a preliminary injunction and dissolved the restraining order based on its belief

that the information sought to be protected were not trade secrets.

In affirming the trial court's decision, the Fourth Appellate District of the California Court of Appeals held that while most of the information sought to be protected were trade secrets, it was confined to the decision of the trial court in determining that there was no undisputed evidence at that point that Whyte had misappropriated any trade secrets. More importantly, the Court rejected Schlage's alternative theory of actual or threatened misappropriation based on the inevitable disclosure doctrine. In rejecting the inevitable disclosure doctrine, the Court determined that the chief ill in the covenant not to compete imposed by the inevitable disclosure doctrine is its after-the-fact nature: The covenant is imposed *after* the employment contract is made and therefore alters the employment relationship without the employee's consent. When, as in Whyte, a confidentiality agreement is in place, the inevitable disclosure doctrine "in effect converts the confidentiality agreement into such a covenant not to compete. The doctrine of inevitable disclosure thus rewrites the employment agreement and "such retroactive alterations distort the terms of the employment relationship and upset the balance which courts have attempted to achieve in construing non-compete agreements."

(b) Globespan v. O'Neill,
151 F. Supp. 2d 1229 (C.D. Cal. 2001).

The court dismissed the plaintiff-employer's claims of misappropriation of trade secrets and unfair competition because the plaintiff relied on inevitable disclosure doctrine and alleged nothing about actual use or disclosure of trade secrets. The court refused to recognize the theory of inevitable disclosure, finding that it creates a de facto covenant not to compete and therefore runs counter to California's public policy favoring employee mobility.

(c) Del Monte v. Dole,
148 F. Supp. 2d 1326 (U.S. Dist. Fla. 2001).

Florida Federal District Court held that the former employers could not utilize the inevitable disclosure doctrine, because neither Florida nor California has adopted the doctrine. Because the former employers failed to show evidence of actual or threatened misappropriation of trade secrets by the employee, the court denied the plaintiff-employers' motion for a preliminary injunction for claim of misappropriation of trade secrets.

(d) Bayer v. Roche Molecular,
72 F. Supp. 2d 1111 (N.D. Cal 1999).

California Federal District Court denied the plaintiff-employer's motion for a preliminary injunction to prohibit its former employee from pursuing employment with the defendant company. The court held that the theory of inevitable disclosure was not the law in California and the plaintiff would have to demonstrate actual use or disclosure or actual threat of misappropriation of a trade secret.

(e) Earthweb, Inc. v. Schlack,
71 F. Supp. 2d 299 (S.D.N.Y 1999).

New York Federal District Court declined to apply inevitable disclosure doctrine, in action seeking to enjoin vice president of internet-based provider of services to information technology ("IT") professionals from joining competitor.

The court concluded the "nebulous standard of 'inevitability'" treads "an exceedingly narrow path through judicially disfavored territory," and should be applied "only in the rarest of cases," and upon evidence that: (1) the employers are direct competitors; (2) the employee's new position is nearly identical; and (3) the trade secrets are highly valuable to both employers.

In rejecting Earthweb's inevitable disclosure argument, the court relied, in part, on the fact that Schlack had no access to Earthweb's advertiser list, source codes or configuration files, nor did he have direct contact with Earthweb's highest executive officers. Moreover, Schlack was not involved developing the Earthweb's overall business strategies and goals, and he had no access to company-wide financial reports or information.

(f) Lexis-Nexis v. Beer,
41 F. Supp. 2d 950 (D. Minn. 1999).

Account manager/salesman who departed Lexis-Nexis to work for competitor Dow Jones would not be enjoined from working for the latter company under the inevitable disclosure doctrine, where Lexis-Nexis presented no evidence that the salesman had the kind of intimate familiarity with corporate policies and strategies that Lexis-Nexis argued were trade secret.

(g) Bendinger v. Marshall Town Trowell Co.,
994 S.W.2d 468 (Ark. 1999).

"The mere fact that a person assumes a similar position at a competitor does not, without more, make it inevitable that he will use or disclose trade secrets."

(h) Standard Brands v. Zumpe,
264 F. Supp. 254, 261, 153 U.S.P.Q. 731 (E.D. La. 1967).

District Court found no inevitability of disclosure where the defendant corporation was not active in the precise areas for which plaintiff claimed trade secrets protection. Moreover, the court found that Louisiana public policy, as manifested in a statute prohibiting non-competition clauses in employment agreements, would prevent a Louisiana court from enjoining employment in which disclosure might appear inevitable. The sole injunctive relief available would be an injunction against disclosure.

(i) Continental Group, Inc. v. Amoco Chemicals Corp., 614 F.2d 351 (3d Cir. 1980).

Court of Appeal affirmed the District Court's refusal to enforce a restrictive covenant, even where the District Court had found that there was a risk of inadvertent disclosure by reason of the former employee's employment in a similar activity with defendant. Court of Appeal also threw out the District Court's preliminary injunction prohibiting disclosure since there was no more than an apprehension of possible inadvertence and no high degree of likelihood found.

(j) Rigging International Maintenance Co. v. Gwin, 128 Cal. App. 3d 594 (1982).

Because the employee's skill and knowledge constitute the basis of his livelihood, the courts should not "hastily brand them as confidential where this will deprive him of employment opportunities."

## C. HOW CAN A COMPANY PROTECT ITSELF FROM TRADE SECRET LIABILITY TO OTHERS?

1. While interviewing potential employees.

a. Note: Many companies view interview as an opportunity to pump candidate for competitive information.

b. Tell candidates not to disclose company confidential information to you.

c. Ask if he has signed any confidentiality, nondisclosure or noncompetition agreements with current or past employers. If so, you should examine them before hiring.

(1) Noncompetition agreements generally are not enforceable in California EXCEPT upon sale of a business (Cal. Bus. & Prof. Code § 16600 et seq.). Moreover, an agreement signed by an out-of-state employee with an out-of-state employer (e.g., before the employee moved to California) may also be unenforceable in California.

