

**PROTECTING TRADE SECRETS IN
A DIGITAL WORLD**

by

**Francis J. Burke, Jr.
Mark G. Kisicki
and John B. Nickerson**

June 18, 2003

**STEPTOE & JOHNSON LLP
201 E. Washington Street, Suite 1600
Phoenix, Arizona 85004-2382**

**PROTECTING TRADE SECRETS IN
A DIGITAL WORLD**

Table of Contents

I. PROTECTING TRADE SECRETS IN A NETWORKED ENVIRONMENT.....	1
I. A. Definition of a Trade Secret	1
II. B. Misappropriation of Trade Secrets.....	5
III. C. The Economic Espionage Act, 18 U.S.C. §§ 1831-1835.....	6
IV. D. Liability Under the EEA.....	8
V. E. Liability Under the CFAA.....	100
VI. F. Practical Considerations.....	15
VII. G. Remedies.....	17
II. DEVELOPING TRADE SECRET PROTECTION POLICIES AND APPROPRIATE NON-DISCLOSURE AGREEMENTS	19
VIII. A. Rationale for Efforts to Preserve Secrecy	199
IX. B. Traditional Prudent Efforts to Preserve Secrecy:..	22
X. C. Efforts to Preserve Secrecy In The Digital Environment:	23
XI. D. Click Wrap, Shrink Wrap and Browse Wrap Agreements and Licenses.....	25
XII. E. Technology Measures That Control Access: The Digital Millennium Copyright Act.....	29
XIII. F. Non-Disclosure/Confidentiality Agreements.....	31
XIV. G. Checklist For Exit Interview	34

XV. H. Post-Departure Investigation: Damage Assessment	35
XVI. I. Computer Forensics Tips When You Know You Have a Problem	36
XVII. J. Countermeasures Short of Litigation.....	36
III. THE ENFORCEABILITY OF NON-COMPETITION AGREEMENTS.....	36
XVIII. A. California	36
XIX. B. Arizona	37
XX. C. Oregon	40
XXI. D. Washington.....	41
XXII. E. Colorado	42
XXIII. F. Restrictive Covenants Involving the Internet:.....	45
XXIV. G. Other Types of Agreements Which Limit New Employment:	446
IV. THE ENFORCEABILITY OF NON-SOLICITATION CLAUSES.....	47
XXV. A. Non-Solicitation Agreements – No Recruit Clauses In General	47
XXVI. B. California	48
XXVII. C. Arizona.....	49
XXVIII. D. Oregon	50
XXIX. E. Washington.....	50
XXX. F. Colorado	51
V. INEVITABLE DISCLOSURE AND INTERNET RELATED CASE LAW.....	51
XXXI. A. Inevitable Disclosure Doctrine.....	51
XXXII. B. Trade Secrets on the Internet: Putting the Genie	

Back Into the Bottle	57
VI. FORMS APPENDIX	67
XXXIII. A. Sample E-mail Policy	68
XXXIV. B. Sample Investigation Questionnaire	69
XXXV. C. Sample Non-Compete, Non-Solicitation Clause..	71
XXXVI. D. Sample Non-Disclosure Clause.....	72
XXXVII. E. Confidentiality and Non-Disclosure Agreement..	73
XXXVIII. F. Forms of Residuals Clauses	77

**PROTECTING TRADE SECRETS IN
A DIGITAL WORLD**

By Francis J. Burke, Jr., Mark G. Kisicki and John B. Nickerson

**STEPTOE & JOHNSON LLP
May 2003**

I. PROTECTING TRADE SECRETS IN A NETWORKED ENVIRONMENT

A. Definition of a Trade Secret

1. Legal Definition

- a. The Uniform Trade Secrets Act defines a trade secret as:

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique or process, that:

- (i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
- (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

See, A.R.S. § 44-401, RCW 19.108.010.

California uses this definition:

“Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- (i) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
- (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. *California Civil Code § 3426.1(d)*

Colorado uses this definition:

“Trade secret” means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value. To be a “trade secret” the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes. *C.R.S. § 7-74-102*

Oregon uses this definition:

“Trade secret” means information, including a drawing, cost data, customer list, formula, pattern, compilation, program, device, method, technique or process that:

- (a) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
- (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. *O.R.S. § 646.461*

- b. Restatement of Torts §757 provides the following definition of a trade secret:

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

(i) *See, Enterprise Leasing Co. v. Ehmke*, 197 Ariz. 144, 148-149, 3 P.2d 1064, 1068-69 (2000) (Applies the Restatement of Torts §157 six-prong test to determine whether the Uniform Trade Secret Act standard is met.)

c. This was modified under the Restatement Third of Unfair Competition which defines in §39 a trade secret as:

“Any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual potential economic advantage over others.”

2. Shorthand Definition

- a. Is the information generally known in the industry?
- b. Would the information be valuable to a competitor?
- c. Have you made efforts to keep the information confidential?

If the answers are “no,” “yes,” and “yes,” respectively, then the information is probably a trade secret. Note that you need not be a high tech company to possess trade secrets.

3. Examples of Trade Secrets:

- a. Computer software systems, *see Rivendell Forest Products, Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042 (10th Cir. 1994); *InFlight Newspapers v. Magazines in-Flight*, 990 F. Supp. 119, 130 (E.D.N.Y. 1997); *Cybertek Computer Products, Inc. v. Whitfield*, 203 U.S.P.Q. 1020 (Cal. Super. 1997); *Ward v. Superior Court*, 3 Computer Law Service Rptr. 206 (Cal. Super. 1972) and *GCA Corporation v. Chance*, 217 U.S.P.Q. 718 (N.D. Cal. 1982).

- b. Computer hardware, *see Forro Precision, Inc. v. IBM*, 673 F.2d 1045 (9th Cir. 1982) and *Digital Development Corp. v. International Memory Systems*, 185 U.S.P.Q. 136 (S.D. Cal. 1973).
- c. Customer lists, *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), cert dismissed, 510 U.S. 1033 (1994); *United Ribbon Co. v. Coast to Coast Computer Products, Inc.*, 2002 WL 922940 (Cal. App. 2 Dist. May 8, 2002). (The Court found that a customer list was a trade secret. It was more than the mere compilation of businesses that use imaging supplies. It contained the name of a contact person, the type of equipment the target customer used, the frequency contact or type of its purchases.)
- d. Customer product use and preferences, *Ecolab v. Paolo*, 753 F. Supp. 1100, 1112 (E.D.N.Y. 1991)
- e. Other customer information, *Doubleclick, Inc. v. Henderson*, 1997 WL 731413 (N.Y. Sup. Ct. Nov. 7, 1997); information about competitive pricing and marketing of products, *Schlage Lock Company v. Whyte*, 101 Cal. App. 4th 1443, 125 Cal. Rptr. 2d 277 (Cal. App. 2002); business plans, marketing strategies and customer information, *Sunbelt Rentals, Inc. v. Head & Engquist Equipment, LLC*, 2002 WL 31002955 (N.C. Super. July 10, 2002).
- f. Customer insurance policy data, *John Hancock Mutual Life Ins. Co. v. Austin*, 916 F. Supp. 158, 164 (N.D.N.Y. 1996)
- g. Internal cost information, *Lumex Inc. v. Highsmith*, 919 F. Supp. 624, 629-30 (E.D.N.Y. 1996)
- h. Production processes, *see, General Electric Company v. Chien-Min Sung*, 843 F. Supp. 776 (D. Mass 1994)
- i. Formulas and recipes, *see, Natural Organics, Inc. v. Proteins Plus, Inc.*, 724 F. Supp. 50, 53 (E.D. N.Y. 1989); In the *Marie Callendar Pie Shops, Inc. v. Bumbleberry Enters., Inc.*, 39 Ore. App. 487, 592 P.2d 1050, 1051 (1979)
- j. Profit margins, *Cardinal Freight Carriers, Inc. v. J.B. Hunt Transport Servs., Inc.*, 336 Ark. 143, 147-149, 987 S.W. 2d 642, 644-645 (1999)

- k. Product strategies, *see, Merck & Co. v. Lyon*, 941 F. Supp. 1443, 1449-50 (M.D.N.C. 1996); *La Calhene, Inc. v. Spolyar*, 938 F.Supp. 523, 530 (W.D.Wis. 1996)
 - l. Know-how, *Picker Int'l Corp. v. Imaging Equip. Servs. Inc.*, 1995 U.S. Dist. LEXIS 11622 (D. Mass. 1995)
 - m. Machine design, process design, combination of processes, *BBA Nonwovens Simpsonville, Inc. v. Superior Nonwovens, LLC*, 303 F.3d 1332 (Fed. Cir. 2002).
4. General Skill and Ability
- a. The knowledge, skills and talents the employees gained while in employed at a company, even if at the company's expense, are not the company's trade secrets. *Amex Distrib. Co. v. Mascari*, 150 Ariz. 510, 515, 724 P.2d 596, 601 (Ct. App. 1986); *Rigging Int'l Maintenance Co. v. Gwin*, 128 Cal. App. 3d 594, 180 Cal. Rptr. 451, 457 (1st Dist. 1981); *McCombs v. McClelland*, 223 Ore. 475, 354 P.2d 311, 316 (1960); *Ed Nowogroski Ins. Inc. v. Rucker*, 137 Wash. 2d 427, 434-435, 971 P.2d 936, 940 (1999). Thus, a company cannot prohibit its former employees from using their general expertise for a competitor.
 - b. *Moss, Adams & Co. v. Shilling*, 179 Cal. App. 3rd 124, 127-130, 224 Cal. Rptr. 456 (1st Dist. 1986) (Individual defendants who service retail customers over a long period of time and who know their names and addresses from that activity are not barred from using information pertaining to such customers.)

B. Misappropriation of Trade Secrets

1. Actual Misappropriation

The Uniform Trade Secrets Act defines the misappropriation of a trade secret as:

- a. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.

- b. Disclosure or use of a trade secret of another without express or implied consent by a person who either:
 - (i) Used improper means to acquire knowledge of the trade secret; or
 - (ii) At the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it, was acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use or was derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
 - (iii) Before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

See, e.g., California Civil Code § 3426.1(b), A.R.S. § 44-401, C.R.S. § 7.74-102, O.R.S. § 646.461, RCW 19.108.010. See also *PMC, Inc. v. Kadisha*, 78 Cal. App. 4th 1368, 1385-89, 93 Cal. Rptr. 2d 663, 675-679 (2nd Dist. 2000) (Use and continuing use of trade secrets can be a misappropriation.); *Cadence Design Systems, Inc. v. Avant! Corp.*, 29 Cal. 4th 215, 57 P.3d 647 (2002). (The continued improper use or disclosure of a trade secret after defendant’s initial misappropriation was viewed under the UTSA as part of a single claim of “continuing misappropriation” occurring at the time of the initial misappropriation.)

C. The Economic Espionage Act, 18 U.S.C. §§ 1831-1835

1. Definition of Trade Secret

- a. EEA definition: “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –
- b. the owner thereof has taken reasonable measures to keep such information secret; and

- c. the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public ...” 18 U.S.C. § 1839(3).
 - d. This definition builds on the definition used in the UTSA, but has two important differences:
 - (i) It updates the definition to make it more applicable to computer crimes, because it more clearly applies to intangible secrets, and to improper transmission of trade secrets by the use of computers.
 - (ii) Under the UTSA, a trade secret is information not generally known to or readily ascertainable by businesspersons or competitors of the owner of the trade secrets. However, under the EEA, a trade secret is information not generally known to or readily ascertainable by the public. *See generally* Arthur J. Schwab and David J. Porter, *Federal Protection of Trade Secrets: Understanding the Economic Espionage Act of 1996*, 4 J. Prop. Rts. 107 (1998).
 - (iii) *United States v. Hsu*, 155 F.3d 189, 195-196 (3rd Cir. 1998) (The Uniform Trade Secret Act definition of a trade secret in Section 1(4) is largely tracked in the Economic Espionage Act, 18 U.S.C. Sections 1831-1839.)
2. Definition of Owner
- a. The EEA defines the owner of a trade secret as a “person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.” 18 U.S.C. § 1839(4).
 - b. This definition may mean that a licensee’s use or disclosure of a trade secret beyond the license agreement is not a violation of the EEA. In this sense, the EEA is more limited than the UTSA, which does cover wrongful use of a trade secret by a licensee.
3. The EEA provides broader coverage than other federal laws, and the UTSA better applies to intangible trade secrets, and crimes involving computers:

- a. The definition explicitly recognizes intangible property.
 - b. The statute applies if someone memorizes a trade secret, even one that exists only in the mind, and later uses it or passes it on. Arthur J. Schwab and David J. Porter, *Federal Protection of Trade Secrets: Understanding the Economic Espionage Act of 1996*, 4 J. Prop. Rts. 107 (1998).
 - c. *See, United States v. Martin*, 228 F.3rd 1, 6, 13 (1st Cir. 2000) (A conviction for conspiracy to steal trade secrets was affirmed even though the matter that was the subject of months of communications between the defendants would not qualify as a trade secret.)
4. The requirement that the secret be “related to or included in a product that is produced for or placed in interstate commerce” could limit prosecutions in cases where a service is involved, or the product is being developed but is not yet being sold.

D. Liability Under the EEA

1. Conduct Proscribed
 - a. The EEA has two basic proscriptions, one aimed at general theft or misappropriation (*18 U.S.C. § 1832*), and one aimed at theft or misappropriation for the benefit of a foreign agent or entity. *18 U.S.C. § 1831*.
 - b. In each case, the Act is aimed at those who steal or otherwise misappropriate trade secrets, those who receive misappropriated trade secrets, and those who conspire to steal or misappropriate or receive trade secrets. More specifically, it applies to one who “(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense

described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), . . .” *18 U.S.C. § 1831 and 1832.*

- c. Where the crime is charged under § 1832, the provision applying to general theft and misappropriation, the prosecutor must also show that
 - (i) the actor intended to convert a trade secret . . . “to the economic benefit of anyone other than the owner thereof,”
 - (ii) that the trade secret is “related to or included in a product that is produced for or placed in interstate or foreign commerce,”
 - (iii) and that the actor intended or knew his acts would injure the owner of the trade secret. *18 U.S.C. § 1832*

- d. Where the prosecution is charged under § 1831, the section aimed foreign theft or misappropriation, it must be shown that the actor intended the acts to benefit “any foreign government, foreign instrumentality, or foreign agent . . .” *18 U.S.C. § 1831.* Congress intended this section of the statute to be aimed economic espionage that is sponsored or coordinated by a foreign government. *142 Cong. Rec. S12,212 (daily ed. Oct. 2 1996 (Managers’ Statement for H.R. 3723)).*
 - (i) Note that while the provision relating to general theft of trade secrets requires that the prosecution show an intent to confer an economic benefit on someone, the section relation to theft for the benefit of foreign agents and instrumentalities requires only an intent to confer any benefit.
 - (ii) In addition, the general provision contains a requirement that the government show an intent to harm the rightful owner of the secret. This requirement is missing from the section pertaining to theft and misappropriation of secrets to benefit foreign agents and instrumentalities.

