GUARDING THE CROWN JEWELS: A GUIDE TO PROTECTING YOUR TRADE SECRETS

by

Arthur J. Schwab
David J. Porter
Buchanan Ingersoll

Foreword
by
Laura Stein
Senior Vice President and General Counsel
H.J. Heinz Company

Introduction
by
John K. Williamson
Assistant General Counsel,
Intellectual Property
PPG Industries

WASHINGTON LEGAL FOUNDATION
WASHINGTON, D.C.

This Monograph is one of a series of original papers published by the Legal Studies Division of the Washington Legal Foundation. Through this and other publications, WLF seeks to provide the national legal community with legal studies on a variety of timely public policy issues. Additional copies of this Monograph may be obtained by writing to the Publications Department, Washington Legal Foundation, 2009 Massachusetts Avenue, N.W., Washington, D.C. 20036.

Other recent studies in the WLF Monograph series include:

A Corporate Counsel's Guide To Discovery In The Information Age by David E. Dukes, James K. Lehman, Michael W. Hogue, and Jason B. Sprenkle, Nelson Mullins Riley & Scarborough, LLP. Foreword by The Honorable Shira A. Scheindlin, U.S. District Court for the Southern District of New York. Introduction by Thomas Y. Allman, Senior Vice President and General Counsel, BASF Corporation. 2001. Library of Congress No. 01-200110977127.

Agricultural Biotechnology: Will Regulatory "Precaution" Expand Liability Risks? by Thomas P. Redick, Esq. Foreword by U..S. Representative Nick Smith. 2001, Library of Congress No. 00-111633.

Daubert *And Its Progeny: Scientific Evidence In Product Liability Litigation* by Frederick T. Smith, McCarter & English LLP. Foreword by John L. McGoldrick, Senior Vice President, Law and Strategic Planning, General Counsel & President, Medical Devices Group, Bristol-Myers Squibb Company. Introduction by The Honorable Harold R. DeMoss Jr., U.S. Court of Appeals for the Fifth Circuit. 2000, Library of Congress No. 99-075716

Attorney-Client Privilege And "Crime-Fraud" Exception: The Erosion Of Business Privacy by The Honorable Dick Thornburgh, Kirkpatrick & Lockhart LLP. Foreword by Stephen L. Hammerman, Vice Chairman and General Counsel, Merrill Lynch & Co., Inc. Introduction by Lawrence A. Salibra, Senior Counsel, Alcan Aluminum Corporation. 1999, Library of Congress No. 99-071355.

Officers And Directors: Liability Exposure Under Civil And Criminal Law by Matthew J. Iverson, Litchfield Cavo, and Stephan M. Kowal, Bell, Boyd & Lloyd. Foreword by Clayton K. Yeutter, Of Counsel, Hogan & Hartson LLP. Introduction by Rick Harrington, Senior Vice President and General Counsel, Conoco Inc. 1999, Library of Congress No. 99-070976.

The Qui Tam *Quagmire: Understanding The Law In An Era Of Aggressive Expansion* by J. Andrew Jackson and Edward W. Kirsch, Dickstein Shapiro Morin & Oshinsky LLP. Foreword by Norman R. Augustine, Chairman of the Board, Lockheed Martin Corporation. Introduction by The Honorable Dick Thornburgh. 1998, Library of Congress No. 98-062037.

Library of Congress Catalog Card No. 2002101077

GUARDING THE CROWN JEWELS: A GUIDE TO PROTECTING YOUR TRADE SECRETS

by

Arthur J. Schwab
David J. Porter
Buchanan Ingersoll

Foreword
by
Laura Stein
Senior Vice President and General Counsel
H.J. Heinz Company

Introduction
by
John K. Williamson
Assistant General Counsel,
Intellectual Property
PPG Industries

WASHINGTON LEGAL FOUNDATION
WASHINGTON, D.C.

FOREWORD

by
Laura Stein
Senior Vice President and General Counsel
H.J. Heinz Company

The corporation has been described as a "nexus of contracts" among interested parties. Under this view, the corporation is a web of contractual relationships linking shareholders, employees, managers, creditors, suppliers, customers and others whose activity bears upon the goals of the firm. This includes the state, whose enabling legislation provides a kind of standard form contract that can facilitate contractual relationships.