Roesgen v American Home Products Corp., 719 F.2d 319 (9th Cir. 1983), applying California law but enforcing provisions of a New York contract that deprived employees of certain benefits if they went to work for a competitor, but did not preclude them from working.

See also, Scott v Snelling & Snelling, Inc., 732 F. Supp. 1034 (N.D. Cal. 1990) and Frame v. Merrill Lynch, Pierce, Fenner & Smith, Inc. 20 Cal. App. 3d 668 (1971), cases in which employee noncompetition agreements were not enforced, as being repugnant to "strong California public policy."

Note, too, that in Scott, the court did say that there could be a "judicially carved exception to Bus. & Prof. Code § 16600," and a noncompetition agreement could be enforced, where the taking of trade secrets was involved.

2. On hiring employees.

   a. Risk assessment prior to hiring.

      (1) Hiring from direct competitor to work on competing product or territory - highest risk.

      (2) Special issues of preserving attorney-client privilege if company counsel meets with potential employee.

      (3) Possible use of intermediary attorney as a "black box" to assess risk and overlap.

   b. First "WOODSHEDDING" of potential employee about trade secrets.

      (1) Convince him that your concern is real, not mere lip service.

      (2) Tell him to bring nothing with him that belongs to, or conceivably may belong to, the prior employer. Tell him that you will expect him to sign an agreement upon hire that says he did not take anything and is not in violation of any prior agreements. Signing this is a condition of his employment with you.

(3) Employees eager to prove their worth may offer information, customers, or the like. Make him aware that this is not why you hired him.

(4) Give him some advice on how to leave his old employer.

(a) He should ask for an exit interview if one is not offered.

(b) List returned items and obtain acknowledgment.

(c) Offer to clean out his office, desk, computer, etc. in presence of Human Resources staff.

(d) Be sure to return everything from his home and car.

(e) Even if parting is unfriendly, do not make threats or predictions about new company destroying the old.

(f) Do not try to persuade or solicit co-workers to leave with you.

c. Managing the emotions and perceptions of other company when hiring away a key employee to reduce risk of lawsuit.

(1) By proper conduct during termination and exit (see above).

(2) By not "raiding" other employees of OldCo.

(3) Signing bonuses, large salary raises and other significant increases in title or compensation for an employee who jumps ship may be appropriate in some cases, but consider them carefully: They always make the old employer suspicious.

(4) Direct communication with old employer may be appropriate; consult counsel first.

d. Second "woodshedding" of employee once he/she is aboard.

(1) Make sure he/she brought nothing.

(a) All files searched for and returned.

(b) All magnetic information deleted (and "shredded")

(2) Explain dangers of paper or e-mail trail.

(a) A trail can be detected in many ways; computer backup tapes and undelete programs can uncover messages and logs that show when particular files were accessed, and by whom.

(b) It is important to convince new employee not to try to outsmart old employer.

e. What information can the employee use? - Skill and experience vs. former employer's property.

(1) To answer this question, we must look to the case law; the facts and circumstances of each situation are considered.

(a) "Tools of the trade" -- an employee is entitled to continue to pursue a livelihood in his chosen field, and to use general experience and knowledge he has gained over years of working in the industry.

(b) Materials, tools, and equipment that are his own property (not purchased for his use by former employer).

(c) Information that is publicly available, or that is generally available to those with some knowledge of the industry (e.g. published by trade associations, purchased in commerce, available from customers, demos and samples freely distributed).

(2) Customer lists and other "non-technical" information such as price lists may be trade secrets if they meet the criteria of the Uniform Trade Secrets Act for economic value, secrecy, and the rest.

(a) Information that could be ascertained or easily compiled by anyone in the business is not a trade secret. Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514 (1997); American Paper & Packaging Products v. Kirgan ,183 Cal. App. 3d 1318, Moss Adams & Co. v. Shilling, 179 Cal. App. 3d 124.

Examples:

(i) A list of potential customers for large telephone systems could be compiled by contacting real estate agents and contractors

to find out about office buildings or hotels being built or renovated, driving around, looking in the phone book, cold calls, etc.

(ii) Information identifying users of a particular type of computer hardware, who might be customers for your software, could be compiled from industry data, users' conferences, trade shows, or published information from the hardware manufacturer.

f. Sign agreement confirming he/she isn't bringing any confidential information and will not use any.

3. During employment.

a. "Raiding" new employee's old company for additional hires.

(1) Legal limitations

(a) Information re employees of the former employer, their salaries, and who are the best employees, may be trade secret or otherwise protected under unfair competition laws, though not specifically covered by UTSA.

(i) Unpublished list of desirable employees and their salaries is confidential information. Bancroft Whitney v. Glen , 64 Cal.2d 327 (1966).

(ii) Revealing other employee's salaries to a competitor while still an officer of the company was a breach of duty. Motorola Inc. v Fairchild Camera and Instrument Co. 366 F. Supp. 1173.

(2) Solicitation of employees of a competitor, even those who are employed at-will, is a dangerous undertaking. The case law in this area is very fact-specific and the "smell test" is widely used.

(a) Solicitation of at-will employees of a competitor is not unfair competition per se (Knudsen Corp. v. Ever-Fresh Foods, Inc. 336 F. Supp. 241 (C.D. Cal.

1971)), but may still be actionable if it involves fraud, malice, breach of fiduciary duty, predatory intent or use of trade secret or confidential information.

(b) For example, in American Republic Insurance Co. v. Union Fidelity Life Insurance Co., 470 F.2d 820 (9th Cir. 1972), the Court stated broadly that the hiring and soliciting of employees for his new company by a manager, before the manager resigned from his old job, constituted unfair competition. But on closer examination, this was something of an extreme case. Before the defendant resigned from his old job, he hired for his new employer 15 of the 25 salesmen who had been under his supervision, and fired the rest.