- e. The territorial reach of this statute is broad. It applies to conduct occurring outside the United States if “(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States.” 18 U.S.C. § 1837

E. Liability Under the CFAA

1. A theft or misappropriation of trade secrets from a computer or website may be a violation of the Computer Fraud Act, 18 U.S.C. §1030, which provides for civil remedies. “Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. §1030(g).
2. In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), a civil action under the Computer Fraud and Abuse Act, the plaintiff alleged that the defendant embarked on a systematic scheme to hire away key employees for the purpose of obtaining the plaintiff’s trade secrets and that some of these employees while still working for the plaintiff used the plaintiff’s computers to send trade secrets to the defendant via e-mail. Ruling upon a motion to dismiss, the court ruled the complaint stated a claim under 18 U.S.C. § 1030(a)(2)(C) which relates to the intentional accessing of a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer. The defendant argued that the employees all had full access to all information allegedly transferred to the defendant. However, the court found that once the employees began acting as agents for the defendant, when the employees used the plaintiff’s computers and information on those computers in an improper way, they were “without authorization.” The court also found that the pleading stated a claim under 18 U.S.C. § 1030(a)(4) for knowingly and with intent to defraud accessing a protected computer without authorization or exceeding authorized access, and by means of such conduct, furthering the intended fraud and obtaining anything of value. The court held that the claim need not state the common law elements of fraud, but need only allege that the defendant participated in dishonest methods

to obtain the plaintiff's secret information. Finally, the court found that the complaint stated a claim under 18 U.S.C. § 1030(a)(5)(C), which relates to persons who intentionally access a protected computer without authorization and as a result of such conduct, cause damage. The court rejected a defense claim that this section of the CFAA only applies to outsiders and not employees. The court also rejected a defense argument that the alleged loss of information by the plaintiff was not damage under the statute. The court noted that damage is "any impairment to the integrity . . . of data . . . or information." 18 U.S.C. § 1030(a)(8)(A), finding that "integrity" in the context of data necessarily contemplates maintaining the data in a protected state. By infiltrating the plaintiff's computer network and collecting and disseminating confidential information, the court found that there was an impairment of the data's integrity, and thus, damage within the meaning of the statute.

3. In *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000), defendant was prosecuted for intentionally causing damage to a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A). After quitting his job as a computer administrator, he accessed his e-mail account and switched to another user's account where he created and deleted accounts and added features to existing accounts. Later, his e-mail account was closed, he logged on to a test account and entered the main computer where he changed passwords, altered the computer's registry, deleted the entire billing system, including programs that ran the billing software and deleted two internal databases. His former employer used two company employees to repair the damage to the system. The Computer Fraud and Abuse Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information, that causes loss aggregating at least \$5,000.00 in value during any one-year period to one or more individuals." 18 U.S.C. § 1030(e)(8)(A). The court rejected Mr. Middleton's argument that Congress intended the phrase "one or more individuals" to exclude corporations. The court rejected his instruction on the definition of "damage", finding that the term includes any impairment to the computer system that caused the loss of at least \$5,000.00, including any monetary loss sustained as a result of any damage to the computer system, which should include any measures reasonably necessary to restore the data, program, system or information that was damaged or to re-secure the data program system or information from further damage. The court also rejected defendant's argument that by using salaried

employees to repair the system, that the victim had suffered no loss. The court reasoned that calculation of the loss could include the amount of time spent by the employees at their imputed hourly rates since the company would have had to hire outside contractors to repair the damage had it not used its own employees.

4. *E. F. Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (Several employees of plaintiff moved to defendant and hired an internet consultant to design a computer program called a scraper which functions like a robot to seek information from a website through the internet. The scraper utilized tour codes provided by the individual defendants, to access plaintiff's website repeatedly and easily obtained pricing information for those specific tours. The scraper sent more than 30,000 inquiries to plaintiff's website and recorded the pricing information into a spreadsheet. The scraper downloaded 60,000 lines of data, the equivalent of eight telephone directories of information. It compiled the data into a spreadsheet and provided it to the defendant corporation which then systematically undercut plaintiff's prices. The Court focused on a confidentiality agreement between one of the individual defendants and the plaintiff which prohibited the use of confidential information "for the employees' own benefit or for the benefit of any other person or business entity." When the defendants provided the tour and gateway codes to the internet consultant, the scraper was able to correlate the tour codes to actual tours and destination points whereas to the general public they would have been gibberish. The court concluded that because of the broad confidentiality agreement, the defendants' actions "exceeded authorized access" for purposes of 18 USC §1030(a)(4). With regard to whether plaintiff had suffered "damage" or "loss" within the meaning of 18 USC §1030(g), the District Court had held that "loss" would encompass a loss of business, good will and the cost of diagnostic measures that plaintiff took after it learned of defendants' access to its website. The defendants' challenged whether diagnostic measures could be included within the minimum damage requirement of \$5,000.00. The court concluded that expenses of at least \$5,000.00 resulting from a party's intrusion are "losses" for purposes of the "damage or loss" requirement of the CFAA.)
5. *E.F. Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). (Later, the Court of Appeals declined to vacate the injunction "as against Zefer," although it found an insufficient basis to support an independent preliminary injunction

against Zefer, because it had not signed a confidentiality agreement. The appellate court declined to affirm the district court's "reasonable expectations" test which was predicated upon the copyright notice on plaintiff's home page, the other defendants' provision to Zefer of confidential information obtained in breach of their confidentiality agreements, and the fact that the website was configured to allow ordinary visitors to the site to view only one page at a time.)

6. *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001) (The court found that a complaint stated a claim under 18 USC §1030(a)(5)(A) when AOL exceeded authorized access by transmitting damaging information through its 5.0 program. Consumers could aggregate their damages for purposes of the \$5,000.00 damage requirement in 18 USC §1030(e)(8). An ISP competitor had standing to sue for damages based on AOL's interference with its relationships with existing and prospective subscribers and the increased time spent by the competitor technical support personnel in dealing with AOL 5.0 problems. The court also found that the competitor had lost a "thing of value" for purposes of 18 USC §1030(a)(4) based upon the alienation of its existing or potential customers and for damages to its good will and reputation.)
7. *Thurmand v. Compaq Computer Corp.*, 171 F. Supp.2d 667 (E.D. Texas 2001) (A plaintiff class sought damages from Compaq under the Computer Fraud and Abuse Act for manufacturing and installing faulty floppy diskette controllers on their computers. In determining whether plaintiffs could establish "damage" within the meaning of 18 U.S.C. §§1030(a)(5)(A) and 1030(e)(8). The court held that plaintiffs would be required to establish \$5,000.00 of damage to each computer owned by a class member and that class members could not aggregate their damages.)
8. *Credentials Plus LLC v. Calderone*, 230 F. Supp. 2d 890 (N.D. Ind. 2002). (Plaintiff alleged that defendant, a former co-owner and officer of plaintiff, had intentionally accessed plaintiff's computer and obtained information on clients and potential clients residing out of state by re-routing client e-mail originally sent to plaintiff. Plaintiff's computer was used to send and receive e-mail to customers throughout the country and qualified as a protected computer under the CFAA. Because of disputed evidence as to who had set up the alternative e-mail address, the Court denied defendant's Motion for Summary Judgment.)

9. *U.S. Greenfiber v. Brooks*, 2002 WL 31834009 (W.D. La. Oct. 25, 2002). (Defendant was quality control manager of plaintiff, responsible for overseeing quality control for 10 plants of plaintiff. Up to her termination at plaintiff's corporate headquarters, she copied documents belonging to plaintiff and took them with her. She later threatened to provide confidential information to adverse parties in litigation and to competitors. On plaintiff's Application for Preliminary Injunction, the Court found it likely plaintiff could prove a violation of the Computer Fraud and Abuse Act because she had a company computer at home which was used to communicate with corporate headquarters and customers in interstate and foreign commerce. Although she was not authorized to access the company's communication system after her termination, she accessed the internal e-mail system and sent messages to employees and also removed all documents, e-mail files and computer files from the computer without authorization. The Court found it likely that plaintiff would establish a violation of the Louisiana Trade Secret Act because of defendant's possession of sensitive quality control and business records, including prior compliance records, e-mails, monthly reports, customer complaints, strategic plans, sales reports and customer pricing lists. In addition, she took further documents from the company computer system and was threatening to provide such information to adverse parties in civil litigation and to competitors.)
10. *Pearl Investments, LLC v. Standard I/O, Inc.*, 2003 WL 1741211 (D. Me. April 2, 2003). (Plaintiff's CFAA claim failed because plaintiff argued that defendant's alleged wrongful connection to its system adversely affected the system's speed and operation thereby causing damages. However, it did not set forth cognizable evidence that the conduct damaged its system in any quantifiable amount let alone an amount approximating more than \$5,000 in one year. Additionally, a claim under the DMCA was sustained based on an allegation that defendant had circumvented the protections of plaintiff's encrypted password-protected virtual private network to gain unauthorized access to data that included plaintiff's copyrighted software.)
11. *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002). (Internet users brought class action against web monitoring company and pharmaceutical companies, alleging that defendants secretly intercepted and accessed their personal information through the use of "cookies" and other

devices in violation of state and federal law. The Court rejected a wiretap claim because the pharmaceutical defendants had contracted with the monitoring company to obtain data regarding their websites and had the code placed on their websites, thereby bringing the web monitoring company into the statutory exception for consent. The Court rejected a Stored Communications Act claim because plaintiff's computers were not facilities which provided electronic communication services. The Court rejected the CFAA claim because plaintiffs did not allege that their computers were physically damaged in any way or that they suffered any damage resulting from the repair or replacement of their computer system.).

12. *United States v. Wiest*, 2002 WL 31235026 (A.F. Ct. Crim. App. Sept. 24, 2002). (Prosecution under 18 U.S.C. § 1030(a)(5)(B). The Court found that the unauthorized access need not be intentional because 1030(a)(5)(B) is a lesser included offense. With regard to defendant's alleged mistake of fact, the Court affirmed the trial court's instruction that the mistake of fact had to be reasonable instead of merely honest. The Court affirmed the verdict finding that any reasonable juror would have concluded that appellant did not have an authorized belief that access to a particular computer system was authorized. The sluggishness of the computer system, jerkiness of the display and presence of two unauthorized programs was sufficient to find damage and the repair and securing of the system was found to constitute damage in excess of \$5,000. The Court properly rejected a defense instruction that would have said that damages should not include expenses for making a computer system more secure than it was before the breach. In fact, damages might include "measures . . . reasonably necessary to re-secure the data, program, system or information from further damage.")

F. Practical Considerations.

1. The plaintiff must prove that the information at issue is a trade secret, and that the trade secrets are not "stale." *See also Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F. Supp. 2d 980, 984-992 (S.D. Cal. 1999) (The California rule set forth in CCP §2019(d) is a rule of substantive law which requires that a trade secret plaintiff identify its trade secrets with reasonable particularity as a condition of the plaintiff seeking discovery from the defendant.)

2. To the extent that the new employer already utilizes technology that the plaintiff claims is a trade secret, the claim will probably fail.
3. The plaintiff will be forced to substantiate its claims regarding the trade secrets by engaging in discovery on what the Plaintiff has done to develop the information and to protect its confidentiality. *Motorola, Inc. v. Fairchild Camera and Instrument Corp.*, 366 F. Supp. 1173 (D. Ariz. 1973) (holding that Motorola had not adequately protected the confidential nature of the information at issue to qualify the information as a trade secret).
4. Once products are sold and are in the public domain, they may be reverse engineered which is a defense to trade secret misappropriation. *See, Kadant, Inc. v. Seely Machine, Inc.*, ___ F. Supp. 2d ___, 2003 WL 354635 (N.D.N.Y. Jan. 30, 2003). (The manufacturer of products that clean and condition paper-making machines and filter water used in the paper making machines was denied a preliminary injunction against a competitor that had employed a former machinist and member of the engineering department who had had access to customer lists and customer buying information, as well as used the computer-assisted drawing machine that contained recipes for plaintiff's products on the customer information. It was unable to persuade the Court that the customer information was not freely available in the public domain from trade associations and telephone books and unable to persuade the Court that the customer buying information was unavailable to anyone who inquired. From the design specifications, plaintiff claimed that reverse engineering would have required two years of work and that its former employee must have utilized its design specifications in helping the competitor develop its products. However, because its products had been sold and were in the public domain, and thus subject to being reverse engineered by any purchaser, and because there was no evidence that the former employee had stolen the design specifications, its trade secret claim was insufficient to support a preliminary injunction, as were its alleged breach of contract and breach of fiduciary duty claims based on the alleged breach of the confidentiality agreement the employee had signed.)

G. Remedies.

1. Available remedies include injunctive relief, lost profits, disgorgement or unjust enrichment remedy, or a reasonable royalty. *Litton Sys., Inc. v. Ssangyong Cement Indus. Co.*, 1993 WL 317266 (N.D. Cal. 1993) (Unjust enrichment principles may apply when defendants' expected profits are too difficult to ascertain.); *Cacique, Inc. v. Robert Reiser & Co.*, 169 F.3rd 619, 49 U.S.P.Q.2d 1997 (9th Cir. 1999) (The California Uniform Trade Secret Act permits plaintiff to receive a reasonable royalty only if it cannot prove damages or unjust enrichment so third-party discovery was improperly granted because it related only to a reasonable royalty claim which was not available in that case.)
2. *Sonoco Prods. Co. v. Johnson*, 23 P.3d 1287 (Colo. Ct. App. 2001). (Where a defendant was found guilty of wrongful acquisition, but not use of the plaintiff's manufacturing trade secret, the court affirmed an award of \$6.9 million in direct and punitive damages based on upon an expert's estimate of the plaintiff's cost of development of its trade secrets.)
3. *Children's Broadcasting Corp. v. Walt Disney Co.*, 245 F.3d 1008, 1016 (8th Cir. 2001). (A plaintiff was permitted recovery of lost profits for the defendant's breach of a contract and to the extent not already taken into account by the lost profits, the defendant's unjust enrichment.)
4. *Olson v. Nieman's Ltd.*, 579 N.W.2d 299 (Iowa 1998). (The trier of fact has discretion to proceed on a reasonable royalty basis where the plaintiff was unable to establish other damages with certainty.)
5. *Yeti by Molly, Ltd. v. Deckers Outdoor Corp.*, 259 F.3d 1101, 1107-1108 (9th Cir. 2001). (The court found that plaintiff had adequately proven \$1.8 million in lost profits and lost business opportunities, so there was no need for recourse to a reasonable royalty basis, but the court reversed the trial court's refusal to consider punitive damages under the UTSA standard as opposed to the general Montana punitive damages statute.)
6. *Vermont Microsystems, Inc. v. Autodesk, Inc.*, 138 F.3d 449, 450 (2nd Cir. 1998). (The Court found that the trial judge properly applied a reasonable royalty

standard where the unjust enrichment to be disgorged by the defendant was too speculative.)

7. *Avery Dennison Corp. v. Four Pillars Enterprise Co.*, 2002 WL 2020041 (6th Cir. Sept. 3, 2002). (In this action, plaintiff Avery uncovered a conspiracy whereby one of its employees was passing confidential adhesive formula manufacturing techniques, product specifications and other fruits of its research to a competitor. After the competitor and its president were convicted under the Economic Espionage Act, Avery brought RICO and state law claims. The evidence at trial showed that the defendant had misappropriated 71 formulas and manufacturing instructions, but did not copy the products exactly, but modified them. Avery's damage expert presented three different theories of recovery: defendant's profits, defendant's avoided costs and reasonable royalties. The verdict included \$10 million on the RICO claims, trebled to \$30 million, \$10 million on the misappropriation claim, \$10 million on the civil conspiracy and conversion claims and \$25 million in punitive damages, for a total of \$81 million in damages. The Court approved the damage theories and found that it was not necessary to prove a commercial use to have a reasonable royalty theory in light of defendant's modification of the formulas and use of the manufacturing specifications to cut their own research time and streamline their own manufacturing processes. It also found that the RICO and state law claims were not presented as alternative theories, so it was acceptable to accumulate them.)
8. *The Eagle Group, Inc. v. Pullen*, 114 Wash. App. 409, 58 P.3d 292 (2003). (Plaintiff construction company had opened a branch office in Portland, Oregon; its manager left and joined a competitor, another general contractor, taking employees, clients, files, construction projects and an office lease with him. One of plaintiff's partners testified to plaintiff's Portland office expenses for the two years of its existence, plus its revenues, and estimated that it generated an average of \$141,000 per year, and estimated that its value was three times that amount. The jury awarded damages of \$332,500. The Court found that the "actual loss" under the UTSA could include the reasonable value of business opportunities, with reasonable probability of profits in the future, and sustained the verdict.)