Intellectual property and trade secrets are increasingly prominent features in these various contractual relationships. That is just as true for global consumer product companies such as my employer, H.J. Heinz Company, as it is for Internet-based and software firms. Doing business with potential business partners or suitors, lenders, advisors, consultants, customers and even governments creates opportunities for the disclosure of confidential or proprietary information.

Antecedent to these relationships is the one between the corporation and its own team of managers and employees — the people who on a daily basis create, process and add value to the firm's confidential information. Accordingly, an effective system of trade secret protection must address the risks of misappropriation or inadvertent disclosure by those who are the earliest and most frequent handlers of the firm's confidential information. A fundamental principle applies to the subject of trade secret protection: security begins at home.

This monograph is a superb introduction to matters relating to trade secret protection, from drafting tips to litigation strategies. Its authors are experienced advisors and trial advocates who deal with such matters in state and federal jurisdictions across the country. Their monograph covers in a very practical manner many

of the key issues that corporations must consider in deciding how to protect their valuable proprietary information.

INTRODUCTION

by
John K. Williamson
Assistant General Counsel,
Intellectual Property
PPG Industries

There is no issue more critical to the success and survival of American businesses today than the need to protect proprietary technology and information from misappropriation by competitors. In simpler times — before globalization and the information age — basic physical security provided adequate protection in most industries. Strong employee loyalty to long-term employers and the sheer bulk of hard copy information served as powerful deterrents to misappropriation. But as the protection derived from traditional physical security continues to erode with advances in electronic storage and transfer of information, and as employee mobilization increases, the importance of effective legal protection becomes paramount.

Advising clients regarding implementation of appropriate legal measures to guard against trade secret theft presents a dilemma for the practitioner. Overly burdensome measures can introduce inefficiencies in a business and may infringe upon the rights of employees. Strict "need to know" processes can be effective but are not compatible with today's collaborative work environment. Employers may take comfort in having broad, iron clad non-compete agreements with their employees but these may be unenforceable in many jurisdictions.

On the other hand, measures designed to be transparent to the business and its employees may not offer adequate protection for valuable information assets. Basic employee confidentiality agreements provide little assistance when key employees defect to direct competitors.

Striking the right legal balance in developing and implementing an information protection strategy is critical. Finding this equilibrium requires a thorough understanding of the issues and the applicable laws.

This monograph summarizes fundamental principles of trade secret law, describes contractual terms that should be used to protect trade secrets and confidential information, and highlights issues typically associated with trade secret litigation. It is an indispensable tool for the business law practitioner.

ABOUT THE AUTHORS

Arthur J. Schwab is Chief Counsel - Complex Litigation and past Chair of Litigation in the law firm of Buchanan Ingersoll, Pittsburgh, Pennsylvania. His litigation practice includes commercial and banking disputes, antitrust, securities and other class actions, technology litigation, employment matters and non-profit tax-exemption litigation.

Over the past 20 years, Mr. Schwab's nationwide practice has focused on the areas of trade secrets, confidential information, employment agreements (covenants not to compete and confidentiality agreements), software copyright infringement, trademark, unfair competition and diversion of corporate opportunities.

Mr. Schwab is past Chair of the Civil Litigation Section of the Pennsylvania Bar Association; past President of the American Inns of Court — Pittsburgh Chapter; past member of the Board of Governors of the Academy of Trial Lawyers of Allegheny County; and past Chair of the Council of the Civil Litigation Section of the Allegheny County Bar Association. Mr. Schwab has also been a frequent speaker at numerous seminars and conferences relating to trial strategies, damages, litigation ethics, evidence, transfer of technology, law and technology, trade secrets and employment agreements. He also serves on the faculty of the Trial Advocacy Institute of the University of Virginia School of Law.

Mr. Schwab is a graduate of the University of Virginia School of Law (Order of the Coif), serving on the *Virginia Law Review*, and clerked for the Honorable Collins J. Seitz, then Chief Judge of the United States Court of Appeals for the Third Circuit. He received his undergraduate degree from Grove City College.

David J. Porter is a shareholder in the law firm of Buchanan Ingersoll, Pittsburgh, Pennsylvania. His litigation practice includes protection of trade secrets and confidential information, restrictive covenants, unfair competition and related business torts. He has litigated a wide variety of commercial and shareholder disputes in state and federal courts.