(i) Non-solicitation agreements, pertaining to solicitation of customers or of employees, will be enforced in California, although, again, the cases are fact-driven.

a) The Moss, Adams case, cited above, held that departing employees who had signed an agreement stating that the names of clients of their old employer were trade secrets nevertheless could take with them the names and addresses of clients with whom they had worked personally, and could send announcements of the opening of their new firm to them. Moss, Adams relied on pre-UTSA California case law, and the much-quoted line:

"Equity has no power to compel a man who changes employers to wipe clean the slate of his memory."

b) Avocado Sales Co. v. Wyse, 122 Cal. App. 627, 632 (1932).

BUT SEE: American Credit Indemnity Co. v. Sacks, 213 Cal. App. 3d 622 (1989), where the court purported to apply the Moss, Adams rule in reviewing denial of a preliminary injunction sought by the former employer, but reached the opposite result!

In Sacks, an employee left her job at a credit insurance company and opened her own independent agency, representing competitors of her old employer. She sent announcements of her new business to 50 customers of her old employer with whom she had had personal contact, soliciting their business, and followed up with phone calls.

Although the court claimed to be following the Moss, Adams rule, it said that here the employee had gone beyond mere announcements to aggressive solicitation, and found that the customer list of the old employer was a trade secret. The court based this ruling on the unique nature of the credit business, the high entry threshold, and the fact that the employer had taken steps to protect the secrecy of its list.

b. Practical considerations

(1) Likelihood of triggering lawsuit may depend on the volubility of the industry; the usual mobility of the type of personnel in question, and the importance of particular individuals and their roles in the company.

(2) How to take more than one employee.

(a) Let them come to you.

(b) Use newspaper ads or headhunters who are not told to target a specific company.

(3) Do not solicit employees to breach written employment agreement.

4. When you find another company's secrets among yours.

a. Isolate and contain them

(1) Make sure you've got them all

(2) Talk to counsel

b. Investigate

(1) Source of information

(2) Extent of contamination

c. Remedial Steps to Consider

(1) Discipline or termination of offending employees

(2) Isolate and keep; destroy; or return information

(3) Confession and negotiation with trade secret owner

(4) Obtain a release in exchange for returning it

(5) Licensing the secrets may be possible

(6) Joint action against the thieves

d. Employees with Knowledge of Competitor Trade Secrets

(1) Terminating an employee for failing to disclose trade secrets of a competitor creates a wrongful termination cause of action against the employer as against public policy

(a) In Norton v. FirstEnergy Corp., No. 05-JE-5, 2006 WL 459266 (Ohio App. 7 Dist. Feb. 23, 2006),

In Norton, a technician at a nuclear power plant was asked to train other technicians in a technique for

oxide thickness testing he had learned from his previous employer. The technician refused, citing a non-disclosure agreement he had entered into before leaving. At his next performance evaluation his rating was "does not meet expectations," as a result of his "failure to train his co-workers in oxide thickness testing." Two years later, after an extended sick leave, he was instructed to apply for long-term disability benefits and his employment was terminated.

The technician filed for retaliatory and wrongful discharge on the theory, inter alia, that his termination was for refusing to disclose his former employer's trade secrets and that this justification was void as against public policy. The court held that indeed there is a clear public policy that prohibits the divulgence of trade secrets, evidenced by the state's adoption of the Uniform Trade Secrets Act. Ohio Rev. Code Ann. § 1333.61 et seq. (2006) (providing for enjoining actual or threatened misappropriation of trade secrets (§ 1333.62), awarding of damages for misappropriation (§ 1333.63), and mechanisms for a court to preserve the secrecy of trade secrets (§ 1333.65)).

Although the court held that a public policy exists in Ohio that prohibits the divulgence of trade secrets, the policy was not implicated in this case, because the technician had failed to raise a triable issue of fact that his firing was not the result of his medical condition. Of particular significance to the decision was that the technician was never able to produce a copy of his agreement with his former employer and that subsequent to his performance review he had trained several employees in oxide thickness testing.

5. Negotiated or voluntary solutions.

   a. Clean Room -- Development of a product using employees and resources other than those who were connected in any way with a competitor or a competitor's products

(1) Keep records of this process (you are doing it for self-protection)

(2) Consult counsel for specific advice

b. "Chinese walls" -- isolation of a newly-hired employee from any projects that may directly relate to work he did at former company; such as competitive products, sales territories, customers, etc.

c. Voluntary noncompetition agreements

(1) Make it part of a settlement agreement to ensure enforceability

(2) Limit scope, duration, markets, etc.

## D. STRATEGIES AND REMEDIES.

1. Remedies for misappropriation of trade secrets.

a. Injunctive Relief

(1) Availability in trade secret cases

(a) Injunctive relief is available under the UTSA to prevent "[a]ctual or threatened" misappropriation. UTSA, § 2(a). The court may enjoin continued future use of the trade secret by the misappropriator for a reasonable period of time until the commercial advantage gained by the misappropriation is eliminated. Commissioner's Comment, 14 U.L.A. 544 at 544.

(b) The court may also compel other affirmative acts to be performed by the misappropriator to protect the trade secret. UTSA, § 2(c). This includes requiring the misappropriator to return the trade secret information to the plaintiff. 14 U.L.A. at 546.

(c) Injunctive relief is also available under the common law and is one of the most frequently sought remedies in trade secret cases. 2 Milgrim on Trade Secrets, § 9.03[ii][b] at 9-255 through 9.256.1; Sketchley v. Lipkin, 99 Cal. App. 2d 849 (1950); Ojala v. Bohlin, 178 Cal. App. 2d 292 (1960) .

(d) Section 2(b) of the UTSA limits the availability of injunctive relief by providing that the court can require the misappropriator to pay a reasonable royalty, in lieu of enjoining any future use of the trade secret where it determines that an injunction would be "unreasonable."