II. DEVELOPING TRADE SECRET PROTECTION POLICIES AND APPROPRIATE NON-DISCLOSURE AGREEMENTS

A. Rationale for Efforts to Preserve Secrecy

1. Information that is valuable and not generally known in the industry can lose its trade secret status if the company does not treat the information as confidential. Put differently, in the trade secret area, the law helps those who help themselves.
2. The Uniform Trade Secrets Act requires the use of “efforts that are reasonable under the circumstances” to maintain the secrecy of the information. See, e.g. A.R.S. §44-401(4). The comment to that provision states:

“. . . [R]easonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on a ‘need to know basis,’ and controlling plant access. On the other hand, public disclosure of information through display, trade journal publications, advertising, or other carelessness can preclude protection.***

The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage. . . . It follows that reasonable use of a trade secret including controlled disclosure to employees and licensees is consistent with the requirement of relative secrecy.” Uniform Trade Secrets Act §1 Comment (1995).

3. See, *Alamar Biosciences, Inc. v. Difco Labs, Inc.*, 1995 WL 912345 (E.D. Cal. 1995) (A failure to take prompt action to prevent trade secret misappropriation may go to the merits of whether plaintiff has met the definition of a trade secret by reason of both the information not being generally known and plaintiff’s having exercised reasonable safeguards to maintain secrecy.)
4. *Gemisys Corp. v. Phoenix Am., Inc.*, 50 U.S.P.Q.2d 1876, 1880-1885, 1999 WL 417411 (N.D. Cal. 1999) (Plaintiff licensed a computer program to defendant; the license agreement required confidentiality for matter delivered with appropriate confidentiality legends but the plaintiff failed to legend any of the

materials that it sought to protect as trade secrets and this was held to constitute inadequate safeguards for trade secret purposes even though the plaintiff exercised reasonable safeguards within its company vis a vis employees.)

5. *Zemco Mfg., Inc. v. Navistar Int'l Transportation Corp.*, 759 N.E.2d 239, 246, 249-252 (Ind. App. 2001). (Court held that plaintiff had granted access to its allegedly secret equipment to both competitors and major customers without requiring confidentiality agreements. This was found to fail to meet minimum safeguard standards.)
6. *Avery Dennison Corp. v. Kitsonas*, 118 F. Supp. 2d 848, 854 (S.D. Ohio 2000). (Password limited access to customer information constituted a reasonable safeguard.)
7. *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002). (Defendant challenged several aspects of whether the information he stole from his employer and attempted to sell constituted trade secrets. The Court concluded that the following constituted "reasonable measures to keep the information secret:" All of its drawing and manufacturing data was stored in a CAD room, protected by a special lock, alarm system and a motion detector; the number of copies of sensitive information is kept to a minimum and surplus copies are shredded; some information in the plans is coded, with few people knowing the keys to the code; drawings and other manufacturing information contain warnings of the owners' intellectual property rights; every employee receives a notice that the information with which he works is confidential; none of the company's subcontractors receive full copies of the schematics; thus by relying on the splitting of tasks, and dividing the work among vendors, the company ensures that none can replicate the product.)
8. *Moss v. O.E. Clark Paper Box Co.*, 2002 WL 849940 (Cal. App. 2 Dist. May 3, 2002). (Plaintiff convinced defendant to hire her because of her contacts with the customers of a defunct competitor and agreed to share the names of these customers with the defendant to bolster its sales in specialty packaging. Because the information was freely supplied, the Court declined to find that it had been misappropriated; the Court went on to find that the customer list was not a trade secret because it was readily ascertainable and its compilation was neither

sophisticated, nor difficult, nor time consuming, and because it was not plaintiff that had compiled the list, but her former employer.)

9. *Petters v. Williamson & Associates, Inc.*, 2003 WL 457823 (Wash. App. Div. 1 Feb. 24, 2003). (The Court found there were reasonable efforts to maintain secrecy of certain drill technology even though it was sold without a requirement to protect it against disclosure and did not include a proprietary notice. The Court found that the pre-contract proposal stated that some pages in the document were proprietary, limited who could view the document, and a plaintiff signature block on the top level assembly drawing stated that the drawing was the property of plaintiff and was not to be reproduced or disclosed without written consent of plaintiff.)
10. *Q-Tech Laboratories PTY Limited v. Walker*, 2002 WL 1331897 (D. Colo. June 4, 2002). (Plaintiff unable to establish that defendant misappropriated trade secrets because the product in question could be purchased and easily reverse engineered by copying the dimensions of certain copper and stainless steel plates as well as the distances in between the plates and because the lengthy passage of time, over four years, that the product had been on the market and susceptible to reverse engineering before the claim was brought showed lack of irreparable present harm.)
11. *Sunbelt Rentals, Inc. v. Head & Engquist Equipment, LLC*, 2002 WL 31002955 (N.C. Super. July 10, 2002). (The reasonable measures to ensure secrecy included an employee handbook which mandated that certain business information be kept confidential, and the fact that access to the customer information stored in computer databases was restricted to authorized personnel with access codes.)
12. *Tyson Foods, Inc. v. Conagra, Inc.*, 349 Ark. 469, 79 S.W.3d 326 Ark. (2002). (The Court found that Tyson had not engaged in reasonable measures to ensure secrecy when its only effort was to adopt a corporate code of conduct and compliance policy and a directive to its employees that the code be read, when the code was primarily an ethical guide which failed to identify what is a trade secret or to mention the particular trade secret in question, and the corporate code did not qualify as an agreement between Tyson and its employees not to disclose

any trade secret in particular. The Court found that hundreds of Tyson's managers were educated about the particular trade secret in question, its nutrient profile, and there was no proof that Tyson took any steps to swear them to secrecy or warn them of the confidential nature of the profile.)

13. *Motorola, Inc. v. DBTel, Inc.*, 2002 WL 1610982 (N.D. Ill. July 22, 2002). (The Court found insufficient information to find that Motorola's alleged transfer of confidential information constituted trade secrets, found that Motorola had waited one year before enforcing its rights, which militated against a preliminary injunction, and found that the information was reasonably ascertainable.)

B. Traditional Prudent Efforts to Preserve Secrecy:

1. Marking documents "Confidential: For Internal Use Only," and limiting distribution of such materials to employees with a "need-to-know." Do not create confusions or weaken your assertion of secrecy by marking as "confidential" material to which no secrecy need attach.
2. Creating a company-wide confidentiality policy distributed at least annually to all employees, and on the date of hire for new employees. Acknowledgment form signed by employee at date of hire and then annually.
3. Requiring employees to execute trade secret/confidentiality agreements.
4. Enforcing disciplinary action against violators.
5. Enforcing a clean desk policy
6. Maintaining records of persons to whom trade secret information was made available, when released and when returned and what confidential information was contained therein.
7. Maintaining a check-out system whereby users of the confidential information sign a release form acknowledging that they have received confidential proprietary or trade secret data and that they have duties to safeguard and not disclose it.

8. Marking the trade secret data with appropriate restrictive legends identifying the information as having confidential or trade secret status.
9. Creating security in the business premises by establishing sign-in procedures, requiring badges, restricting access for visitors and employees, placing locks on cabinets or rooms containing sensitive information, and/or requiring a password to computers.
10. Keeping “one-of-a-kind” documents and items under lock and key.
11. Inventorying items prior to employee departures.
12. Documenting your efforts to develop and protect the trade secrets.
13. Scheduling exit interviews, so that employees leaving the company can be reminded of their continuing obligations to maintain secrecy, and to collect all confidential documents and other information. Follow-up with a letter to the employee reminding him of his obligations.

C. Efforts to Preserve Secrecy In The Digital Environment:

1. E-mail. Corporate employees may intentionally or unintentionally destroy the confidentiality of trade secret information by transmitting it to others.
 - a. Adopt confidentiality plans that are made known to the employees who must be sensitized to the significance of providing confidential information to others outside the company.
 - b. If the confidential information must be shared with vendors, those parties should be required to enter into confidentiality agreements as well.
 - c. Distribute an e-mail policy informing employees that any e-mail that passes through a company computer is considered company property and may be monitored. Have employees sign an acknowledgment.

- d. The Company should have a policy prohibiting the forwarding of any company document to an outside e-mail account without prior supervisory approval.
2. Web Pages. Companies can intentionally or unintentionally place confidential information on their web pages, including customer lists or other information about their customers or distributors of their products, employees who are members of key product teams, product specifications, business plans or even portions of computer source code to those who have the right expertise.
 - a. Trade secret owners should take great care in examining the kinds of information that are placed on the web page and should consider mechanisms to protect the most confidential information that is deemed necessary to be on the web site, through some form of digital lock or password protection plan, or at a minimum, some form of click through confidentiality agreement.
 3. Chat Rooms and Discussion Groups. This has many of the same problems of e-mail, but usually there would be no valid reason for a corporate employee to post confidential information on a chat room or discussion group, other than for some improper purpose.
 - a. The same precautions mentioned above should apply to posting of information or chat rooms or in discussion groups, and the company must have some form of plan for minimizing the damage of such an event.
 4. Computer or digital information
 - a. Should be protected through electronic labeling, electronic locks, passwords, warning screens, encryption or coding or shrink wrap licenses or agreements on software provided to employees or vendors requiring that users agree to nondisclosure terms.

D. Click Wrap, Shrink Wrap and Browse Wrap Agreements and Licenses.

1. A click-through agreement appears on a web page (or a computer screen) and requires that the user click “I accept” before moving on to the next page. In *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1020 (N.D.Cal. 1998), the court assumed, without analyzing, the enforceability of a click-through agreement. *See also, eBay, Inc. v. Bidders’ Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D.Cal. 2000), regarding defendant’s non-compliance with guidelines established by eBay pursuant to a Robot Exclusion Standard. *See also Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000); *See also I.LAN Systems, Inc. v. Netscout Service Level Corp.*, 183 F. Supp.2d 328 (D. Mass. 2002) (The court enforced a click wrap license agreement to which plaintiff necessarily agreed when it installed the software at issue. The click wrap license agreement in question contained both a limitation of warranties and a limitation of remedies available to the buyer.)
2. A “browse wrap” license appears on a web page but will probably not be enforced unless it is set up to require users to click “I accept” before copying or downloading information. *Pollstar v. Gigmania Ltd.*, 170 F. Supp.2d 974 (E.D. Cal. 2000) (Plaintiff maintained a website that contained concert information which users could download and use pursuant to the conditions of a license agreement. Defendant downloaded information from the website and placed it on its own website in violation of the terms of the license agreement. Plaintiff alleged that its license was a “Browse Wrap” license which is part of the website and the user assents to the contract when the user visits the website. Notice of the license agreement is provided by small gray text on a gray background. The court declined to dismiss the complaint “at this time.” The license agreement is not set forth on the home page but is on a different web page that is linked to the home page. A visitor is alerted to the fact that “use is subject to license agreement” because of the notice in small gray print on gray background but the notice is not linked to the license agreement.); *Specht v. Netscape Communications Corp.*, 150 F. Supp.2d 585 (S.D.N.Y. 2001) *aff’d*, 306 F.3d 17 (2nd Cir. 2002) (This case involved defendants who had downloaded SmartDownload software from Netscape and brought claims against Netscape alleging that the software unlawfully transferred information about the user’s file transfer activity on the Internet to Netscape. Netscape attempted to compel

arbitration pursuant to the terms of an End User License Agreement allegedly contained on the website from which the software was downloaded. The court found that visitors wishing to obtain the software arrive at a page containing a button labeled “Download” but the only reference to the license agreement appears in text that is visible only if the visitor scrolls down to the page of the next screen. At that point they do not even see the license agreement, they only see an invitation to review the license agreement. Visitors were not required affirmatively to indicate their assent to the license agreement or even to view the license agreement before proceeding with a download of the software. If a visitor chose to click on the underlying text in the invitation, the hypertext link would take the visitor to a web page entitled “License and Support Agreements” which contained the referenced End User License Agreement. The court found that this was an attempt to create a “Browse Wrap” license but it was ineffective because there is no requirement that the user assent to the terms of the license before acquiring the software. Because there was no assent, there is no agreement and the court declined to enforce the agreement.) (The District Court’s opinion was affirmed on appeal. The Court ruled that there was not reasonably conspicuous notice of the existence of contract terms because they were placed on the next page of the website, which required a user to scroll down to see them, and there was not unambiguous manifestation of assent to those terms by consumers. The Court held that a reasonably prudent offeree in plaintiffs’ position would not have known or learned, prior to acting on an invitation to download, of the reference to license terms hidden below the “Download” button on the next screen, and were not on inquiry notice of the existence of such terms.)

3. Trespass may also be available as a legal remedy. *Oyster Software, Inc. v. Forms Processing, Inc.* 2001 WL 1736382 (N.D. Cal. December 6, 2001) (After plaintiff learned that defendant was using metatags copied from plaintiff’s website to defendant’s website it brought an action alleging various theories. On the trespass claim, the Court held that the plaintiff must show an intentional interference with the possession of personal property which has proximately caused injury, but that the plaintiff need not prove that the defendant’s robots interfered with the basic function of plaintiff’s computer system in a way that was more than negligible. The court held that plaintiff need only prove that defendant’s conduct amounted to “use” of plaintiff’s computer.)

4. For examples of cases which have enforced shrink-wrap licenses, *see ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), where the court enforced both a shrink-wrap and a bootscreen software license which restricted use of the software for non-commercial purposes; *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148 (7th Cir. 1997), where the court enforced an arbitration agreement in a standard form agreement packed inside the box of a new computer; *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996), where the court enforced CompuServe's standard Shareware Registration Agreement after a defendant had agreed to it prior to placing his software on CompuServe's system; *M.A. Mortenson Co. v. Timberline Software Corp.*, 970 P.2d 803 (Wash. Ct. App. 1999), which the court found to be a valid "accept or return" license which contained limitations on consequential damages; *Brower v. Gateway 2000, Inc.*, 246 A.D. 2d 246, (N.Y. App. Div., 1998), where the court enforced a Gateway 2000 arbitration agreement; *I-A Equipment Co. v. ICode, Inc.*, 43 UCC Rep. Serv. 2d 807, 2000 WL 33281687 (Mass. Dist. 2000) *aff'd*, 2003 WL 549913 (Mass. App. Div. Feb. 21, 2003) (Court enforced an End User License and Service Agreement which was in the form of a shrink wrap license printed on the outside of the sealed envelope bearing the software, and also in the form of a click-wrap license: when the customer installed the software as part of the installation process, the End User License Agreement appeared on the screen and the customer had to accept the agreement before being able to complete the installation and registration of the software. The agreement contained a forum selection clause requiring that all litigation be brought in the Commonwealth of Virginia.); *Adobe Systems, Inc. v. Stargate Software, Inc.*, 216 F. Supp. 2d 1051 (N.D. Cal. 2002). (Court enforced On-campus Educational Reseller Agreement ("OCRA") and shrink wrap End User License Agreement ("EULA") and determined that Adobe had licensed its software, not sold it, subject to the significant restrictions in the OCRA and EULA.); *Bowers v. Baystate Technologies, Inc.*, 320 F.3d 1317 (Fed.Cir. 2003). (The Court enforced the shrink wrap license agreement that prohibited reverse engineering, finding the contract not preempted by the Copyright Act, and finding extensive evidence of reverse engineering in the action.); *Lozano v. AT&T Wireless*, 216 F. Supp. 2d 1071 (C.D. Cal. 2002). (The Court found that an arbitration agreement contained in the "Welcome Guide" provided with the cellular telephone was a binding agreement even though the terms and conditions were provided after the initial transaction. The Court thus compelled arbitration and found enforceable the

punitive damage limitation and the prohibition of class or representative claims.); *O'Quin v. Verizon Wireless*, ___ F. Supp. 2d ___, 2003 WL 1889293 (M.D. La. 2003) (the Court enforced an arbitration clause in a terms and conditions pamphlet that was included in the telephone handset boxes for two PCS telephones purchased by the plaintiff at the same time that it obtained wireless service from the defendant. The Court followed the Pro-CD line of cases.).