Mr. Porter also represents print and electronic media in all phases of the news gathering and publishing process, including media access, pre-publication review, and libel and First Amendment litigation. He has represented some of the nation's most prominent publishers of newspapers, books, magazines and television programming.

Mr. Porter has published numerous articles relating to trade secret protection, including: "Protecting Confidential Information: The Nondisclosure Agreement," in *CorporateIntelligence.com*; "Federal Protection of Trade Secrets: Understanding the Economic Espionage Act of 1996," in the *Journal of Proprietary Rights*; and "Enjoining Competitive Employment in the Absence of a Covenant Not to Compete," in the *Pittsburgh Legal Journal*.

Prior to joining Buchanan Ingersoll, Mr. Porter clerked for the Honorable D. Brooks Smith of the United States District Court for the Western District of Pennsylvania. Mr. Porter is a graduate of the George Mason University School of Law, where he served on the editorial board of the *George Mason University Law Review*. He received his undergraduate degree from Grove City College.

TABLE OF CONTENTS

INTRODUCTION 1

I. **BASIC PRINCIPLES** 2

A. **What Is a Trade Secret?** 2

1. ***Restatement Definition*** 2
2. ***Uniform Trade Secrets Act*** 4

B. **How to Protect a Trade Secret? — Maintaining Secrecy and Security of Confidential Information** 6

1. ***General Security Measures*** 6
a. External Security Measures 6
b. Internal Security 6
2. ***Protection Through Applications/ Policy Manuals*** 7
3. ***Protecting Computer-Related Information*** 7

C. **Agreements Not to Disclose Trade Secrets and Covenants Not to Compete** 8

1. ***Confidentiality Agreements*** 9
2. ***Covenants Not to Compete*** 9
a. Duration 9
b. Scope 9
c. Consideration 10

D. **Post-Employment Considerations** 10

1. ***Informal Investigation — The***

Exit Interview 10
2. ***Post-Employment Documentation*** . . . 11
a. Statement Executed by Employee 11
b. Correspondence to New Employer 12

E. **Litigation** 12

1. ***Potential Causes of Action*** 13
2. ***Discovery*** 13
3. ***Injunctive Relief*** 13
4. ***Damages*** 14

II. **WHAT IS A TRADE SECRET?** 15

A. **Uniform Trade Secrets Act** 15
B. **Section 757 of the First Restatement of Torts** 16
C. **The Economic Espionage Act** 17
D. **Requirements of Confidentiality and Economic Value** 18

1. ***Information Must Be Kept Sufficiently Confidential*** 18
2. ***Information Must Derive Economic Value*** 19

E. **Information That Has Been Afforded Trade Secret Protection** 20

1. ***Scientific Information*** 20
2. ***Computer Information*** 21
3. ***Business Information*** 23
a. Business and Strategic Plans . . 23
b. Pricing and Credit Policies 23
c. Marketing Plans 24

d. Financial Information 24
e. Customer Lists 25
f. Compilations of Information . . 26
4. ***An Employee's General Skill and Knowledge*** 27

III. **COVENANTS NOT TO COMPETE IN THE EMPLOYMENT CONTEXT** 27

A. **Initial Considerations** 28
B. **Validity of Covenants Not to Compete** 29

1. ***How the Protectable Interest and Restriction Relate*** 30
2. ***Is the Restriction Reasonable in Time and Geographic Limitations?*** 31
3. ***Undue Hardship on the Employee*** . . 33
4. ***Consideration in Exchange for the Covenant*** 34

C. **Miscellaneous Drafting Considerations** . . . 35

IV. **POST-EMPLOYMENT CONSIDERATIONS: HOW TO PREVENT THE LOSS OF TRADE SECRETS AND CUSTOMERS** 36

A. **Post-Employment Procedures** 37

1. ***Effect of Involuntary Termination*** . . . 38
2. ***The Exit Interview*** 38
3. ***Protecting the Customer Base*** 41
a. Protecting the Customer List . . 42
b. Importance of Communicating with Customers During the Transition Phase 43
4. ***Whether to Provide Notice to the***

New Employer 44
a. A Word of Caution Regarding Interference with Contractual Relations 45