(2) Standard for obtaining

(a) The standard for obtaining injunctive relief under the common law varies widely. Some of the factors considered are whether the plaintiff would be irreparably injured absent an injunction Digital Development Corp. v. International Memory Systems, 185 U.S.P.Q. 136, 142 (S.D. Cal. 1973); whether the misappropriator would be unjustly enriched absent an injunction, (Winston Research Corp. v. Minnesota Mining & Manufacturing Co., 350 F.2d at 142; and the public interest in enjoining a particular use. Republic Aviation Corp. v. Schenk, 152 U.S.P.Q. 830, 835 (ICY. Sup. Ct. 1967).

b. Damages

(1) Compensatory

(a) Availability in trade secret cases

Section 3 of the UTSA provides that damages are also available to a complainant for trade secret misappropriation, either in lieu of or in addition to injunctive relief. This is also true under the common law. 2 Milgrim on Trade Secrets, § 9.04[9][d] at 9-317 through 9-320.

(b) Plaintiff's actual loss or defendant's unjust enrichment

(i) Section 3(a) of the UTSA provides that the damages awarded can be based on plaintiff's "actual loss" and on the amount of the defendant's "unjust enrichment" to the extent that has not already been taken into

account in calculating actual loss. Commissioner's Comment, 14 U.L.A. 456.

(ii) This codifies the common law principle found in Tri-Tron International v. Velto, 525 F.2d 432 (9th Cir. 1975). Commissioner's Comment, 14 U.L.A. 456.

(iii) Recovery for defendant's unjust enrichment is prohibited under the UTSA to the extent it has already been accounted for in calculating actual loss. UTSA, § 3(a).

(iv) The express prohibition on this kind of double recovery in the UTSA was felt to be necessary in order to repudiate common law cases that seemed to permit such a double recovery. Commissioner's Comment, 14 U.L.A. 456. See, e.g., Telex Corp. v. IBM Corp., 510 F.2d 894 (10th Cir. 1975) (per curiam), cert. dismissed, 423 U.S. 802 (1975).

(c) Punitive damages

(i) Section 3(b) of the UTSA authorizes the court to award punitive damages against a party found to have engaged in "willful and malicious misappropriation;" provided, however, that the award of punitive damages is no more than twice the amount of the compensatory damages award made under § 3(a).

(ii) Punitive damages are also available under the common law for willful and deliberate misappropriation. Sperry Rand Corp. v. A-T-O, Inc., 447 F.2d 1387, 1394-95 (4th Cir. 1971), cert. denied, 405 U.S. 1017 (1972); Electronic Data Systems Con). v. Sigma Systems Corp., 500 F.2d 241, 246 (5th Cir. 1974), cert. denied, 419 U.S. 1070 (1974).

(iii) Attorney's fees and costs

a) Section 4 of the UTSA authorizes the court to award reasonable attorney's fees to the prevailing party if (1) a claim of misappropriation is made in bad faith, (2) a motion to terminate an injunction is made or resisted in bad faith, or (3) willful and malicious misappropriation exists.

b) Attorney's fees and costs have been awarded under a wide variety of circumstances under the common law as well. See, 2 Milgrim on Trade Secrets, § 9.04[9][d]–[e] and the cases cited therein.

c. Civil litigation

(1) Reasons to consider

(a) Need to protect truly important trade secrets

(b) Send message to other employees or competitors

(c) Make sure no other employees follow the first

(2) Reasons for caution

(a) High cost

(b) Commencement of lawsuit that may not be easy to drop once immediate goals have been achieved

(c) Injunctions that actually stop an employee from working for competitor unlikely

(d) Risks of cross-complaint

d. Progress of a civil action

(1) Filing of complaint with application for temporary restraining order

(a) Ex parte, which usually means on very short notice (4 hours to 24 hours, depending on the court), but

which can mean on no notice at all to the other side, on a showing of good cause.

(b) Good cause for truly ex parte relief may be the likelihood that the stolen trade secrets will be destroyed or hidden if notice is given

(c) Action may be filed in state or federal court if jurisdictional requirements are met

(i) May combine with claims of patent or copyright infringement in federal court where appropriate

(2) Hearing on temporary restraining order

(a) Usually abbreviated

(b) Done on the papers, declarations and arguments of counsel

(c) Moving party must show immediate danger of irreparable injury

(3) Issuance of temporary restraining order by court

(a) Short duration

(b) Court will set hearing date for preliminary injunction

(c) Parties may request expedited discovery

(d) Bond or undertaking may be required

(4) Preliminary injunction

(a) Court will consider evidence, usually in written form but can hear testimony

(b) A more full and complete presentation by all parties, usually after some discovery has been conducted

(c) Court will issue (or deny) preliminary injunction

(d) Injunction will remain in place for the duration of the lawsuit, until either a permanent injunction is entered, or it is dissolved

(e) Prevailing plaintiff must post injunction bond

(5) Many cases get settled at this point

(6) If the case does not settle, it proceeds like any other lawsuit; cross-claims may be filed, discovery taken, and the case eventually will be tried.

e. Criminal prosecution.

(1) Criminal vs. civil trade secret standards

(a) California Penal Code § 499c defines a trade secret as "scientific or technical information, design, process, procedure, formula, computer program or information stored in a computer . . . ."

(b) This may be a narrower definition than most civil definitions, though it is unclear whether non-technical business information is included.

(2) It is a crime (theft) to

(a) steal, take or use a trade secret without authorization.

(b) copy it without authority.

(c) To bribe or conspire with someone else to steal, use or copy a trade secret also is a crime.

(d) It is <u>not</u> a defense that the criminal returned or intended to return the trade secret to its owner.

(3) Special prosecution teams exist in several counties:

(a) Santa Clara County, California District Attorney's Office has High Tech and Computer Crimes Unit.

(b) others may not have the resources or expertise to prosecute.

(4) Federal criminal statutes:

(a) 18 U.S.C. §§ 1831 - 1839 -- the Economic Espionage Act.