5. For examples of cases which have not enforced shrink-wrap licenses, see *Step-Saver Data Systems, Inc. v. Wyse Technology, Inc.*, 939 F.2d 91 (3d Cir. 1991), where the court refused to enforce disclaimer of warranty and limitation of liability provisions contained in a shrink-wrap agreement of a vendor where a value-added e-seller was seeking contribution for problems suffered by the ultimate customers; *Arizona Retail Systems, Inc. v. The Software Link, Inc.*, 831 F. Supp. 759 (D. Ariz. 1993), where the court was willing to enforce a shrink-wrap agreement in an initial test shipment, but declined to enforce shrink-wrap agreements on subsequent transactions, finding that the terms and conditions of the sale had been established in telephone orders and that the subsequent shrink-wrap license could not amend the original agreement; and *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988), where the Fifth Circuit upheld a district court finding that a shrink-wrap license which prohibited reverse engineering was a contract of adhesion and therefore unenforceable; *Klocek v. Gateway, Inc.*, 104 F. Supp.2d 1332 (D. Kansas 2000) (The court ruled that Gateway's standard terms and conditions agreement which were included in the computer box were unenforceable because they constituted either an expression of acceptance or written confirmation, and Gateway could provide no evidence that at the time of the sales transaction it informed the customer that the transaction was conditioned on the customer's acceptance of the standard terms. By shipping the goods with the terms in the box, Gateway did not communicate to the customer any unwillingness to proceed without the customer's agreement to the standard terms. The court therefore concluded that the arbitration agreement set forth in the standard terms was unenforceable.); *Licitra v. Gateway, Inc.*, 189 Misc.2d 721, 734 N.Y.S.2d 389 (2001) (The court declined to enforce the terms on a form included in a computer box because there was no evidence that the consumer had agreed to the terms.); *Softman Products Company LLC v. Adobe Systems Inc.*, 171 F. Supp.2d 1075 (C.D. Cal. 2001) (A distributor was purchasing bundled collections of software from the defendant,

unbundling them and selling them separately, allegedly in violation of an End User License Agreement. The court held that the transaction constituted a sale rather than a license, so defendant's activities could not constitute copyright infringement. The court found that the End User License Agreement was in the form of a click wrap license which appeared on the screen when the consumer loads the defendant's programs and begins the installation process. Because the defendant never loaded the software, there is no evidence that it had ever read or assented to the End User License Agreement. Thus, the court declined to enforce the End User License Agreement.); *Mattingly v. Hughes Electronics Corporation*, 147 Md. App. 624, 810 A.2d 498 (Md. App. 2002). (Plaintiff entered into an oral agreement with defendant to provide cable TV service. Thereafter, defendant sent him an invoice, along with a "Customer Agreement" which included a clause which said that defendant reserves the right to change the terms and conditions and would do so by sending a written notice describing the change and its effective date. One month later, it mailed a new Customer Agreement which contained an arbitration clause. After plaintiff initiated a class action suit, defendant attempted to invoke the arbitration clause by moving to compel arbitration. The Court ruled that defendant had not provided proper notice of the change in the agreement, i.e., the addition of the arbitration clause, and could not enforce it.)

E. Technology Measures That Control Access: The Digital Millennium Copyright Act.

1. To the extent the trade secret material is included with copyrighted material that is protected by a "digital lock" or "technology access device" such as a password protection system, it will be protected by the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1204. A "digital lock" is shorthand for a technological measure that requires the application of information or a process or a treatment with the authority of the copyright owner to gain access to the work. One violates the DMCA by circumventing the technological measure either by descrambling a scrambled work, decrypting an encrypted work or otherwise avoiding, bypassing, removing, deactivating or impairing the technological measure without the authority of the copyright owner. 17 U.S.C. § 1201(a)(3). To enforce the DMCA, a district court may grant a temporary or permanent injunction, impound the violative device or product, and award damages, costs

and attorney's fees. Damages may include actual damages and additional profits of the violator or statutory damages. 17 U.S.C. § 1203(c).

2. *Universal City Studios Inc. v. Corley*, 273 F.3rd 429 (The Second Circuit affirmed the District Court's ruling that a defendant who posted a decryption computer program named "DeCSS" on his website which was designed to circumvent the encryption technology that motion picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures constituted a violation of the Digital Millennium Copyright Act, 17 U.S.C. §1201 et. seq.)
3. *United States v. Elcom Limited*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002). (The District Court declined to find the DMCA unconstitutional, as vague, overbroad or violative of the intellectual property clause. Although defendant's software contained expression, thus implicating First Amendment issues to the extent that the DMCA targets computer code, Congress sought to restrict the code not because of what it says, but rather because of what it does. Therefore DMCA's restriction on speech is content neutral and subject to intermediate scrutiny. The Court found that the DMCA is not an unconstitutional restriction of speech under the intermediate scrutiny test. The Court found that the government had legitimate interest in preventing the unauthorized copying of copyrighted works in promoting electronic commerce. The Court found DMCA is sufficiently tailored to governmental interests, and that the means chosen do not burden substantially more speech than is necessary to further the government's interest.);
4. *Lexmark International, Inc. v. Static Control Components, Inc.*, 2003 WL 912614 (E.D.Ky. Feb. 27, 2003). (The Court held that for preliminary injunction purposes, plaintiff had established a likelihood of success on the DMCA claims: defendant admitted that its microchips avoided or bypassed plaintiff's authentication sequence and thereafter the printer accesses without authority the printer engine program. The authentication sequence that occurs between plaintiff's printers and the microchips contained on authorized plaintiff toner cartridges constitutes a "technology measure" that "controls access" to copyrighted material. Defendant's microchips thus violate the DMCA in three ways: they were developed to circumvent the authentication sequence that controls access to plaintiff's copyrighted printer engine program; the microchips have no commercial purposes other than to circumvent the authentication

sequence that controls access to the copyrighted printer engine program; and the defendant marketed the microchips as being capable of circumventing the access control protections provided by the original microchips on plaintiff's original products.)

F. Non-Disclosure/Confidentiality Agreements

1. Most trade secret protection programs include some form of confidentiality protection. An employer will want to have its employees sign confidentiality agreements to protect the employer's trade secrets or other information, and prevent disclosure of such information both during and following the termination of employment. Properly drawn confidentiality provisions are generally enforceable in accordance with their terms. *See Lessner Dental Laboratories, Inc. v. Kidney*, 16 Ariz. App. 159, 161, 492 P.2d 39, 41 (1971); *IDX Systems Corp. v. Epic Systems Corp.*, 285 F.3rd 581 (7th Cir. 2002) (In an action based upon a breach of a confidentiality agreement, the Court of Appeals ruled that the agreement was not preempted by the Uniform Trade Secrets Act and rejected the District Court's conclusion that the contractual agreement was unenforceable because it was unlimited in temporal and geographic scope and thus an undue restraint of trade.)
2. The agreement should include statements that the employer has trade secrets and other certain confidential information to which the employee will have access during the course of his employment (often with a series of examples), that the information is "proprietary" to the employer, and a promise by the employee to keep the information confidential, a promise that the employee will not use or disclose the information outside the workplace or to those without a "need to know" without the employer's consent, and a promise to return all such confidential information upon termination of employment. These agreements should be signed at the commencement of employment, or at the time the employee's position gives him access to proprietary information.
3. Several courts have held that requiring employees to sign confidentiality agreements respecting the trade secrets was sufficient to constitute reasonable steps to ensure secrecy of the information for trade secret protection. This was a holding in *MAI Systems Corp.*, 991 F.2d 511 (9th Cir. 1993), cert. dismissed 510

U.S. 1033 (1994), and *American Credit Indemnity Co. v. Sacks*, 213 Cal. App. 3rd 622, 262 Cal. Rptr. 92 (1989). In *Religious Technology Center v. Netcom On-Line Communication Servs., Inc.*, 923 F. Supp. 1231 (N.D.Cal. 1995) stated that reasonable efforts could include advising employees of the existence of a trade secret and, limiting access to the information on a need-to-know basis and requiring employees to sign confidentiality agreements. In that particular case, the plaintiff had gone far beyond those requirements, including using locked cabinets and safes, logging and identifying materials, making materials available only to a handful of persons worldwide, attaching electronic sensors to documents, using locked briefcases to transport the documents, using alarms, photo identification and security personnel and requiring confidentiality agreements. In *Morlife Inc. v. Perry*, 56 Cal. App. 4th 1514, 1521 66 Cal. Rptr. 2nd 731 (1997) the court approved trade secret protection upon a showing that a plaintiff had limited circulation of its customers lists and advised its employees through an employment agreement and employee handbook that the information was confidential.

4. Other places to reinforce the importance of protecting confidential information would include codes of conduct, employee handbooks or intellectual property policies.
5. In addition to employees, companies should ask contractors, vendors, potential business partners or potential merger or acquisition partners to sign confidentiality and non-disclosure agreements if they will become exposed to trade secrets. Such agreements are enforceable through injunctive relief and damages, *see, e.g., Celeritas Techs. Ltd. v. Rockwell Int'l Corp.*, 150 F.3d 1354, 1357-60, (Fed. Cir. 1998), *cert. denied*, 525 U.S. 1106 (1999); *Boeing Co. v. Sierracin Corp.*, 108 Wash. 2d 38, 46-54, 738 P.2d 665, 673-76 (1987).
6. *Energex Enterprises, Inc. v. Anthony Doors, Inc.*, 2003 WL 1217490 (D. Colo. Mar. 6, 2003). (Plaintiff revealed confidential information and trade secrets to defendant pursuant to a confidential disclosure agreement in the course of developing a business arrangement. Defendant eventually declined to go forward and developed a competing product, which eventually contained much of the confidential information revealed to it. In analyzing the breach of contract claim, the Court found that the confidentiality agreement contained both a non-

disclosure clause and a non-competition clause. It found that the agreement did not violate C.R.S. § 8-2-113 on its face and also because of the exception for contracts for the protection of trade secrets. Nevertheless, the Court determined that it had to determine whether the agreement could be construed as reasonable in duration or geographic scope, which were found to be fact questions that could not be determined on a motion to dismiss. It also declined to dismiss a tortious interference with prospective business advantage claim, rejecting the defendant's assertion of a "competitor's privilege" because the allegations of independently actionable conduct such as misappropriation of trade secrets or breach of confidentiality agreement constitutes "wrongful conduct," defeating the competitor's privilege.)

7. *BBA Nonwovens Simpsonville, Inc. v. Superior Nonwovens, LLC*, 303 F.3d 1332 (Fed. Cir. 2002). (The Court found evidence of misappropriation since it was acquired in whole or in part by a consultant who knew or believed he was bound by a non-disclosure agreement and by the former president of the division who had reason to know the information was secret and had been acquired by improper means.)
8. A sample confidentiality and nondisclosure agreement is set forth as Form E in the appendix. In such agreements, it is important to define "Confidential Information"; to determine whether Confidential Information must be reduced to writing; whether it must be marked "Confidential" or "Proprietary"; whether it only relates to a particular subject, product, or process; and whether the agreement will cover oral disclosures or disclosures where the recipient has reason to know the information is Confidential. It is important to describe those categories of persons to whom the Confidential Information can be shown: examples include all employees; employees with a need to know; employees who have signed confidentiality agreements; identified third parties; third parties with a need to know; third parties subject to Confidentiality Agreements; legal counsel; other professionals; consultants; other agents. It may be important to describe the purposes for which the Confidential Information may be used and to disclaim various types of intellectual property licenses. The agreement should provide for the return of the Confidential Information.

9. Various types of exceptions or carve-outs are commonly included: information rightfully in the possession of or already known to the recipient; legally and publicly available information; information rightfully obtained by the recipient from a third-party source; information available from lawful inspection or analysis of products offered for sale; information inherently disclosed in the marketing or sale of products; or information independently developed by the recipient.
10. Residuals clauses are sometimes used by larger companies or third-party vendors providing for the right to use residual information in their employees' minds either before or after the receipt of confidential information, or as modified by the receipt of confidential information. Smaller companies should require the return or destruction of the documentary information, physical product or other tangible embodiment of the confidential information, and may wish to limit the residual clause to the employees of the other party who were intended to have access to the confidential information. Examples of residuals clauses are set forth as Form F in the appendix.

G. Checklist For Exit Interview

1. Verify that employee has returned all confidential materials, or collect them at the interview.
2. Tell employee about the information that they have been exposed to that the company considers a trade secret.
3. Remind employee of his or her legal duty not to use or disclose this or any other trade secret information.
4. Document the interview, and follow up with a letter to the employee reminding him or her of their obligations.
5. Tell departing employee that company considers information regarding the roles and skills of other employees within the company to be confidential information. Document the interview.

H. Post-Departure Investigation: Damage Assessment

1. Interviews of remaining employees and vendors
2. Computer search, including searching for information downloaded or copied from system. This should include laptops, network servers, minicomputers, mainframes, all the various types of removable data storage, Internet browser cache, cookies, bookmarks, firewall logs, and all the places where e-mail might be stored, and all contact manager files.
3. Phone records and PBX reports and voicemail
4. Pager records
5. Travel records
6. Building access control system and CCTV security system
7. Employee's own website, but in one case, an employee claimed that his employer's unauthorized access to his secure, password-protected website violated the Electronic Communications Privacy Act. 18 U.S.C. §§ 2510-2520 and 18 U.S.C. §§ 2701-2710. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002). (The Court first held that for a website such as Konop's to be "intercepted" in violation of EPCA, it must be acquired during transmission, not while it is in electronic storage; since defendant's conduct did not constitute an "interception" of an electronic communication, the Ninth Circuit affirmed the District Court's grant of summary judgment on the wire tap claims. The other portion of the Opinion dealt with the issue of whether two pilots who had authorization to access Konop's website could grant permission to a Hawaiian Airlines vice president to view the website. If so, Hawaiian would be exempt from liability under the Stored Communications Act. The Ninth Circuit ruled although the two pilots were "authorized users," they had never been "actual users" and did not fall within the statutory category of persons who could authorize a third party's access to their electronic communications. Thus, the District Court's summary judgment to Hawaiian on Konop's Stored Communications Act claim was reversed.)

I. Computer Forensics Tips When You Know You Have a Problem

1. Resist the urge to turn on the ex-employee's computer and see what you find. Instead, leave it alone and call someone who understands computer forensics. That person will almost never be someone who works in the IT department of the company.
2. Make sure that all backup media, particularly backup tapes, are immediately pulled out of rotation in order to avoid overwriting.
3. Intervene in normal HR procedures whereby an ex-employee's space on the server is immediately re-allocated. Make sure that the employee's account remains untouched (but be sure to cut off remote login access).
4. Document each and every step to avoid chain of custody questions that may be raised by your opposition's expert.

J. Countermeasures Short of Litigation

1. Letter from your attorneys to attorneys of competitor, or from one high level executive to another, voicing concerns regarding trade secrets
2. Resolution through business channels

III. THE ENFORCEABILITY OF NON-COMPETITION AGREEMENTS

A. California

1. The California Business and Professions Code § 16600 prohibits the use of covenants not to compete. It states:

“[E]very contract by which anyone is restrained from engaging in a lawful profession, trade or business of any kind is to that extent void.”
2. Using the statute, California courts routinely invalidate covenants restricting an employee's right to work for a competitor after the employee departs. *See, e.g., Metro Traffic Control, Inc. v. Shadow Traffic Network*, 22 Cal. App. 4th 853, 859

27 Cal. Rptr. 2d 573, 577 (1994); *Kolani v. Gluska*, 64 Cal. App. 4th 402, 407, 75 Cal. Rptr. 2d 257, 260 (1998). California courts also routinely invalidate any clause which provides for a loss of benefits or imposes penalties for working for a competitor after completion of employment. *See, e.g., Muggill v. Reuben H. Donnelley Corp.*, 398 P.2d 147 (Cal. 1965) (loss of pension benefits); *Beneficial Life Ins. Co. v. Knoblauch*, 653 F.2d 393, 396 (9th Cir. 1981) (advances); *Ware v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 24 Cal. App. 3d 35, 42-43, 100 Cal. Rptr. 791, 796-97 (1972) (forfeiture of rights and profit sharing plan).