V. **ENFORCEMENT OF TRADE SECRET RIGHTS** 45

A. **To Sue or Not to Sue** 46
B. **Fact-Finding** 48
C. **Initial Tactical Decisions** 49

1. ***Whether to Send a Warning Letter*** . . 49
2. ***Where to Sue*** 50
3. ***Whom to Sue*** 51

D. **Temporary or Preliminary Injunctive Relief** 51
E. **Initial Pleadings** 52
F. **Motions for TRO and/or Preliminary Injunction** 54
G. **Motion for Order of Court Directing Preservation of Documents, Software and Things** 54
H. **Motions for Expedited Discovery and Proposed Order Setting Specific Dates for Depositions and Production of Documents** 55
I. **Protective Orders** 55

VI. **DISCOVERY IN A TRADE SECRET/ COVENANT CASE** 56

A. **Discovery Goals and Objectives** 56
B. **Likely Motions** 56

1. ***Motion to Expedite*** 56

2. ***Motion to Preserve Evidence*** 57
3. ***Motion for Protective Order*** 58

C. **Sources and Types of Information** 59

1. ***The Plaintiff Company*** 59
2. ***Ex-Employee and New Employer*** 60
3. ***Recruiters*** 62

D. **Discovery of Computer and Electronic Data** 63

1. ***Internal Investigation*** 63
2. ***Discovery of Computer Data from Defendants*** 64

VII. **RELIEF AVAILABLE IN TRADE SECRET MISAPPROPRIATION CASES** 65

A. **Overview of Available Relief** 66

1. ***Injunctive Relief*** 66
2. ***Royalties*** 68
3. ***Unjust Enrichment*** 68
4. ***Exemplary Damages*** 69
5. ***Attorneys' Fees*** 69
6. ***Prejudgment Interest or Lost Opportunity Costs*** 69
7. ***Tort Recovery*** 70

B. **Monetary Relief** 70

1. ***Relief Theories*** 70
   a. Legal Damages 71
   b. Equitable Damages 72
   c. Market Share Damages 74
2. ***Proof of Damages*** 75

a. Actual Damages 75
b. Deductions 76

VIII. **FEDERAL PROTECTION OF TRADE SECRETS: UNDERSTANDING THE ECONOMIC ESPIONAGE ACT OF 1996** . . . 76

A. **Trade Secret Law: An Overview** 77

1. ***Common Law*** 77
2. ***Restatement of Torts*** 77
3. ***Uniform Trade Secrets Act*** 78

B. **Legislative Background of the Act** 79
C. **Analysis of the Act** 81

1. ***Definition of "Trade Secrets" Under the EEA*** 81
a. Types of Trade Secrets 82
i. *The EEA Expands the UTSA's List of Representative Trade Secrets* 82
ii. *The EEA Expressly Protects Intangible Information* 83
iii. *The EEA Protects Information Existing in Any Form Without Regard to the Means by Which it is Stored* 83
b. Trade Secrets Must Be Protected by "Reasonable Measures" 84
c. Trade Secrets Derive Value Through Not Being Known or Readily Ascertainable by Others . . 85

2. ***Conduct Prohibited by the EEA*** 86
3. ***Some Possible Ambiguities*** 87
a. Reverse Engineering 87
b. The EEA Only Protects Trade Secrets Related To Products Produced for or Sold in Interstate/ Foreign Commerce 88
c. Criminal State of Mind 88
d. Criminal Penalties 89
i. *Fines and Prison Terms* 89
ii. *Criminal Forfeiture* . . . 89

D. **Handling an Economic Espionage Act Violation** 89
E. **Conclusion** 92

APPENDIX A: States Adopting Uniform Trade Secrets Act 93

APPENDIX B: Exit Interview Sample Forms 97

GUARDING THE CROWN JEWELS: A GUIDE TO PROTECTING YOUR TRADE SECRETS

by

Arthur J. Schwab
David J. Porter
Buchanan Ingersoll

INTRODUCTION

The "New Economy" is a catch phrase describing the efforts of entrepreneurs to supply consumers' insatiable demand for information. The demand was always there, but with the advent of the Internet and other technologies it has been unleashed like never before, creating new and vast opportunities for firms specializing in the creation, storage, management and transmission of information. Technologies facilitate the New Economy, but at bottom the information itself is the lifeblood of this worldwide market.