This federal statute is aimed specifically at trade secret misappropriation, and contains provisions similar to Cal. Pen. Code 499c (including a definition of "trade secret" that coincides with that of the UTSA). Section 1832 deals with the theft of trade secrets generally (as opposed to "economic espionage," or the theft of trade secrets for the benefit of foreign governments, addressed in section 1831). Section 1832 requires proof of the defendant's "intent to convert a trade secret," and that the trade secret at issue be "related to or included in a product that is produced for or placed in interstate or foreign commerce." This last provision casts some doubt on whether trade secret information that is not related to or included in a product" is covered by the statute; an argument may exist that this law does not punish thefts of pure research information or service-related data (for example). Trade Secrets, § 13.9A, p. 410.

Punishment for violation is a fine of up to $250,000 (see 18 U.S.C. § 3571), imprisonment for up to ten years, or both. "Organizations" (including business entities) convicted under this statute face fines of up to $5 million. Section 1834 also allows the court, in addition to the sentence imposed, to order violators to forfeit to the Unites States any property or proceeds resulting from the violation or used in connection with the violation.

(b) 18 U.S.C. § 1030 -- the "computer crimes" statute.

This statute does not expressly deal with trade secrets, but does criminalize the use of computers during the course of other activities (particularly during the conduct of otherwise fraudulent actions). One provision is of particular interest: Section 1030(a)(5) makes it a crime to knowingly transmit a program, information, code, or command with the intent thereby to cause unauthorized damage to

another computer (or otherwise intentionally to access another computer without authorization and thereby cause damage). This provision criminalizes many activities, such as the transmission of computer viruses and so-called software "time bombs" (i.e., bits of code that can be used to disable software programs at a pre-set time or date). See North Texas Preventive Imaging, LLC v. Eisenberg, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. Aug. 19, 1996). Violations are punishable by fines of up to $250,000 (see 18 U.S.C. § 3571), imprisonment for one to twenty years, or both.

(c) 18 U.S.C. §§ 1341, 1343 -- mail and wire fraud.

Sections 1341 and 1343 prohibit schemes to defraud or obtain money or other property by false or fraudulent pretenses via use of the United States Postal Service (mail fraud) or wire, radio or television communications, or writings, signs, signals, pictures, or sounds (wire fraud). Trade secrets and other confidential information qualify as "property" under these statutes. Trade Secrets, § 13.6, p. 407; Carpenter v. U.S., 484 U.S. 19, 26 (1987); U.S. v. Louderman, 576 F.2d 1383, 1387 (9th Cir. 1978) cert. denied, 439 U.S. 896 (1978). Punishment for violations of these statutes is a fine of up to $250,000 (see 18 U.S.C. § 3571), imprisonment for up to five years, or both. Because these statutes define elements of a crime that are easier to prove that those of the Economic Espionage Act, federal prosecutors often may prosecute a trade secrets case under the mail and wire fraud statutes.

(d) 18 U.S.C. §§ 1961 - 1968 -- RICO

The federal Racketeer Influenced and Corrupt Organizations Act ("RICO") allows the federal government to bring criminal proceedings alleging that stealing trade secrets constitutes the forming of an "enterprise" to engage in "a pattern of racketeering activity." Trade Secrets, § 13.7, p. 408. A RICO violation requires continuity of the illegal conduct; a single act of trade secret theft may

not be enough. Compare Celpaco, Inc. v. MD Papierfabriken, 686 F. Supp. 983 (D. Conn. 1988) (no RICO violation because scheme to use plaintiff's trade secret customer lists lasted no longer than time needed to steal the lists) with General Motors Corp. v. Ignacio Lopez de Arriortua, 948 F. Supp. 670 (E.D. Mich. 1996) (civil action; pattern of trade secret misappropriation can be established by multiple acts within a "single scheme"). Punishment for violation is a fine of up to $250,000 (see 18 U.S.C. 3571), imprisonment for up to twenty years (or both), plus forfeiture of all proceeds of the racketeering activity. The injured party may also bring a civil action for treble damages, attorneys' fees, and costs.

(e) 18 U.S.C. §§ 2311 - 2333 -- the National Stolen Property Act.

This federal statute, similar to Cal. Pen. Code § 496, prohibits (among other things) the receipt, sale, or transportation in interstate or foreign commerce stolen "goods, wares, merchandise, securities, or money, of the value of $5,000 or more." Based on a theory that stolen trade secrets are "goods, wares, [or] merchandise," this statute can apply to trade secret theft (assuming the value of the information is at least $5,000). Trade Secrets, § 13.8, p. 408-409.

A critical issue for this statute is whether the trade secrets must be embodied in some physical form, or whether mere electronic transmission of data qualifies. See Dowling v. U.S., 473 U.S. 207 (1985) (some physical embodiment required); United States v. Brown, 925 F.2d 1301 (10th Cir. 1991) (stolen property must have a tangible form, no matter what its value (such as a computer disk or file folder), to fall under section 2314, holding that "purely intellectual property" was not covered); but see United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990) (analogizing a stolen computer file transported exclusively via electronic means to an imperceptible gas stored and moved across state

lines, and concluding that the stolen file fell within the statutory definition of "goods, wares, [or] merchandise"). Violation is punishable by fines of up to $250,000 (see 18 U.S.C. § 3571), imprisonment of up to ten years, or both.

(f) 18 U.S.C. § 1029 -- fraud in connection with access device.

This federal statute criminalizes many activities performed with counterfeit or unauthorized "access devices," defined as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." Trade Secrets, § 13.9, p. 410. In particular, it is a crime to use a counterfeit or unauthorized access device to obtain money, goods, services, *or any other thing of value*. 18 U.S.C. § 1029(a),(e)(1). If a trade secret (by definition a "thing of value") was obtained in this way, this statute could apply. Punishment for violation is a fine of at least twice the value of the thing obtained (or $250,000, whichever is *greater),* imprisonment of up to twenty years, or both.

f. Impact on civil action where parallel criminal action is brought.

(1) Civil action effectively stayed.

(2) More difficult to protect the company's trade secrets from disclosure in the criminal action.

(a) Scope of what may be protected is much narrower. Calif. Evidence Code § 1061 sets forth the procedure to apply for a protective order to protect the confidentiality of trade secrets in criminal cases.