3. However, where an employee signed a confidentiality agreement or a covenant not to disclose trade secret information without the employer's consent, California courts will grant an injunction against actual or threatened use of misappropriated trade secrets, *see, e.g., Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 66 Cal. Rptr. 2d 731 (1997).
4. In those states which allow non-compete agreements, in determining whether to enforce a noncompetition agreement, the court must consider the potential harm to the employee from the type of restriction involved including the employee's ability to support him or herself during the noncompetition period and the impact on the employee's ability to reestablish his occupation after the noncompetition period expires. The court must balance those impacts against the harm to the former employer including the impact on its relationships with customers, where the court may consider how long it would take for a new employee to redevelop those relationships, and impact on trade secrets and confidential information where the court would look at how long the information would remain current.

B. Arizona

1. In Arizona, public policy generally disfavors restraints of trade, including agreements which limit an employee's ability to seek or accept work. *Valley Med. Specialists v. Farber*, 194 Ariz. 363, 367, 982 P.2d 1277, 1281 (1999); *Bryceland v. Northey*, 160 Ariz. 213, 216, 772 P.2d 36, 39 (Ct. App. 1989). Covenants not to compete are enforceable, but only to the extent of the employer's "legitimately protectable interests." *Amex Distrib.Co. v. Mascari*, 150 Ariz. 510, 515, 724 P.2d 596, 601 (Ct. App. 1986).

2. Arizona courts apply a three-part balancing test to determine the enforceability of restrictive covenants. *See Valley Med. Specialists v. Farber*, 194 Ariz. 363, 367, 982 P.2d 1277, 1281 (1999); *Truly Nolen Exterminating, Inc. v. Blackwell*, 125 Ariz. 481, 610 P.2d 483 (Ct. App. 1980); *see also Lassen v. Benton*, 86 Ariz. 323, 324-25, 346 P.2d 137, 138-39 (1959). Under this test, a non-compete provision in an employment agreement is enforceable only when the restraint on the employee:
 - a. is not beyond that reasonably necessary to protect the employer's legitimate business interests,
 - b. is not unreasonably restrictive upon the rights of the employee, and
 - c. does not contravene public policy.
3. The restrictive covenant must also be reasonable in geographic scope. *Olliver/Pilcher Ins. Inc. v. Daniels*, 148 Ariz. 530, 532, 715 P.2d 1218, 1220 (Ariz. 1986). The reasonableness of the geographic scope depends upon the circumstances and the nature of the restriction, and may be influenced by its duration. *See Alpha Tax Servs., Inc. v. Stuart*, 158 Ariz. 169, 761 P.2d 1073 (App. 1988).
4. *Varsity Gold, Inc. v. Porzio*, 202 Ariz. 355, 45 P.3d 352, 45 P.2d 352 (2002). (The Court ruled that Arizona law prohibits the rewriting of overly broad restrictive covenants, even where the parties' agreement specifically authorized the court to modify the covenant's restrictions to render them reasonable and enforceable. The Court affirmed the trial court's conclusion that the geographic scope of the restrictive covenant in question was unreasonable because it prohibited competition in Pennsylvania and contiguous states while the evidence showed that defendant had worked with plaintiff only in the southern portion of Pittsburgh and the plaintiff had no active sales representatives anywhere in the State of Pennsylvania other than its two representatives in Pittsburgh.)
5. Additionally, the restraint must be limited to the particular specialty of the present employment. *Valley Med. Specialists v. Farber*, 194 Ariz. 363, 367, 982 P.2d 1277, 1281 (1999).

6. The employer's "legitimate protectable interests," which can be covered by a non-compete agreement, do not include a desire to limit competition.
 - a. As a matter of Arizona law, a person's skills and abilities, including the tools "for the aggressive pursuit of success in a highly competitive field of business," cannot be the subject of a restrictive agreement. *Amex Distrib. Co.*, 150 Ariz. at 515-516, 724 P.2d at 601-602. *See also Bryceland*, 160 Ariz. at 217, 772 P.2d at 40 ("A restrictive covenant is not enforceable to prevent a former employee from using the skills and talents he learns on the job in a new job"). Thus, an employer cannot use a restrictive covenant to keep his former employee from entering the workforce as a competitor on the basis that the employee learned skills or developed talents of the trade while working for the employer. In addition, eliminating or avoiding competition is not a legitimate protectable interest. *Amex Distrib. Co.*, 150 Ariz. at 518, 724 P.2d at 604.
 - b. An employer does have a protectable interest in maintaining customer relationships and in protecting information about its clients when an employee leaves. This interest cannot be protected indefinitely, however, and will generally be protected only "for as long as may be necessary to replace the employee and give the replacement a chance to show that he can do the job." *Bryceland*, 160 Ariz. at 217, 772 P.2d at 40. In addition, the restraint must not unreasonably restrict the rights of the employee.
 - c. When customer relationships are at issue, depending on the skills necessary to conduct the employee's job, most courts hold that a restraint for a period of several months would usually be reasonable, although a longer period may be justified if the selling relationship was relatively complex. *See Bryceland* (holding two-year restriction on disc jockey unreasonable, in light of evidence that "it took approximately fourteen weeks for adequate schooling and on-the-job training of new personnel" to replace the employee)
 - d. In addition, the appropriate duration of a restrictive covenant is shorter when the particular market is more competitive and the former employer's

business is less “unique.” *See Truly Nolen*, 125 Ariz. at 482, 610 P.2d at 484.

C. Oregon

1. In the context of employment relationships, Oregon Revised Statutes § 653.295 prohibits noncompetition agreements, i.e., any agreement that prevents a former employee from providing similar products or services, unless the agreement is secured “upon initial employment” or upon a “subsequent bona fide advancement.”
 - a. Section 653.295 excludes agreements to forfeit unpaid bonuses or profit-sharing in the event of post-employment competition, provided the agreement specifies a period of time, geographic area, and the activities restricted. This exception is only available for agreements with employees who are substantially involved in management; personally contact customers; or have knowledge of relevant customer requirements, trade secrets, or other proprietary information of the employer.
 - b. “Initially-employed,” for purposes of section 653.295, means the time that the employee starts work. *Olsten Corp. v. Sommers*, 534 F. Supp. 395, 397-98 (D. Or. 1982).
 - c. Except in the event of bona fide advancement, section 653.295 prohibits enforcing a subsequent noncompetition agreement with more burdensome terms than in the agreement entered into at the time of initial employment. *Pac. Veterinary Hosp., P.C. v. White*, 72 Or. App.533, 538, 696 P.2d 570, 572-73 (1985). See also *IKON Office Solutions, Inc. v. American Office Products, Inc.*, 178 F. Supp.2d 1154 (D. Oregon 2001) *aff’d*, 2003 WL 1818589 (9th Cir. April 4, 2003) (The case involved a requested preliminary injunction against two employees who moved to a direct competitor, and a claim against the competitor. With regard to one of the employees, the court found that the noncompetition agreement was void under Oregon law because it was signed seventeen days after the employee commenced his employment. With regard to both employees, the court found that the plaintiff was estopped to enforce the noncompetition agreements because prior to their move to the competitor, plaintiff informed each of the

employees and the competitor that there were no noncompetition agreements in place, and only after the employees switched employers and the new employer made an extremely large investment in a new office did the former employer find copies of the noncompetition agreements and attempt to enforce them.)

2. Oregon law generally disfavors contracts that restrain the ability to carry on a trade or profession. Even if the statutory requirements are met or inapplicable, e.g., the sale of a business to non-employees accompanied by a non-compete agreement, Oregon courts have required additional criteria to enforce non-compete agreements, *Olsten Corp. v. Sommers*, 534 F. Supp. 395, 397 (D. Or. 1982):
 - a. Non-compete agreements must be limited in duration and geographic area,
 - b. Non-compete agreements must be supported by consideration, and
 - c. Non-compete agreements must be reasonable and not unduly restrictive. The restrictions must protect a legitimate interest, e.g., customer contacts and proprietary information. The hardships imposed on the party agreeing to the restrictions must not be unreasonable or unduly interfere with public interests.

D. Washington

1. In Washington, covenants not to compete must be accompanied by consideration. Continued employment and training are sufficient consideration to enforce an agreement not to compete upon separation from employment. *Knight, Vale and Gregory v. McDaniel*, 37 Wash. App. 366, 368-69, 680 P.2d 448, 451 (1984).
2. In Washington, the restrictions of non-compete agreements must be reasonable. To determine reasonableness, Washington courts balance the public interest in the availability of goods and services and the impact on the employee against the interests of the protected party. *Lehrer v. Dep't of Social and Health Servs.*, 101 Wash. App. 509, 513, 5 P.3d 722, 725 (2000). Three criteria must be met to enforce a non-compete agreement:

- a. The restraint must be necessary to protect the business or goodwill of the employer,
 - b. Restrictions must not impose restraint greater than that required to protect the business interests, and
 - c. The injury to the public due to the loss of the products and services must be slight.
3. Contracts restraining competition will only be enforced in Washington when the restrictions are reasonable. *Copier Specialists, Inc. v. Gillen*, 76 Wash. App. 771, 773, 887 P.2d 919, 920 (1995) (voiding a covenant not to compete based solely on training the employee received to repair business equipment, where employee had limited contact with customers and no access to customer lists). Restrictions must be no greater in scope than required to protect the employer's business or goodwill. *Knight, Vale and Gregory v. McDaniel*, 37 Wash. App. 366, 370, 680 P.2d 448, 452 (1984) (finding a non-compete agreement reasonable and enforceable where an accountant agreed to refrain for three years from serving any clients contacted as a direct result of former employment).
 4. Washington Courts will apply the test of reasonableness to noncompetition agreements, and enforce agreements only as far as reasonableness dictates. *Alexander & Alexander, Inc. v. Wohlman*, 19 Wash. App. 670, 686-87, 578 P.2d 530, 539-40 (limiting enforcement of an agreement between a Seattle brokerage office and a former employee to prevent selling to customers of the brokerage office in the greater Seattle area for a period of two years).
 5. Courts are required to examine non-compete agreements carefully, even when a legitimate business interest has been demonstrated, due to the equally compelling concern for freedom of employment and public access to goods and services. *Knight, Vale and Gregory v. McDaniel*, 37 Wash. App. 366, 370, 680 P.2d 448, 452 (1984).

E. Colorado

1. Colorado Revised Statutes § 8-2-113 prohibits agreements that prevent a former employee from receiving “compensation for skilled or unskilled labor” from any subsequent employer, with four exceptions:
 - a. Contracts to sell or purchase a business or the assets of a business,
 - b. Contracts to protect trade secrets,
 - c. Contractual provisions to recover training and education costs, limited to employees who have worked less than two years, and
 - d. Contracts restricting the future employment of officers, executives, and management personnel as well as the professional staff of management and executives.
2. In addition to subsequent employment, Colorado’s statutory restrictions on covenants not to compete apply to subsequent self-employment. *Mgmt. Recruiters of Boulder, Inc. v. Miller*, 762 P.2d 763, 765 (Colo. Ct. App. 1988).
3. Colorado law disfavors covenants not to compete and construes the statutory exceptions narrowly. *Gold Messenger, Inc. v. McGuay*, 937 P.2d 907, 910 (Colo. Ct. App. 1997). Absent a statutory exception, covenants not to compete are contrary to public policy and void. *DBA Enters., Inc. v. Findlay*, 923 P.2d 298, 302 (Colo. Ct. App. 1996).
4. Even if a covenant not to compete meets a statutory exception, Colorado law further requires that restrictions be reasonable. *Am. Express Fin. Advisors, Inc., v. Topel*, 38 F. Supp. 2d 1233, 1238 (D. Colo. 1999).
5. Temporal and geographic scope of the covenant not to compete must be reasonable. *Nutting v. RAM Southwest, Inc.*, 106 F. Supp. 2d 1121, 1226-27 (D. Colo. 2000) (finding perpetual and worldwide ban on marketing similar product unreasonable in duration and scope under Colorado law); *Elec. Distrib. v. SFR, Inc.*, 166 F.3d 1074, 1086 (10th Cir. 1999) (finding a covenant enforceable under

Colorado law where the employee was prevented from engaging in the wholesale electrical supply business anywhere in Utah for seven years).

6. While an assignee may enforce a covenant not to compete, once a business benefiting from a restrictive covenant is terminated or abandoned, the right to enforce a restrictive covenant is extinguished. *Nat'l Propane Corp. v. Miller*, 18 P.3d 782, 785-87 (Colo. Ct. App. 2000) (finding an assignment enforceable, but limiting enforcement to the period before assignee closed the business office, ceased operating under the purchased business name, and merged the assets and operations into its existing operations); *Gibson v. Eberle*, 762 P.2d 777, 778-79 (Colo. Ct. App. 1988) (distinguishing the instant case from selling a business as a going concern, when the owner liquidated the assets and inventory and leased the location to others for unrelated use).
7. To fit within the statutory exception for trade secrets, the purpose of the covenant must be protecting trade secrets, and the restriction must be reasonably limited in scope to the protection of trade secrets. *Gold Messenger, Inc. v. McGuay*, 937 P.2d 907, 910 (Colo. Ct. App. 1997). Merely inserting a companion clause regarding trade secrets will not validate a covenant not to compete agreement otherwise void under Colorado law. *Dresser Indus. v. Sandvick*, 732 F.2d 783, 787-88 (10th Cir. 1984).
8. *Energex Enterprises, Inc. v. Anthony Doors, Inc.*, 2003 WL 1217490 (D. Colo. Mar. 6, 2003). (Plaintiff revealed confidential information and trade secrets to defendant pursuant to a confidential disclosure agreement in the course of developing a business arrangement. Defendant eventually declined to go forward and developed a competing product, which eventually contained much of the confidential information revealed to it. In analyzing the breach of contract claim, the Court found that the confidentiality agreement contained both a non-disclosure clause and a non-competition clause. It found that the agreement did not violate C.R.S. § 8-2-113 on its face and also because of the exception for contracts for the protection of trade secrets. Nevertheless, the Court determined that it had to determine whether the agreement could be construed as reasonable in duration or geographic scope, which were found to be fact questions that could not be determined on a motion to dismiss.)

9. *Quizno's Corporation v. Kampendahl*, 2002 WL 1012997 (N.D. Ill. May 20, 2002). (The Court concluded that a non-competition covenant preventing defendant from operating a sandwich shop within five miles of his Quizno's restaurant was reasonable both in geographical scope and substantive scope because the Court interpreted the term "sandwich shop" to mean a sandwich shop using the same format, signage and recipes used as a Quizno's franchisee. The Court also concluded that the franchise agreement fell within two exceptions to the general prohibition on non-compete agreements under the Colorado Revised Statutes §8-2-113: first, a franchise agreement is equivalent to a sale of business, and second, a franchise agreement has the purpose of protecting trade secrets.)

F. Restrictive Covenants Involving the Internet

1. For those states which recognize noncompetition provisions, they require a balancing between the employer's legitimate business interests against the employee's right to pursue his chosen livelihood.
2. A recent case involved the Internet industry and found that a twelve-month noncompetition agreement was unreasonable given the dynamic nature of the industry, *EarthWeb v. Schlack*, 71 F. Supp. 2d 299 (S.D.N.Y. 1999), *aff'd* for denial of preliminary injunction based on restrictive covenant, *remanded* for further findings of fact for denial of preliminary injunction against use or disclosure of information, 205 F.3d 1322 (2d Cir. 2000) (unpublished). The court refused to enforce a noncompetition agreement or apply the inevitable disclosure doctrine to enjoin plaintiff's former employee for working for another online company in the information technology industry. The employee had worked for a long time as a senior editor of print magazines focusing on the software and Internet industries. While at EarthWeb he worked as a vice president in charge of worldwide content relating to several web sites. After a year he moved to another web site company. There was conflicting testimony regarding whether the companies would be competing. The court found that the noncompete agreement, which had a duration of one year, was too long given the dynamic nature of the Internet industry and it was not necessary to protect EarthWeb's trade secrets, since there was little evidence that the former employee had access to any of them, and that much of the information did not rise to the level of trade secrets. The court also declined to apply the inevitable

disclosure doctrine finding no imminent and inevitable risk of disclosure. The court was also reluctant to use the doctrine to alter the express terms of a restrictive covenant.