The most valuable assets of New Economy companies are intangibles such as ideas, know-how, compilations of data and intellectual property rights. The business of New Economy companies essentially consists of managing that information in such a way as to maximize its value. If valuable information is mismanaged — revealed prematurely or disclosed to someone other than the intended audience — its value may be lost to competitors or squandered entirely. Accordingly, maintaining the confidentiality of valuable material is of utmost importance in the information age. In this respect, New Economy firms are no different than traditional businesses that profit by exploiting trade secrets and/or confidential information.

But just as paper gains in a stock portfolio are not realized until the shares are disposed of, the value of trade secrets and confidential information is not realized until it is used or disclosed to others. So, how does a party use trade secrets or confidential information while protecting its value? There are, of course, procedural and technological safeguards against the improper disclosure of such information and each firm should implement those safeguards as a matter of policy. Beyond internal safeguards, legal contracts are the instruments by which parties establish legal rights with respect to the use and flow of information; and the enforcement of contractual terms through litigation or alternative dispute resolution is the means by which businesses protect the value of trade secrets and confidential information.

This monograph summarizes fundamental principles of trade secret law, describes contractual terms that should be used to protect trade secrets and confidential information, and highlights issues typically associated with trade secret litigation.

I.

BASIC PRINCIPLES

A. What is a Trade Secret?

A trade secret is any information, not generally known in one's industry or trade, which provides the business with the opportunity to obtain an advantage over a competitor who does not know or use that information. Specifically, a "trade secret" includes formulas, patterns, compilations, devices, methods, techniques, processes, plans and designs, as well as the application of computer software.

1. Restatement Definition

In 1939, the Restatement (First) of Torts was published and attempted to provide a comprehensive analysis of the trade

secret concepts that had evolved from the common law. Importantly, as further defined in Section 757, comment b of the Restatement, which has been cited and followed in numerous states,[1] the subject matter of a trade secret must be secret. The Restatement identifies some factors to be considered in determining whether given information is one's trade secret:

1. the extent to which the information is known outside his business;

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

3. the extent of measures taken to guard the secrecy of the information;

4. the value of the information to him in developing the information;

5. the amount of effort or money expended by him in developing the information; and

6. the ease or difficulty with which the information could properly be acquired or duplicated by others.

The following types of confidential information have been held, under state law, to be trade secret by various courts under the Restatement definition: customer lists, customer data and information, policy manuals, and pricing information, including codes for determining discounts, rebates, or other concessions in

[1]Various portions of the Restatement and its comments have been cited approvingly in the following jurisdictions: Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Georgia, Illinois, Iowa, Kansas, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Texas, Utah, West Virginia and Wisconsin. *See* Roger M. Milgrim, MILGRIM ON TRADE SECRETS, § 2.01 (Matthew Bender, 1992).

price list or catalogue.[2] It is apparent from the applicable case law that the Restatement's commentary on trade secret law significantly contributed to the analysis and development of modern trade secret laws. One commentator has observed that the Restatement's analysis of trade secret concepts has become so universal that it remains difficult to find a modern judicial opinion concerning trade secret law that does not cite, and heavily rely on, some of the Restatement's rules and comments.

2. Uniform Trade Secrets Act

In 1979, the National Conference of Commissioners on Uniform State Laws approved the Uniform Trade Secrets Act. The Uniform Trade Secrets Act, which has been adopted by over 40