(b) Criminal defendant's constitutional rights to fair and public trial are given great weight

g. Other considerations

(1) No control over scope, timing, publicity or outcome.

(2) No injunction unless a civil suit also brought.

(3) Consequences severe for the defendants if convicted.

(4) Possible exposure of the company to collateral civil actions, e.g. from shareholders

2. Alternate/Additional Theory of Liability: Breach of Fiduciary Duty

a. A claim for breach of fiduciary duty is often alleged together with a trade secret misappropriation claim. It can serve as a companion to a trade secrets claim, or it can stand alone. A fiduciary duty claim can be particularly helpful where a former employee may not have misappropriated trade secrets, but nonetheless, may have taken company property, and the company desires a remedy. For instance, while a customer list may not necessarily constitute trade secret information, the taking of such a list by a former employee may constitute a breach of fiduciary duty.

It is well established that the physical taking or disclosure of a company's property or information by an employee who has a fiduciary duty to the company may give rise to a claim for breach of fiduciary duty, even where the property contains no trade secret or confidential information. UFG International, Inc. v. DeWitt Stern Group, Inc., 1998 U.S. Dist. LEXIS 15216 (1998).

b. This concept of fiduciary duty with regard to confidential information is well-established. In Bancroft-Whitney Co. v. Glen, 64 Cal. 2d 327 (1966), the California Supreme Court held that an executive's disclosure to a competitor of a confidential, unpublished list of desirable employees and their salaries constituted a breach of fiduciary duty.

The president of Bancroft-Whitney (a publisher of legal texts), while still employed by the company, negotiated with Bancroft's main competitor, Bender, to join the company, and to entice Bancroft editors to follow. In the course of these negotiations, the president revealed to Bender a detailed list of current Bancroft editors, their salaries, and the factors which made them desirable

employees, which Bender and the president utilized to make employment offers to the editors.

The court concluded that the president breached his fiduciary duty to Bancroft. The court stated that "[c]orporate officers and directors are not permitted to use their position of trust and confidence to further their private interests. While technically not trustees, they stand in a fiduciary relation to the corporation and its stockholders. "The mere fact that an officer makes preparations to compete before he resigns his office is not sufficient to constitute a breach of duty." It is the nature of his preparations which is significant." It is beyond question that a corporate officer breaches his fiduciary duties when, with the purpose of facilitating the recruiting of the corporations' employees by a competitor, he supplies the competitor with a selective list of the corporation's employees who are, in his judgment, possessed of both ability and the personal characteristics desirable in an employee, together with the salary the corporation is paying the employee."

c. Which employees are bound by a fiduciary duty?

(1) Do only high level employees (directors, officers, managers) have a fiduciary duty to their employer? No.

(2) Must an employee sign a confidentiality agreement and/or non-disclosure agreement (NDA) before he or she is found to bear a fiduciary duty to the company regarding confidential information? No.

See Envirotech Corp. v. Callahan, 872 P.2d 487 (Ct. App. Utah 1994), *cert. denied*, 883 P. 2d 1359 ("A written contract or formal employment contract is not required in order to create this duty. It is settled . . . that the duty of an employee not to disclose confidential information is grounded on basic principles of equity . . . and upon an implied contract, growing out of the nature of the employer-employee relation . . . . This duty does not turn on the existence of a legally enforceable contract").

d. When does the fiduciary duty end/expire?

(1) Does the fiduciary duty end upon termination of employment? Generally, yes.

See First Equity Devp't, Inc. v. Risko, 1998 WL 294061, 1998 Conn. Super. LEXIS 1475 (1998) (the fiduciary duty owed by an officer or director of a corporation does not continue "ad infinitum after the officer or director terminates employment with the company . . . there is no Connecticut case which has found a fiduciary relationship to exist between an ex-officer or ex-director and its former employer").

Envirotech, supra (Plaintiff's former sales manager, who retired from Envirotech nearly three years before starting new company, breached a fiduciary duty to Envirotech when he took, while still an employee of Envirotech, confidential information with him to the new company, and failed to preserve other confidential information to which he was privy, despite defendant's argument that he did not owe the company a fiduciary duty three years after his employment terminated).

e. Cases Supporting Breach of Fiduciary Duty

(1) UFG Int'l, Inc. v. DeWitt, supra.

Although customer lists ordinarily are not trade secrets or confidential information, a physical taking of the lists may give rise to a claim for breach of fiduciary duty.

(2) Bancroft-Whitney, supra.

f. Cases Rejecting Breach of Fiduciary Duty

(1) Pony Computer v. Equus Computer Etc., 162 F.3d 991 (8th Cir. 1998).

Where former employer based breach of fiduciary duty claim against former employees on the fact that they could only access the employer's computer system with a password, such that each employee must have known of the confidential nature of the information, trial court correctly entered summary judgment in favor of defendant employees.

"A confidential relationship between employer and employee giving rise to fiduciary duties exists if (1) there is an express understanding that the employee is receiving confidential information, or (2) the employee acquired the

information in such a way that he must have known of its confidential nature."

(2) Western Medical v. Johnson, 80 F.3d 1331 (9th Cir. 1996).

Employee's failure to disclose her intent to open a new business in another state which would compete with her employer did not constitute a breach of fiduciary duty to the employer; the employee had no affirmative obligation to disclose her plans to leave.

3. Website publication of trade secret may not be enjoined.

In O'Grady v. Superior Court, 139 Cal. App. 4th 1423 (2006), Apple Computer sought authority to issue civil subpoenas to the publishers of a Web site to uncover the source of misappropriated trade secret information published on the site– including illustrations, marketing plans and product details. The defendants moved for a protective order on multiple grounds, including that the requested information was protected by the reporter's privilege provided by free press guarantees. The Court of Appeal directed the trial court to grant the protective order, holding that where trade secret law and free speech rights collide "it is the quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information." Id. at 1476. In balancing these interests, the court emphasized the "newsworthiness" of the pending product release and downplayed the potential harm to the company resulting from the disclosure of the proprietary information. Though, not ruling on whether the disclosed information constituted a trade secret, the court held that the protection of "confidential marketing plans," that provide no proprietary technology that could help anyone build a competing product, has no "direct and obvious tendency to serve the central purposes of the law (misappropriation law)." Id. at 1467-1467. The opinion thus suggests that even when the trade secret owner has no other means to obtain essential information necessary to protect its trade secrets, the courts may refuse to require disclosure when the trade secret concerns matters of great public importance.