G. Other Types of Agreements Which Limit New Employment

1. The Ninth Circuit also upheld a covenant which required an employee to return profits from stock options if he worked for a competitor within six months of exercising the stock options, *IBM Corp. v. Bajorek*, 191 F.3d 1033, 1041 (9th Cir. 1999). Another bona fide method of restricting a former employee's ability to compete is to enter into a bona fide consulting agreement involving a non de minimus payment term, *Crespinel v. Color Corp. of America*, 160 Cal. App. 2d 386, 325 P.2d 565 (1958).
2. *Weissman v. Transcontinental Printing USA, Inc.*, 205 F. Supp. 2d 415 (E.D. Pa. 2002). (Plaintiff and former employer entered into a written employment contract that provided for base salary monetary payments for a year after termination without cause and a restrictive covenant which precluded disclosing confidential information, and contained a non-competition provision, and a non-solicitation provision. The Court found the covenant not to compete to violate New York law but declined to find that the other provisions violated New York law. The Court found that the post-termination base salary payments were for the purpose of compensating plaintiff for his early termination and also for the non-solicitation agreement. It found that the payments would compensate him for the time during which he lacked paid employment and on account of his early termination. Thus, the Court found that plaintiff was entitled to the payments only for the time that he was unemployed.)
3. Some companies have drafted far more narrow noncompetition agreements which allow an employee to join a competitor but provide that the employee will not render services directly or indirectly in connection with any product which would compete with the former employer's current or anticipated business. Such an agreement may be combined with a nonsolicitation agreement.
4. The courts may not always prohibit a former employee from working for a competitor in order to protect the former employer's trade secrets. Sometimes

the courts will fashion a remedy which screens the employee from positions where they would use, rely on or disclose their former employer's trade secrets. In *Merck & Co. v. Lyon*, 941 F. Supp. 1443 (M.D.N.C. 1996) the former Merck employee was prohibited from discussing anything related to Merck's product line with his new employer for a period of up to two years.

IV. THE ENFORCEABILITY OF NON-SOLICITATION CLAUSES

A. Non-Solicitation Agreements – No Recruit Clauses In General

1. In a non-solicitation agreement, an employee agrees not to solicit the business of his or her employer's customers for some period of time after the employment relationship is terminated. A no-recruit or no-hire clause is an added agreement whereby an employee, usually a manager, agrees not to recruit his or her colleagues for a new employer.
2. Some courts have upheld nonsolicitation provisions while rejecting no hire provisions, *see, e.g. The Ingle Co. v. VideoTours, Inc.*, 116 F.3d 1485 (9th Cir. 1997) and *Loral Corp. v. Moyes*, 219 Cal. Rptr. 836, 844 (Ct. App. 1985). In *Combined Ins. Co. v. Hansen*, 756 F. Supp. 458, 462 (D.Or. 1991), the court upheld a two-year nonsolicitation provision and in *Harrison v. Sarah Coventry, Inc.*, 184 S.E.2d 448, 449 (Ga. 1971), the court upheld a two-year nonsolicitation provision.
3. In *Lane Co. v. Taylor*, 330 S.E.2d 112, 117 (Ga. Ct. App. 1985), the court upheld a one-year agreement which contained both a nonsolicitation and no hire provisions.
4. At least one court rejected a nonsolicitation provision because its geographic scope was unreasonable—the plaintiff was attempting to apply it to employees of defendant's former employer in Indiana in a situation where the employee had formerly worked in California, *see, Cap Gemini America, Inc. v. Judd*, 597 N.E.2d 1272, 1287 (Ind. Ct. App. 1992).
5. *See also, CMI International, Inc. v. Internet International Corp.*, 251 Mich. App. 125, 649 N.W. 2d 808 (Mich. App. 2002). (The parties entered into a confidentiality agreement pursuant to merger discussions which prohibited the

defendant from hiring any of plaintiff's employees for 18 months, followed by a later agreement which prevented the defendant from soliciting any of plaintiff's employees for 18 months. Plaintiff was eventually purchased by another company and its chief technology officer was demoted to a business-oriented position, which he held for a time. He then resigned, sought out employment with defendant and was eventually hired. The Court denied injunctive relief, finding that the second agreement superseded the first and that there was no evidence of solicitation. The Court declined to find any threatened misappropriation because plaintiff failed to specify any trade secrets that would be misappropriated.)

6. *MicroStrategy, Inc. v. Business Objects, SA*, 233 F. Supp. 2d 789 (E.D. Va. 2002). (Court interprets non-solicitation clause under Virginia law. The Court found that it was reasonable in duration as it only lasted for one year. The Court declined to strike down the clause prohibiting the solicitation of Microstrategy customers, but found that the clause prohibiting the solicitation of employees of Microstrategy was overbroad and therefore struck it down.)

B. California

1. California courts will enforce an anti-employee solicitation covenant with the former employer, see, e.g., *Loral Corp. v. Moyes*, 174 Cal. App. 3d 268, 275, 219 Cal. Rptr. 836 (1985). See also, *GAB Bus. Servs., Inc. v. Lindsey & Newsom Claim Servs., Inc.*, 83 Cal. App. 4th 409, 416-423, 99 Cal. Rptr. 2d 665, 669-675 (4th Dist. 2000) (Individual former officers subject to a claim for unfair competition due to their role in enticing seventeen key employees of plaintiff to move companies.)
2. California courts will enforce covenants against solicitation of customers where the customer identities or specific information regarding the customers constitute trade secrets, see, e.g., *Courtesy Temporary Service, Inc. v. Camacho*, 222 Cal. App. 3d 1278, 272 Cal. Rptr. 352, 360 (1990); *Gordon v. Wasserman*, 153 Cal. App. 2d 328, 330, 314 P.2d 759 (1957); *Weissensee v. Chronicle Publishing Co.*, 59 Cal. App. 3d 723, 728, 129 Cal. Rptr. 188 (1976). Some such covenants have not been enforced where the customer information was not kept in a confidential manner and did not acquire trade secret status, *Moss, Adams & Co. v. Shilling*,

179 Cal. App. 3d 124, 130, 229 Cal. Rptr. 456 (1986). A recent Ninth Circuit decision upheld a covenant barring a subcontractor from soliciting or dealing directly with a specifically named customer, *General Commercial Packaging, Inc. v. TPS Package Eng., Inc.*, 126 F.3d 1131, 1134 (9th Cir. 1997).

C. Arizona

1. Anti-piracy agreements, or agreements not to solicit employees or customers of the employer, are enforceable in Arizona to protect the former employer's interests. See, e.g., *Olliver/Pilcher*, 148 Ariz. 530, 715 P.2d 1218; *Alpha Tax Servs., Inc.*, 158 Ariz. 169, 761 P.2d 1073. Such agreements are more narrow than covenants not to compete, in that they are "designed to prevent former employees from using information learned during their employment to divert or to steal customers from the former employer." *Alpha Tax Servs., Inc.*, 158 Ariz. at 171, 761 P.2d at 1075. However, like restrictive covenants, in the absence of a protectable interest, such agreements are unenforceable. See, *Hilb, Rogal and Hamilton Co. v. McKinney*, 190 Ariz. 213, 946 P.2d 464 (Ct. App. 1997).
2. Like covenants not to compete, anti-piracy agreements are subject to certain restrictions. For example, an employee's agreement not to solicit customers of his prior employer does not prohibit the employee from merely informing those customers that his employment has changed, or from accepting the unsolicited invitation from a former client to do business. *Alpha Tax Servs., Inc.*, 158 Ariz. at 171-72, 761 P.2d at 1075-76. Nor is the former employee prohibited from advertising his new business in newspapers or through broad-based mailings, so long as the employer's clients are not purposefully targeted. *Id.* at 172, 761 P.2d at 1076.
3. Protection of the employer's business relationships should extend only to those clients with whom the employee had actual business relationships. See *Amex*, 150 Ariz. at 518, 724 P.2d at 604. See also *Bryceland*, 160 Ariz. at 217, 772 P.2d at 40 (noting, without deciding, that a restriction against competing for "any potential customer or client" of the former employer may be overly broad, because it goes beyond restricting the employee's use of the relationships he established while working for the employer). Thus, anti-piracy agreements typically cannot prohibit an employee from doing business with the employer's

customers whom the employee did not service. *Amex*, 150 Ariz. at 517, 724 P.2d at 603 (employer has “no protectable interest in denying [former employee] the right to compete for a customer it last serviced 35 months ago, and which [the employee] never knew.”).

4. No recruit clauses are subject to similar restrictions. The clause must be reasonable in scope, and typically cannot prevent a former employee from accepting, as opposed to soliciting, job applications from former employer’s current employees.

D. Oregon

1. Oregon’s statutory limitation on noncompetition agreements covers agreements preventing former employees from soliciting customers. Non-solicitation agreements must be secured when the employee starts work or upon a bona fide advancement. *Dymock v. Norwest Safety Protective Equipment*, 334 Ore. 55, 45 P.3d 114 (2002). (The Supreme Court reversed a judgment on behalf of an employee who was terminated for refusing to sign an agreement after the employee was already working, finding that the statute renders such agreements void, but did not confer a right on the employees to refuse to sign such agreements. Since plaintiff had no other provision it could point to allowing it to refuse to sign the agreement, it denied his claim.) (construing Or. Rev. Stat. § 653.295).
2. Oregon courts will enforce no-hire clauses, provided the prohibited activity and a time period are specified in the agreement. *See Combined Ins. Co. v. Hansen*, 756 F. Supp. 458, 462 (D. Or. 1991) (enforcing an agreement entered into upon termination providing a district manager additional compensation in exchange for a two year promise not to induce employees to leave the company and work for a competitor).

E. Washington

1. Anti-solicitation agreements are enforceable in Washington, subject to the requirement of reasonable restrictions. *See, e.g., Perry v. Moran*, 109 Wash. 2d 691, 697, 748 P.2d 224, 227 (1987) (enforcing as valid and reasonable an agreement that prevented an accountant from serving former customers for three

years following separation from employment, and in the alternative required as liquidated damages half of any fees so earned), *modified on reconsideration*, 111 Wash. 2d 885, 766 P.2d 1096 (remanding for factual determination of the reasonableness of the liquidated damages clause); *Knight, Vale and Gregory v. McDaniel*, 37 Wash. App. 366, 370, 680 P.2d 448, 452 (1984) (enforcing an accountant's agreement to refrain for three years from serving any clients contacted as a direct result of former employment).

F. Colorado

1. Colorado law requires that the terms of a non-solicitation agreement be reasonable in scope and duration. *Nat'l Graphics Co. v. Dilley*, 681 P.2d 546, 547 (Colo. Ct. App. 1984) (finding unlimited duration and scope unreasonable even though the non-compete agreement was limited to customers serviced by the former employee). See also *Atmel Corp. v. Vitesse Semiconductor Corp.*, 2001 WL 125909 (Colo. App. 2001) (Court narrowly construed anti-solicitation clause to prevent former employee from actually soliciting employees but not from interviewing employees who had approached new employer.)

V. INEVITABLE DISCLOSURE AND INTERNET RELATED CASE LAW

A. Inevitable Disclosure Doctrine

1. The Inevitable Disclosure Doctrine is a method of proving a misappropriation claim. It is based on the theory that certain employees cannot resign and work for a competitor without inevitably using, in their new jobs, their former employer's trade secrets, even if they do not intend to.
2. To prevail on an inevitable disclosure claim, a Plaintiff must prove the following:
 - a. The employee had access to trade secrets of his former employer (using the same definition found in the Uniform Trade Secrets Act, cited above);
 - b. The employee was hired by a competitor of the former employer, to whom such trade secrets would have an economic or competitive advantage; and

- c. The employee's position with the competitor makes the use of trade secret knowledge “likely to result” or “impossible not to result.”
3. Inevitable disclosure does not require a showing of improper acquisition of trade secrets, or intent to misappropriate. Rather, the analysis focuses on the employee’s position with the current and former employers; *i.e.*, his decision-making authority and influence, and whether the employee could perform his job for the new employer without inevitably using the former employer’s trade secrets, even if acting in good faith. Traditionally, this doctrine is applied only to very high-ranking employees who occupy a similarly high rank at the competitor.
4. Although not required by the inevitable disclosure analysis, it is a plus factor to preliminary injunction balancing when the prior employer had restrictive covenants or confidentiality agreements in place which are in danger of being violated.
5. The leading inevitable disclosure case is *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995). Redmond had been PepsiCo’s California General Manager. His position gave him access to significant confidential information and trade secrets, including PepsiCo’s strategic plans, operational innovations, and marketing decisions. Quaker, one of PepsiCo’s direct competitors, recruited Redmond. Eventually Redmond accepted the position of Vice President of Quaker’s Gatorade division. Redmond had kept the status of his negotiations with Quaker secret from PepsiCo, during which time he obtained greater access to PepsiCo’s customers. Less than a week after Redmond informed PepsiCo of his new employment with Quaker, PepsiCo filed suit seeking a preliminary injunction to enjoin Redmond from assuming his duties at Quaker and to prevent him from disclosing trade secrets and confidential information to Quaker. PepsiCo argued that Redmond could not work at his job at Quaker without using that information.

Although PepsiCo failed to produce sufficient evidence of actual misappropriation, the Seventh Circuit upheld the injunction entered against Redmond. The court concluded that PepsiCo had presented substantial evidence that Redmond possessed extensive knowledge about PepsiCo’s trade secrets and

business plans and that Redmond would inevitably use that information in his position with Quaker, even if he tried to avoid doing so.

6. In *Doubleclick Inc. v. Henderson* (1997 WL 731413 (N.Y. Sup. 1997)) an online advertising firm secured a preliminary injunction preventing two former executives from competing with it for a term of six months. Both dependents had entered into confidentiality agreements with their employer. One had entered into a noncompetition agreement, but it did not clearly apply to the facts of the case. One of the defendants had access to the plaintiff's business plan, revenue projections, future project plans, pricing and product strategies and databases with information concerning plaintiff's clients. The other defendant had access to the same confidential information and other documents distributed only to top management. Both defendants worked to create a competing Internet advertising agency while still employed by Doubleclick. They drafted a business plan, sought out investors and customers and began discussions with at least one other employee. Plaintiff Doubleclick persuaded the courts that its trade secrets included the rates it has charged its customers, its site shares, and the percentages it earned from various customers. The court noted that Internet advertising companies used different software and sales techniques to maximize their advertising. The court felt that the defendants could not eliminate Doubleclick's trade secrets from their minds. The court's injunction prohibited the defendants from operating a competing business for six months. However, they were not prohibited from working in the field of Internet advertising, finding that they could work for companies that engaged in advertising in a variety of media including the Internet so long as they did not become involved in the company's Internet advertising projects
7. *Barilla America, Inc. v. Wright*, 2002 WL 31165069 (S.D. Iowa July 5, 2002). (The Court applied the threatened disclosure standard and the inevitable disclosure standard and enjoined the plant manager from working at AIPC or any competitor for one year, misappropriating Barilla's trade secrets and maintaining trade secret information he had been provided. The plant manager had been given access to extensive trade secret information concerning Barilla's premium methods for producing pasta, its secret manufacturing processes and vendor and financial information, including extensive CDs containing the same. At the time

of hearing, the plant manager had not returned all of the CDs and pictures he took of manufacturing facilities in Italy while on a trip there.)