---

[2]*See*, *e.g.*, *Murrco Agency, Inc. v. Ryan*, 800 S.W.2d 600 (Tex. Ct. App. 1991) and *Owens v. Penn Mut. Life Ins. Co.*, 851 F.2d 1053 (8th Cir. 1988) (applying Arkansas law) (customer lists); *Cape Mobile Home Mart, Inc. v. Mobley*, 780 S.W.2d 116 (Mo. Ct. App. 1989) and *Affiliated Paper Cos. v. Hughes*, 667 F. Supp. 1436 (N.D. Ala. 1987) (pricing information); *Morgan's Home Equip. Corp. v. Martucci*, 390 Pa. 618, 136 A.2d 838 (1957) (customer information); and *Union Electric Steel Corp. v. John R. Colosimo, et al.*, C.A. 91-1891 (W.D. Pa. December 11, 1991) (Bloch) (standard practice manuals, customer lists and customer data and information). *Compare BDO Seidman v. Pfizer, Inc.*, 162 A.D. 2d 197, 556 N.Y.S. 2d 322 (1990), and *Southern Ill. Med. Bus. Assocs. v. Camillo*, 190 Ill. App. 3d 664, 546 N.E. 2d 1059 (1989) (clients developed through employee's own effort was not protectable interest of employer); *Moore Bus. Forms, Inc. v. Foppiano*, 181 W. Va. 305, 382 S.E. 2d 499 (1989) (general managerial skills such as supervising, merchandising, purchasing and advertising were not protectable employer interests); *Agra Enters., Inc. v. Brunozzi*, 302 Pa. Super. 166, 448 A.2d 579 (1982) (customer lists that are publicly available are not protectable interest of employer); and *Porter Indus. v. Higgins*, 680 P.2d 1339 (Colo. App. Ct. 1984) (pricing and bidding structure for commercial janitorial services not a "trade secret").

states with some modifications,[3] provides a uniform definition of a Trade Secret:

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

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The following types of confidential information have been held to be a trade secret under the Uniform Trade Secrets Act, as modified by the various states: cost data, customer lists, formulae, processes, methods and techniques, and business information.

A business should not disclose its trade secret any more widely than absolutely necessary. Often, in order to properly recognize its economic value and benefit from its trade secret, a business must necessarily disclose it to certain individuals and/or entities. For example, a business may be required to disclose its trade secrets to investors, suppliers, clients, customers, distributors, consultants or its employees. However, to maintain its legitimate "protectable" interest, a business must take appropriate and

[3]The Uniform Trade Secrets Act, with modifications which vary from state to state, has become law in the following forty states: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Utah, Virginia, Washington, West Virginia, and Wisconsin. *See* Melvin F. Jager, TRADE SECRETS LAW, § 3.05 (Clark Boardman Callaghan, 1996).

complete measures to properly secure the secrecy of its trade secret.

B. How to Protect a Trade Secret? — Maintaining Secrecy and Security of Confidential Information

Before any disclosure is made to employees or third parties, the business must inform the individual and/or entity that the information is confidential and proprietary to the business. Therefore, any confidential and proprietary trade secret must be appropriately labeled "confidential." Further, the business must take appropriate steps to maintain the confidentiality of its trade secrets. In addition to a formal employment agreement with its employees, which will be discussed in greater detail in Section III below, a business has numerous means of increasing the privacy, and protectability, of its trade secret information.

1. General Security Measures

a. External Security Measures

External security measures include controlling all entrances to facilities by guards and/or receptionists and requiring all visitors to sign in. Visitors on group tours should be escorted and excluded from areas where trade secrets are visible. Also, doors to rooms and containers housing trade secrets should be locked and access to those areas should be limited. Warning signs should be placed in areas containing trade secrets notifying employees and visitors that the area is restricted due to the nature of confidential information found within. Although secrecy need not be absolute, security should be such that, except for the use of improper means, one would have difficulty in acquiring the trade secret.

b. Internal Security

Such measures include: (i) limiting access of confidential documents to specifically named individuals who must account for

the purpose and duration of use of the document; (ii) properly handling, routing and destroying confidential documents; (iii) locking desk drawers and cabinets where confidential information is stored; and (iv) requiring that any literature or presentations related to the trade secrets be approved by corporate or outside legal counsel prior to their disclosure to third parties.

Internal security measures must be continuous because trade secret information is subject to protection from the time of its creation but is abruptly terminated when secrecy is breached. Employers must take affirmative steps to maintain secrecy for as long as a trade secret exists. Businesses should also obtain written nondisclosure agreements from vendors, contractors or any third person to whom the employer discloses the trade secrets.

2. Protection Through Applications/Policy Manuals

Initially, employers can incorporate confidentiality and nondisclosure provisions into applications for employment. Also, job descriptions should include a statement that employees will be exposed to confidential information that is proprietary to the owner. Furthermore, all businesses should develop written policies for internal use of trade secrets.

3. Protecting Computer-Related Information

The prominent use of computers to create and store trade secrets raises additional and unique issues which businesses should consider. Often, computer disks, printouts and manuals contain confidential trade secrets; accordingly, such computer-related items must be labeled as confidential, protected and properly stored.