4. Choice of forum.

a. What are the key considerations in choosing a forum?

(1) Jurisdiction over defendants

(a) See generally Efco Corp. v. Aluma Sys., USA, Inc., 983 F. Supp. 816, 818–23 (S.D. Iowa 1997) (providing an extended discussion of personal jurisdiction in the context of trade secrets litigation).

(2) Discovery procedures of the forums

(3) Available remedies

(a) Jurisdictional fora differ with regard to the more unusual remedies available. Besides injunctive relief and damages (discussed supra), litigation strategy considers the receptiveness of the forum to replevin, destruction of physical property, impressments of a trust, and, in some cases, the assignment of patents or patent applications.

(b) Replevin or Destruction of Physical Property

(i) Available where value is embodied in some tangible object, such as plans or machinery.

(ii) See, e.g., Remington Rand Corp. v. Business Sys. Inc., 830 F.2d 1260, 1269–70 (3d Cir. 1987) (voluminous documentation); Institutional Management Corp. v. Translation Sys., Inc., 456 F. Supp. 661, 669–71 (D. Md. 1978) (computer program materials); Picker Int'l, Inc. v. Blanton, 756 F. Supp. 971, 983 (technical service manuals); Standard Brands, Inc. v. U.S. Partition & Packaging Corp., 199 F. Supp. 161, 175 (E.D. Wis. 1961) (drawings and copies); Kelite Corp. v. Chem Chems., Inc., 162 F. Supp. 332, 337 (N.D. Ill. 1958) (chemical formulas and customer lists); Telex Corp. v. IBM, 367 F. Supp. 258 (N.D. Okla. 1973) (manuals).

(c) Impressment of Trust

(i) Generally regarded as a drastic and unusual remedy. See, e.g., Remington Rand Corp. v. Business Sys. Inc., 830 F.2d 1260, 1269–70

(3d Cir. 1987) (imposing a constructive trust on plans and drawings).

(d) Assignment of Patents or Patent Applications

(i) If defendant wrongfully appropriated plaintiff's trade secrets and applied for (or obtained) patents, plaintiff can seek assignment of the patent applications or patents. See Monovis, Inc. v. Aquino, 905 F. Supp. 1205, 1235 (W.D.N.Y. 1994); De Long Corp. v. Lucas, 176 F. Supp. 105, 134 (S.D.N.Y. 1959); Carter Prods., Inc. v. Colgate Palmolive Co., 230 F.2d 855, 865 (4th Cir.), *cert. denied*, 352 U.S. 843 (1956); Liquid Carbonic Corp. v. Goodyear Tire & Rubber Co., 38 F. Supp. 520, 524–27 (E.D. Ohio 1940); Paley v. DuPont Rayon Co., 71 F.2d 856, 858 (7th Cir. 1934); Ransburg Electro Casting Corp. v. DeVilbiss Co., 340 F. Supp. 1385 (N.D. Ill. 1971).

(ii) Allen Qualley Co. v. Shellmar Prods. Co., 31 F.2d 293 (N.D. Ill.), aff'd, 36 F.2d 623 (7th Cir. 1929), later history, 87 F.2d 104, 109, 32 U.S.P.Q. 24 (1936), cert. denied, 301 U.S. 695 (1937)

In the often cited Allen Qualley Co., Allen-Qualley had disclosed an invention (candy bar wrap and the processes and machinery for making it) to Shellmar in confidence. Allen-Qualley obtained an injunction against Shellmar's use of its methods to produce the wrap. After certain patents had issued which disclosed the wrap and process, Shellmar sought relief from the injunction on the ground the information was no longer secret. The Seventh Circuit affirmed the district court's denial of relief, however, stating that "the consensus of authority is that by its inequitable conduct [Shellmar] has precluded itself from enjoying [the rights of the general public to] the patent disclosure . . . ."

(4) Judicial receptivity (or hostility)

(a) California's pro-employee inclination has its roots in the California Business and Professions Code section 16600, discussed above.

(b) Georgia is among the most difficult states for an employer to obtain enforcement of an employment-related non-compete agreement as a result of its Supreme Court's interpretation of Article III of the Georgia Constitution, which disallows enforcement of contracts that defeat or lessen competition. GA. CONST. art. III, § 6, ¶ V(c). If a court finds a single term or clause of a noncompetition agreement ancillary to an employment agreement to be unreasonable, the court will refuse to enforce the entire covenant, as well as any other noncompetition agreements within the overall employment agreement. See, e.g., Advance Tech. Consultants, Inc. v. RoadTrac, LLC, 551 S.E.2d 735, 737-38 (Ga. Ct. App. 2001).

(c) The "Blue Penciling" issue: Many states support the partial enforcement approach, which permits courts to modify, rather than strike in its entirety, an unreasonably worded covenant. See Ehlers v. Iowa Warehouse Co., 188 N.W.2d 368, 370, 372 (Iowa 1971); Bess v. Bothman, 257 N.W.2d 791, 795 (Minn. 1977); Solari Indus. Inc. v. Malady, 264 A.2d 53, 56, 61 (N.J. 1970); Raimonde v. Van Vlerah, 325 N.E.2d 544, 546–49 (Ohio 1975); Wood v. May, 438 P.2d 587, 591 (Wash. 1968); Fullerton Lumber Co. v. Torborg, 70 N.W.2d 585, 592 (Wis. 1955).

California courts will strike offending language while preserving any enforceable language. However, California courts will not write an agreement not negotiated nor will they enforce an agreement putrid with illegal covenants.