8. *Willis of New York, Inc. v. DeFelice*, 299 A.D.2d 240, 750 N.Y.S.2d 39 (App. Div. 2002). (The Court modified an injunction against certain insurance brokers who went to work for a competitor. The Court held that the trial court's order which restrained three of the employees from soliciting clients actually enforced restrictive covenants entered into those by those employees. Since the employer had not shown that two of those employees were unique, they should not have been enjoined. The third employee's services were unique and the two-year duration of his restrictive covenant was found to be reasonable. Since he was working at the New York office of a competitor, it was found to be reasonable to enforce a restrictive covenant covering New York. However, the Court found that the record showed that many of that broker's clients were loyal to him personally and he should not be enjoined from soliciting the clients he originally brought with him to the plaintiff's or related accounts. With regard to a portion of the trial court's order which restrained the individual defendants from divulging plaintiffs' confidential or proprietary information, the plaintiffs failed to demonstrate that they would likely prevail in demonstrating that the individual defendants were in fact misappropriating and exploiting their confidential information. However, two of the defendants were undisputedly high-level employees with access to confidential information that could be easily utilized by them in their new positions to their former employers' detriment. The Court found that it was inevitable that they would disclose confidential information and therefore found the likelihood of irreparable injury.)
9. Practical Considerations.
 - a. The doctrine of inevitable disclosure has been criticized by several courts that have considered it outside of the Seventh Circuit, and various commentators have argued that the theory allows a former employer to "create" a covenant not to compete when none was bargained for, and restricts competition in the absence of the necessary elements for a traditional misappropriation claim. There is no clear trend reflected in recent decisions. *See, e.g., Electro Optical Indus., Inc. v. White*, 76 Cal. App. 4th 653, 90 Cal. Rptr. 2d 680 (1999) (depublished).

- b. *Bayer Corp. v. Roche Molecular Sys., Inc.*, 72 F. Supp. 2d 1111, 1119 (N.D. Cal. 1999) (Holds that the inevitable disclosure theory is not the law in either California or the Ninth Circuit.); *Del Monte Fresh Produce Co. v. Dole Food Co.*, 148 F. Supp.2d 1326 (S.D. Fla. 2001) (The court found no actual or threatened disclosure of trade secrets by a high level scientist who moved from one firm to its competitor, and found that neither Florida nor California recognizes the Inevitable Disclosure Doctrine, so the court denied plaintiff's request for a preliminary injunction.); *Globespan Inc. v. O'Neill*, 151 F. Supp.2d 1229 (C.D. Cal. 2001) (The court ruled that the Central District of California has considered and rejected the Inevitable Disclosure Doctrine.); *Cardinal Health Staffing Network, Inc. v. Bowen*, ___ S.W.3d ___, 2003 WL 1742180 Tex. App. - Hous. (1 Dist. April 3, 2003). (Court denied temporary restraining order based on lack of irreparable injury and the Court was unwilling to use the inevitable disclosure doctrine as a substitute for irreparable injury.); *Safety-Kleen Systems, Inc. v. McGinn*, 233 F. Supp. 2d 121 (D. Mass. 2002). (The Court rejected breach of contract and trade secret claims because there was no evidence of actual disclosure of any confidential information, and no evidence that defendant had breached an agreement by soliciting any customers with whom he was contact while at plaintiff's. The Court declined to adopt the inevitable disclosure doctrine in the matter.); *Schlage Lock Company v. Whyte*, 101 Cal. App. 4th 1443, 125 Cal. Rptr. 2d 277 (Cal. App. 2002). The Court affirmed the denial of a preliminary injunction because the evidence established that the defendant did not threaten to or actually misappropriate the plaintiff's trade secrets. In so doing, the Court also rejected the inevitable disclosure doctrine as the law of California, primarily because it creates a *de facto* covenant not to compete after the employment contract is made, usually containing a confidentiality agreement, but not a non-compete provision. The application of the inevitable disclosure doctrine gives the employer the benefit of a contractual provision it did not pay for, while the employee is bound by a court-imposed contract provision, with no opportunity to negotiate terms or consideration.).
- c. *See, Marietta Corporation v. Fairhurst*, 754 N.Y.S.2d 62 (App. Div. 2003). (Defendant had an employment contract which included a confidentiality provision and an express covenant not to compete effective for so long as he continued receiving payments from plaintiff, up to a maximum of one year.

When that agreement expired, plaintiff had defendant sign a separate non-durational confidentiality agreement, with no express restriction on competitive employment or participation. Defendant left his employer and joined plaintiff's direct competitor, after which he contacted several customers to inform them of his new affiliation and to initiate a relationship on behalf of his new employer. The Court found no persuasive evidence that defendant had intentionally disclosed any proprietary information. The trial court applied the inevitable disclosure doctrine and enjoined the defendant's continued employment by the competitor for a period of 11 months. On appeal, the injunction was reversed, because no evidence was proffered to support the assertion that defendant had already intentionally disclosed any proprietary information and the non-competition agreement was not in effect, there was no evidence that he had breached the confidentiality agreement or that the confidential information also constituted a trade secret. The Court declined to use the inevitable disclosure doctrine, finding it an implied in fact covenant not to compete, and that it should not allow an end-run around the confidentiality agreement. Thus the injunction was dissolved.)

- d. Distilling the cases that have applied the doctrine, proof of the following elements will be required:
 - (i) the two employers are direct competitors in a highly competitive industry;
 - (ii) the defecting employee has knowledge of trade secrets that are integral to the products or services of the former employer;
 - (iii) the former employee's job duties and responsibilities for the new employer are substantially similar to his old ones;
 - (iv) the new employer has not provided adequate measures to preclude the disclosure of trade secrets; and
 - (v) although perhaps not technically a formal element, courts may want to see circumstantial evidence of an intent to misappropriate such as a

lack of candor in the employee's departure or actual misappropriation of other trade secrets or confidential information.

10. Inevitable Disclosure Exit Interview Tip

- a. During the exit interview, be sure to ask departing employees what kind of work they will be doing for their new employer. Document the interview.

B. Trade Secrets on the Internet: Putting the Genie Back Into the Bottle

1. In *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745 (E.D. Mich. 1999) the court refused to enjoin the posting of plaintiff's trade secrets on a web site. The court concluded that the requested preliminary injunction would have amounted to a prior restraint and violation of the first amendment. However, in *Conley v. DSC Communications Corp.* (1999 WL 89955 (Tex. Ct. App. Feb. 24, 1999)), the court rejected a first amendment overbreadth challenge to a trade secret injunction because the injunction was the only way to prevent destruction of the trade secret.
2. A series of cases involving the Church of Scientology attempted to protect trade secret confidential religious documents which had been posted online by former scientology members. In *Religious Technology Center v. Lerma*, 897 F. Supp. 260, 266 (E.D.Va. 1995), the court declined trade secret protection because the documents had "escaped into the public domain and onto the Internet." The court ruled that the defendant was not the only source of the documents containing the secrets on the Internet, and ruled that the plaintiff could not establish that the documents are not "generally known." Later in the same case, the same judge ruled that the allegedly confidential documents had been posted on the Internet and remained available for more than ten days "potentially available to the millions of Internet users around the world." The court granted a summary judgment to one of the defendants on the misappropriation of trade secrets claim, *Religious Technology Center v. Lerma*, 908 F. Supp. 1362, 1368 (E.D.Va. 1995). In *Religious Technology Center v. F.A.C.T. Net, Inc.*, 901 F. Supp. 1519 (D.Co. 1995), the court noted that publication on the Internet would destroy the trade secret status of any allegedly confidential documents. The court found that the work had come into the public domain by numerous means but

portions had been made available on the Internet with the potential to be downloaded by millions of users. Similarly, in *Religious Technology Center v. Netcom On-Line Communications Servs., Inc.*, 923 F. Supp. 1231 (N.D.Cal. 1995), the court found that there was evidence that many persons had put the material into the public domain. Even though the defendant could not rely on his own postings to the Internet to support the argument that the documents were no longer trade secrets, postings by others were found to have destroyed the trade secret status. In that opinion the court expressed frustration that any Internet user, including those acting maliciously, could destroy valuable intellectual property rights by posting them over the Internet.

3. In a later case, *DVD Copy Control Association, Inc. v. McLaughlin*, 2000 WL 48512 (Jan. 21, 2000), the court ordered the removal from the Internet of postings revealing the DVD encryption code even though they had been online for over three months. The court concluded that the trade secret owners had moved quickly to protect their rights and that injunctive relief was appropriate, and that to hold otherwise would encourage misappropriators of trade secrets to post them on the Internet to destroy the trade secret status of the information. On appeal, the California Court of Appeals held that computer source code is protected by the First Amendment, that the program in issue, DeCSS, is a written expression of the author's ideas and information about decryption of DVDs, and that the trial court injunction was an unconstitutional prior restraint on defendant's right to publish the DeCSS program, *DVD Copy Control Ass'n v. Bunner*, 113 Cal Rptr. 2d 338 (2001), review granted, 117 Cal Rptr. 2d 167 (2002).

**FACTORS CONSIDERED BY COURTS IN
APPLYING INEVITABLE DISCLOSURE
DOCTRINE TO PROTECT TRADE SECRETS
BY PRELIMINARY INJUNCTIONS**

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<i>Pepsico, Inc. v. Redmond</i> , 54 F.3d 1262 (7 th Cir. 1995) (<u>no</u> restrictive covenant; confidentiality agreement).	Evidence of <u>bad faith</u> demonstrates a willingness to misuse trade secrets (at 1270-71).	Both were high-level marketing positions.	None shown or alleged - injunction granted because disclosure was "inevitable" (at 1270).	Marketing and business strategies, "pricing architecture" (at 1265).	<u>Injunction granted</u> prohibiting Defendant from "assuming his position" at Quaker for six months (the life of the trade secrets at issue) (at 1267, 1272).
<i>Merck & Co. v. Lyon</i> , 941 F. Supp. 1443 (M.D.N.C. 1996) (<u>no</u> restrictive covenant; confidentiality agreement).	Although not requiring a showing of bad faith (at 1460), finding that former employee's misrepresentations show his willingness to use former employer's proprietary information to advance his career (at 1461).	"Involve similar responsibilities," although his new position was "broader" (at 1460-61).	None shown – court held that <u>threat</u> was sufficient (at 1457).	Marketing strategies and product launch dates.	<u>Injunction granted</u> prohibiting former employee from working on a particular product (antacids), as opposed to general area of expertise, because trade secrets were limited to those competing products (at 1458).

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<i>La Calhene, Inc. v Spolyar</i> , 938 F. Supp. 523 (W.D. Wis. 1996) (non-compete agreement; confidentiality agreement).	None shown.	Both involved marketing and management responsibilities.	None shown – injunction may be granted based on <u>threat</u> of disclosure (at 531).	Technologies relating to containment of hazardous materials, and marketing and business strategies.	<u>Injunction granted</u> for one year, prohibiting defendant from “participating directly or indirectly in businesses that <u>deal with or relate to</u> products or services that are the <u>same or similar</u> ” to plaintiff’s and from having <u>any</u> contacts with plaintiff’s suppliers or customers or potential customers he dealt with at Plaintiff (at 532).
<i>FMC Corp. v. Varco Int’l, Inc.</i> , 677 F.2d 500 (5 th Cir. 1982) (no restrictive covenant).	Acknowledgement that former employee <u>does not know what constitutes a trade secret</u> indicates likelihood of disclosure (at 504).	Both were high level engineering positions.	None shown - but employee’s salary was tied to performance (indicating likelihood of disclosure) (at 504).	Mechanical design of oil field fitting and flow technology.	<u>Enjoining</u> disclosure of trade secrets, and enjoining former employee from holding <u>any</u> position that “poses an inherent threat of disclosure or use of FMC’s trade secrets” (at 505).

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<p><i>Novell, Inc. v. Timpanogos Research Group, Inc.</i>, 46 U.S.P.Q.2d 1197 (D. Utah 1998) (no restrictive covenant).</p>	<p>Former employee's "<u>predatory intent</u>," and his "penchant . . . for <u>deliberate misrepresentation</u>" show high probability of disclosure of trade secrets (at 1215, 1204).</p>	<p>At plaintiff employer, the individual defendants (engineers) were the 2 principal inventors of the trade secrets; at their new employer, they continued to develop equivalent technologies.</p>	<p>One defendant's computer hard drive was irretrievably damaged, indicating an intent to "prevent recovery of deleted material" and a "malicious intent" to misappropriate (1204, and 1211, n.3). Another defendant finally produced a notebook containing plaintiff's trade secrets (after avowing he had none in his possession) -- court found his defense of "forgetfulness" incredible (at 1205, 1206).</p>	<p>Technical information regarding computer software development (including "negative knowledge" of "what worked and did not work") (at 1202) and the unique manner in which "public domain concepts" are combined (1214).</p>	<p><u>Enjoining</u> defendants from engaging in the same "field" of software development (involving the technologies they had developed or learned at plaintiff) for nine months (at 1210, 1218).</p>
<p><i>Lumex v. Highsmith</i>, 919 F. Supp. 624 (E.D.N.Y. 1996) (restrictive covenant).</p>	<p>Notwithstanding former employee's <u>good intentions</u> and candor, court found that disclosure was inevitable (at 630, and 631).</p>	<p>High level marketing at both.</p>	<p>None shown - but similarity of positions and employee's bonus and salary structure rendered disclosure inevitable (at 631).</p>	<p>Pricing, marketing and product information regarding fitness machines.</p>	<p><u>Enjoining</u> defendant employee from "working with or for" defendant employer, or from soliciting plaintiff's customers (at 636).</p>

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<p><i>National Starch and Chem. Corp. v. Parker Chem. Corp.</i>, 530 A.2d 31 (N.J. Super. Ct. App. Div. 1987) (<u>no</u> restrictive covenant).</p>	<p>None shown.</p>	<p>Only 5% - 10% of duties were similar.</p>	<p>None shown or alleged -- circumstances gave "rise to an inference that substantial threat of disclosure exists" (at 33).</p>	<p>Information (including trial and error process) regarding the development, manufacturing and marketing of envelope adhesives.</p>	<p><u>Enjoining</u> former employee from performing <u>any work</u> at competitor in the area of envelope adhesives for 15 months, because new employer had tried unsuccessfully to create a similar formula that defendant could recite from memory (at 32, 33).</p>
<p><i>DoubleClick Inc. v. Henderson</i>, 1997 W.L. 731413 (N.Y. Sup. Ct. 1997) (one of the 2 former employees signed a very limited restrictive covenant; both entered confidentiality agreements).</p>	<p>Defendants' "cavalier attitude" and evidence of actual misappropriation "bolstered" the court's finding of inevitable disclosure (at *5, 6).</p>	<p>Both high level management executive.</p>	<p>Yes.</p>	<p>Revenue projections, pricing and product strategies and client information for Internet advertising business.</p>	<p><u>Enjoining</u> defendants for 6 months (life of trade secrets) from "launching any company ..., which competes with DoubleClick," where defendants' job functions would include "any aspect of" those they had at plaintiff. (at *8)</p>

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<i>Air Prods. & Chems., Inc. v. Johnson</i> , 442 A.2d 1114 (Pa. Super. Ct. 1982) (no restrictive covenant).	No dispute as to defendant's integrity (at 1118).	Employee's primary responsibility (on-site gas sales) for plaintiff was one of his many duties for defendant.	None alleged.	Technical data concerning on-site gas delivery methods, negotiations with clients, market opportunities and other "commercial" trade secrets.	<u>Enjoining</u> former employee from "accepting employment or being engaged in, directly or indirectly, the on-site or tonnage gas business" and prohibiting new employer from hiring employee "in any capacity involving directly or indirectly" the alleged trade secrets (at 1125).
<i>American Totalisator Co. v. Autotote Ltd.</i> , 1983 WL 21374 (Del. Ch. 1983) (no restrictive covenant; no confidentiality agreement).	None alleged against individual defendant, but court noted that hiring of individual defendant represented the corporate defendant's second hiring of "critical administrative officers" of plaintiff corporation.	Both high level management positions.	None shown or alleged.	Strategic plans for bidding, profit and loss reports, projected costs and profits, and specific contract proposals, all regarding equipment and services for the wagering industry.	<u>Enjoining</u> defendants from using plaintiff's trade secrets in bidding for contracts.