(d) There are signs Georgia may not continue in its pro-employee direction. In Palmer & Cay of Ga., Inc. v. Lockton Cos., 629 S.E.2d 800 (Ga. 2006) the Georgia Supreme Court reversed a lower court

decision that refused to enforce a potentially overbroad non-compete agreement. In its opinion, the court emphasized that refusal to enforce such agreements would adversely impact the "state's business climate."

(5) Maximizing Substantive and Remedies Law

(a) Careful analysis of applicable substantive law and remedies available in a state or federal action may garner the best of all possible worlds. See Bryan v. Kershaw, 366 F.2d 497, 500, 503–04 (5th Cir. 1966), cert. denied, 386 U.S. 959 (1967) (applying Texas substantive and federal remedies law, both favorable to the plaintiff).

b. Who decides the forum?

(1) Typically, the plaintiff trade secret owner selects a forum. The exception is when the owner threatens an imminent proceeding in such a way as to permit a prospective defendant to assert a declaratory judgment action. See Enron Capital & Trade Resources Corp. v. Polasky, 490 S.E.2d 136, 138 (Ga. App. Ct. 1997) (declaratory judgment available where a legal judgment is sought that would control or direct future action like ongoing competition and employment).

(2) The "race to the courthouse."

(a) In most states, a court may not issue a temporary restraining order (TRO) enjoining a person from filing an action in another state, except where it would prevent a multiplicity of lawsuits. See Advanced Bionics v. Medtronic, 29 Cal. 4th 697, 702 (2002); Golden Rule Ins. Co. v. Harper, 925 S.W.2d 649, 651 (Tex. 1996); Gannon v. Payne, 706 S.W.2d 304, 306 (Tex. 1986); Arpels v. Arpels, 170 N.E.2d 670, 671 (N.Y. 1960); Pfaff v. Chrysler Corp., 610 N.E.2d 51 (Ill. 1992).

(i) Advanced Bionics v. Medtronic, 29 Cal. 4th 697 (2002)

In Advanced Bionics, a Minnesota employer

sought in Minnesota to enforce a covenant not to compete against its former employee and his new, California-based employer. Shortly after the employee and new employer filed a lawsuit in California seeking declaratory relief as to the invalidity of the noncompetition covenant, the former employer filed a parallel lawsuit in Minnesota. A judicial melee ensued, with the two courts taking conflicting positions and granting conflicting injunctions and restraining orders. The California Court of Appeal held that—despite a Minnesota choice of law provision in the agreement—the dispute should be litigated in California and California law should determine the rights of the parties because (1) the Minnesota law governing covenants not to compete was contrary to California's fundamental policy against covenants not to compete, (2) California had a materially greater interest than Minnesota in enforcing its law, and (3) the California action was filed first (even if the Minnesota court entered judgment first in the subsequently filed action).

The California Supreme Court reversed, holding that the Court of Appeal had exceeded its jurisdiction, and that a California court could not enjoin a party subject to parallel jurisdiction in another state from commencing litigation over a noncompetition agreement in another state.

(b) That two lawsuits may proceed concurrently results in the possibility that one action may lead to a judgment first and then be applied as res judicata in another action. Courts addressing this possibility have regarded it as "a natural consequence of parallel proceedings in courts with concurrent jurisdiction, and not reason for an injunction." Auerbach v. Frank, 685 A.2d 404, 407 (D.C. 1996). Moreover, "[T]he possibility of an 'embarrassing

race to judgment' or potentially inconsistent adjudications does not outweigh the respect and deference owed to independent foreign proceedings." Id.; see also Advanced Bionics, 29 Cal. 4th at 706.

(c) Therefore, what results is a need by the employer to file any action immediately with the appropriate jurisdiction so as to obtain a binding judgment that can be considered *res judicata* in any subsequent filing.

(d) Moreover, companies often send "cease and desist" letters prior to an enforcement action. Now, prolonged letter writing may no longer be a useful tactic against a former employee willing to rush to the courthouse to obtain a declaratory judgment in a favorable jurisdiction.

(e) The result is litigants must balance the merits of a forum where jurisdiction is easily obtained and where quick trigger dockets allow for an early hearing on a temporary restraining order to be set against the importance of a foreign forum applying unfavorable law. Litigation strategy must recognize that it is not the first court that enters a TRO or preliminary injunction, but the first to enter a final judgment that will have its judgment followed in other jurisdictions. See Hulcher Servs. Inc. v. R.J. Corman R.R. Co., 543 S.E.2d 461, 464 (Ga. C. App. 2000) (not first injunction, but final adjudication of the merits entitled to claim preclusive effect).

(f) The impact of the race to the courthouse may be somewhat tempered, however, by recent cases that restrict the permissible breadth of an injunction.

(i) Keener v. Convergys Corp., 342 F.3d 1264, 1271 (11th Cir. 2003)

In Keener, the Eleventh Circuit restricted the scope of Georgia courts' ability to invalidate noncompetition agreements by limiting the courts' ability to enjoin a party's

enforcement attempts. Before Keener, the Georgia Court of Appeals had enjoined an employer from attempting to enforce a noncompetition agreement to which Georgia law applied and invalidated, on a global scale. Enron Capital & Trade Res. Corp. v. Pokalsky, 490 S.E.2d 136, 138–39 (Ga. Ct. App. 1997). The district court, in trying Keener, followed this precedent and crafted an injunction against the employer that was also global in scope, effectively rescinding the contract and allowing the employee to compete at will.

The Eleventh Circuit, in Keener, curtailed this worldwide injunctive relief for noncompetition agreements that violate Georgia public policy. The court held that Georgia may only apply its public policy within the borders of the state. Therefore, a Georgia court that strikes down a noncompetition agreement can only enjoin the employer-promisee from enforcing the covenant within Georgia. The court implicitly overruled the Georgia Court of Appeals' injunctive technique in Enron.

* * * * * * * * * * * * *