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<p><i>Branson Ultrasonics Corp. v. Stratman</i>, 921 F. Supp. 909 (D. Conn. 1996) (non-compete agreement; confidentiality agreement).</p>	<p>None alleged.</p>	<p>Court found “significant overlap” and substantial similarity between former employee’s engineering positions at old and new companies.</p>	<p>None alleged. Note: case does not involve a claim for trade secret misappropriation. Instead, the court used an inevitable disclosure analysis in arriving at the conclusion that the plaintiff would suffer irreparable harm if preliminary injunction enforcing non-compete and confidentiality agreements were not granted.</p>	<p>Computer controls for ultrasonic joining equipment.</p>	<p><u>Injunction granted</u> for remainder of one-year period contained in non-compete agreement, prohibiting defendant from continuing to work for new employer.</p>

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<p><i>Southwestern Energy Co. v. Eickenhorst</i>, 955 F. Supp. 1078 (W.D. Ark. 1997) (confidentiality agreement).</p>	<p>After gaining access to confidential information relating to adversary's oil and gas leases as attorney for a natural gas production company, attorney then resigned her position at law firm and filed a proposed class action on behalf of royalty owners against companies whose records she had reviewed.</p>	<p>None: case did not involve employee changing jobs.</p>	<p>Plaintiffs alleged actual use of trade secret information.</p>	<p>Natural gas company's production data, volume and price information, lease files, royalty owner records, and title opinions and abstracts.</p>	<p>None: court denied defendant's motion for summary judgment on misappropriation of trade secrets claim (noting that "injunctive relief should be granted to protect trade secrets where there is a belief, not simply that future acts are threatened, but that such acts will in all probability be committed"), and held that plaintiffs could maintain their action for injunctive relief.</p>

Case	Defendant's Bad Faith or Incredibility	Similarity of the Positions	Actual Misappropriation of Trade Secrets	Type of Trade Secrets at Issue	Scope of Injunction
<p><i>Ackerman v. Kimball Int'l, Inc.</i>, 652 N.E.2d 507 (Ind. 1995) (non-compete agreement; confidentiality agreement).</p>	<p>Defendant engaged in “pre-departure harvesting” of former employer’s proprietary customer and supplier lists; when later questioned about the whereabouts of those lists, defendant claimed that he had left them in his old office. Lists were never found.</p>	<p>Both were high-level executive positions.</p>	<p>None shown – court affirmed trial court’s finding of threat of misappropriation.</p>	<p>Customer and supplier lists.</p>	<p>On appeal, affirming trial court’s entry of an injunction prohibiting defendant from accepting direct or indirect employment with defendant corporation or any of plaintiff’s other competitors for a period of one year.</p>
<p><i>Uncle B’s Bakery, Inc. v. O’Rourke</i>, 920 F. Supp. 1405 (N.D. Iowa 1996), <u>modified</u>, 938 F. Supp. 1450 (N.D. Iowa 1996) (non-compete agreement; confidentiality agreement).</p>	<p>Plaintiff alleged that former employee absconded with original copy of his non-compete/non-disclosure agreement, but court found both plaintiff and defendant credible on the issue. Plaintiff also alleged that former employee concealed his intent to work for a competitor.</p>	<p>Bagel plant manager for both old and new employer.</p>	<p>None shown – court found “significant danger of an inadvertent disclosure” by former employee.</p>	<p>Recipes and manufacturing process for refrigerated bagels.</p>	<p>Injunction granted prohibiting former employee from working for any entity which competes directly or indirectly with former employer within a 500 mile radius of any of former employer’s marketing outlets, until further order of the court.</p>

VI. FORMS APPENDIX

- A. Sample E-mail Policy**
- B. Sample Investigation Questionnaire**
- C. Sample Non-Compete, Non-Solicitation Clause**
- D. Sample Non-Disclosure Clause**
- E. Confidentiality and Non-Disclosure Agreement**
- F. Forms of Residuals Clauses**

Exhibit "A" Description of Confidential Information

A. Sample E-Mail Policy:

All electronic communication systems and all electronic communications and stored information transmitted, received, or contained in or over the employer's information systems are the property of the employer and, as such, are to be used solely for job-related purposes. This includes e-mail passing over employer's system and information viewed on the World Wide Web. Additionally, the employee's use of such equipment and software for private purposes is strictly prohibited. Employees using these systems, equipment and software for personal purposes do so at their own risk. Further, employees shall not use a code, access a file or retrieve any stored communication, other than where authorized, unless there has been prior clearance by an authorized company representative.

FURTHERMORE, NO EMPLOYEE SHALL FORWARD ANY CONFIDENTIAL COMPANY DOCUMENT TO A NON-EMPLOYER E-MAIL ADDRESS WITHOUT PRIOR SUPERVISORY APPROVAL.

Violators of this policy are subject to disciplinary action, up to and including discharge from employment. To ensure that the use of the employer's information systems, equipment and software, and other electronic communications systems is consistent with the employer's legitimate business interests, authorized representatives of the employer may monitor the use of the systems, equipment, and software from time to time.

Use of these systems constitutes consent to monitoring as stated above.

[Attach an acknowledgement form to be signed by employee and returned to HR]

B. Sample Investigation Questionnaire:

1. Describe in detail how Competitor competes with Company and how long it has been in competition with Company.
2. What is the specific market in which Competitor competes with Company?
3. Does Competitor need a device, concept, product or other property that Company has developed? If so, describe in detail.
4. Has Competitor tried to obtain the device, concept, product or other property in any other way? If so, describe how.
5. Did any of the employees download or print an unusual amount of information prior to leaving?
6. Did anyone review the contents of the computers used by any of the employees after their departure?
7. Did any of the employees try to hide the fact that they were leaving?
8. Was all Company property returned?
9. Do travel or expense records reflect possible contact with Competitor?
10. What Company technical trade secrets and technical confidential information does the employee possess? Describe in detail.
11. Why is it a trade secret or confidential information?
12. What Company commercial trade secrets and confidential information does the employee possess? Did the employee have possession or knowledge of business plans, pricing structures, special customer requirements and the like?
13. Why is it a trade secret or confidential information?

14. If some of this information has been released to our customers, was it released under a nondisclosure agreement with the customer?
15. What is the value of the trade secret information possessed by each employee and for how long it will be valuable?
16. What steps are taken in your operation to maintain the secrecy or confidentiality of trade secret information in general? What steps were taken to maintain the secrecy of this specific trade secret information?
17. Do you believe that your operation has lost or is likely to lose, any future contracts or business opportunities as a result of these employees' departure and/or misappropriation of trade secrets? Which customers? Which opportunities?
18. Are you aware of any recruiting engaged in by the former employees on behalf of Competitor prior to their departure?
19. Who conducted the exit interviews for each of the departing employees?
20. Do you know what the former employees are currently working on at Competitor?
21. Do you know whether Company has recruited any employees from Competitor in the past two years?
22. What compensation was each of the former employees receiving at Company?
23. Do you know what type of financial package Competitor offered each of the former employees?
24. Is there anything else that you should tell me?

C. Sample Non-Compete, Non-Solicitation Clause:

The employee shall not, for a period of [insert reasonable duration in relation to facts] ____ months (years) following the termination of the employee's employment with the employer, directly or indirectly, render competing services to or, with respect to such services, solicit any actual [or active prospective] customer of the employer for whom the employee performed services while employed by the employer during the ____ months preceding the employee's termination of employment with the employer nor render competing services to or competitively solicit with respect to such services within a ____ mile radius of the employer's principal place of business in _____.

D. Sample Non-Disclosure Clause:

Except as shall be required by, in the course of, in connection with, and during the employee's employment, the employee shall not during or after his employment with the employer use or disclose the employer's proprietary information without the employer's prior written authorization.

E. Confidentiality and Non-Disclosure Agreement:

1. Covenant of Non-Disclosure and Non-Use.

As a material inducement to each party to furnish such party's Confidential Information to the other party the Confidential Information, each party hereby covenants and agrees that, subject to the provisions set forth in Section 5 hereof, it shall not, directly or indirectly or intentionally, disclose any of the other party's Confidential Information, or any portion thereof, to any person or party, or use or exploit the other party's Confidential Information, or any portion thereof, or suffer or permit any of its agents, representatives or employees, to so disclose, use or exploit the same except in order to evaluate and consummate the Acquisition, without first obtaining the express written consent of the other party to such disclosure, use or exploitation.

2. Reproduction of Confidential Information Prohibited.

Each party agrees that it shall not copy, photograph, photocopy, reduce to writing or otherwise reproduce or duplicate the other party's Confidential Information other than for its own use or for the use of its authorized agents which use shall not be in violation of this Agreement.

3. Return of Confidential Information.

Each party shall return to the other party, within a reasonable time following such other party's written demand for return of the same, all physical manifestations of such other party's Confidential Information (other than information covered by any subparagraph of Section 5 hereof). All notes, summaries, abstracts, compilations and analyses of the other party's Confidential Information in each party's possession or control shall be maintained by each party in confidence or be destroyed if requested by the other party.

4. Limited Obligation.

Under no event or circumstance is either party obligated to disclose or make available to the other party any information, including the Confidential Information, which such

party in its sole discretion, refuses or objects to disclosing. The decision by either party to make available to the other party such party Confidential Information or any portion thereof or any other information rests in the sole and absolute discretion of such party. Purchaser and Company both acknowledge and agree that each of their resourcing methodologies and partners are extremely confidential and sensitive and that each of them will most likely elect to disclose such portions of that Confidential Information to the other party only after completion of other due diligence and resolution of all major business issues.

5. Duration of Confidentiality Obligations.

The obligations of each party under this Agreement to maintain the confidentiality of the other party's Confidential Information and not to use it shall continue for a period of five (5) years from the date hereof; provided, however, such obligations shall terminate upon the occurrence of any of the following, but only to the extent hereafter described: (a) where such information is now or hereafter becomes part of the public domain, but only to the limited extent it, or any portion thereof, is in the public domain not as a result of any breach or violation of this Agreement or (b) any information which is already or hereafter comes into the possession of either party from a third party without breach of this Agreement, or without any breach by the third party of any confidentiality obligation to such party or any other person or entity or without any misappropriation or improper means. If Purchaser or any subsidiary or any successor makes the Acquisition prior to August 31, 1999, or prior to any further date mutually agreed to between Company and Purchaser, Company agrees to maintain the confidentiality of all Confidential Information for a period of five (5) years from the date of the Acquisition.

EXHIBIT "A"

Description of Confidential Information

Subject to the exclusionary provisions of Section 5 of this Agreement, the term “Confidential Information” shall mean and include all of the following information that is hereafter provided by either party under this Agreement:

1. All financial statements and other financial information.
2. All existing and prospective customers and accounts and any information regarding the amount, nature and type of business of those customers or accounts and the identity of the primary contact persons with such customers or accounts.
3. Any proprietary software programs and/or information systems, routines or subsystems, and any documentation thereof, owned by either party.
4. Any forecasts, business plans or similar assessments of the business of either party or projections regarding further business of either party.
5. All advertising and marketing strategies, methods, research and related data.
6. The names of any consultant recruiters, vendors, suppliers or software consultants.
7. The cost, type and quantity of materials and/or supplies ordered by either party.
8. The prices that either party obtains or has obtained or sells or has sold its services.
9. The parties’ respective resourcing, recruiting and sales methods, costs and objectives.
10. Any technical information owned by either party.
11. Any inventions owned by either party.
12. Any pending or issued patents owned by either party.

13. Any drawings, specifications, methods of quality control and formulas or equations used in connection therewith by either party.
14. The compensation, performance evaluations and any other terms and conditions of employment of employee, except to the extent any such information is provided by any employee or other person not legally bound to keep such information confidential.
15. Any “trade secrets” owned by either party as such term is defined in Section 3426.1(d) of the California Civil Code.
16. Such other confidential information or data owned by either party of any kind, nature or description as hereafter expressly identified in writing by either party to the other party as being confidential and owned by a party and as having been provided solely for purposes of this Agreement.

F. Forms of Residuals Clauses:

Notwithstanding anything herein to the contrary, Owner acknowledges that Contractor shall benefit from the skill, knowledge and experience acquired by Contractor prior to its association with Owner under this Agreement and further acknowledges that as an independent contractor, Contractor must be free to continue to use and build upon such skills, knowledge, expertise and experience. Consequently, the parties agree that Contractor shall be free to use and provide to other persons, work and products, ideas, concepts, expressions, designs and information similar to the work, products, ideas, concepts, expressions, designs and information furnished under this Agreement.

Exception for Commonly Used Skills and Know-how. Notwithstanding any other provision in this Agreement, and recognizing the Company's exclusive ownership of all Works created by Employee, the parties recognize that the development and creation of these Works may require the skills and experience of Employee which have been developed over time. These skills include industry standard knowledge of the general state of computer software programming and hardware solutions applicable to the business lines of the company. To avoid any unreasonable restriction on Employee, and to induce Employee to grant Company the protections afforded it under this Agreement, Employee retains the right to use industry standard knowledge comprising and including ideas, techniques and concepts, and general skills used by it in developing and creating the Works. This exception is solely intended to assure that Employee's skills which are commonly present and routinely practiced by similarly situated information services employees are not subject to the exclusive ownership and assignment provisions of this Agreement. The terms and existence of this clause shall be treated as confidential information not to be disclosed by Employee without the consent of the Company.

IBM Confidentiality form

5. EXCEPTIONS

No obligation of confidentiality applies to any information that the Recipient:

- a) already possesses without obligation of confidentiality;
- b) develops independently; or
- c) rightfully receives without obligation of confidentiality from a third party.

No obligation of confidentiality applies to any information that is, or becomes, publicly available without breach of this Agreement.

In addition, no obligation of confidentiality applies to any ideas, concepts, know-how, or techniques contained in Information that are related to the Recipient's business activities (Knowledge). However, this does not give the Recipient the right to disclose, except as set forth elsewhere in this Agreement, 1) the source of Knowledge, 2) any financial, statistical or personnel data, or 3) the business plans of the Discloser.

Neither this Agreement nor any disclosure of Information grants the Recipient any license under any patents or copyrights.

NOTHING IN THIS AGREEMENT SHALL BE DEEMED TO ASSIGN TO OWNER OR PROHIBIT CONTRACTOR FROM USING ITS GENERAL KNOW-HOW, TECHNIQUES, TOOLS, EXPERTISE, OR OTHER UNIQUE CAPABILITIES WHICH IT USES EITHER IN THE DEVELOPMENT OF ANY DELIVERABLES UNDER THIS AGREEMENT OR IN ITS PERFORMANCE UNDER ANY ASSIGNED TASK, EVEN IF THE SAME WERE REFINED OR IMPROVED DURING THE COURSE OF THE CONTRACTOR'S WORK UNDER THIS AGREEMENT. NOTHING SHALL BE DEEMED TO LICENSE CONTRACTOR UNDER ANY OWNER'S INVENTIONS, PATENTS, COPYRIGHTS, OR TRADE SECRETS.

4. *Handling of Confidential Information*

Each party agrees that at all times and notwithstanding any termination or expiration of this Agreement it will hold in strict confidence and not disclose to any third party Confidential

Information of the other except as approved in writing by the other party to this Agreement, and will use the Confidential Information for no purpose other than _____ with the other party to this Agreement. Each party shall only permit access to Confidential Information of the other party to those of its employees or authorized representatives having a need to know and who have signed confidentiality agreements or are otherwise bound by confidentiality obligations at least as restrictive as those contained herein.

5. Residual Knowledge

Recipient may use its knowledge retained in intangible form in the unaided memories of its directors, employees, contractors and advisors as a result of exposure to the disclosing party's ("Discloser") Confidential Information. The Discloser acknowledges that the Recipient may have in conception or development technology and/or software which may be very similar or even identical to Discloser's Confidential Information and, as long as the Recipient abides by Section 4 herein, Discloser shall have no rights in such technology and/or software.