Because computer disks can be copied and misappropriated easily, businesses should protect and restrict access to the computers and computerized trade secrets by requiring passwords or special access numbers before the computer acknowledges entry into the system. Importantly, these passwords

and access numbers should be changed regularly, and a current master list of the passwords and access numbers should be safely stored and kept confidential. Also, "fingerprinted" disks can block access to data by unauthorized users, and "timelocks" on software can be adapted to limit software access to specific time periods during the day. These measures help prevent employees from accessing an employer's computer and making copies of secret information from the employee's home or elsewhere. Businesses should not overlook the importance of establishing and following a procedure to ensure the protection of computer-related material.

Finally, because more and more businesses are transmitting otherwise-confidential information over telephone lines and through cellular phone transmissions, which are vulnerable to misappropriation, businesses should alleviate these potential sources of intrusion into their corporate confidential information by effectively encoding or scrambling the computer-generated trade secrets before transmitting the information.

If a business has a legitimate and protectable trade secret and has taken reasonable steps to maintain the confidentiality of the secret, it should execute agreements with the employees or third parties who receive the otherwise-confidential information during the course of their relationship, employment [or otherwise], not to disclose, divulge or use the business' trade secrets.

C. Agreements Not to Disclose Trade Secrets and Covenants Not to Compete

Agreements not to disclose, divulge or use confidential trade secrets can be implied or expressed. Implied agreements are the result of an employee or third party's fiduciary and common law obligations not to misappropriate or disclose confidential information which was provided to the individual while the individual was employed or in a position of trust and confidence with the business. In order to establish a fiduciary obligation, the business must own the rights to the trade secret and provide the secret to the individual for the exclusive use and benefit of the business. In addition to the implied obligations an employee owes

his or her employer, a business can execute contracts to create expressed obligations to protect its trade secret information.

1. Confidentiality Agreements

Confidentiality agreements should explicitly recite that the employee or third party's duties and obligations to refrain from disclosing, divulging or using any confidential information continue after the relationship ends unless, and until, the information becomes generally known to the industry through proper means.

The most significant protection employers have against misappropriation of trade secrets is the creation of express contractual obligations through covenants not to compete.

2. Covenants Not to Compete

Generally, a covenant not to compete limits a former employee's ability to compete against her or his former employer for a reasonable period of time. Whether governed by statute or common law, most courts have enforced these agreements if they are ancillary to employment, reasonably limited in scope and duration and designed to protect legitimate business interests (in particular, customer goodwill and trade secret and confidential information).

a. Duration

The length of time restriction contained in a covenant should be no greater than is reasonably necessary to protect the employer's legitimate business interests. While the reasonableness of any restriction depends upon the protectable interest involved in each case, many courts have affirmed covenants covering one to three years after the employment ends.

b. Scope

Courts generally consider territorial restrictions in covenants to be reasonable if they are limited to the former

employee's service area. These restrictions do not need to be expressed in geographic terms. Limitations expressed in terms of particular customers serviced by the employee may more closely approximate the employer's actual vulnerability.

c. Consideration

In order for the covenant to be held enforceable, it must be supported by adequate consideration. While each state considers different forms of consideration to be sufficient, most courts have traditionally held that a restrictive covenant is enforceable provided that the agreement is ancillary to employment. Moreover, the majority of states will enforce a restrictive covenant when signed after work began based upon continued employment. However, a minority of states have conversely held that employment can only be adequate consideration when the covenant is entered into before, or simultaneously with, initial employment, or if the agreement is accompanied by a change in employment position or some other additional compensation. Accordingly, in a minority of states, a covenant is unenforceable if it is purportedly entered into after employment begins, because mere continued employment, without more, is inadequate consideration.

Because a trade secret loses its protectability once it is disclosed to the applicable industry, and because the overwhelming majority of trade secret losses occur through departing employees, special security measures must occur when the employment relationship terminates.

D. Post-Employment Considerations

Importantly, the employer should conduct an immediate, informal investigation when employees depart. This investigation must involve an exit interview.

1. Informal Investigation — The Exit Interview

The exit interview has at least three distinct purposes. First, it is a final opportunity to remind the departing employee of

his or her obligation not to disclose, divulge or use the business' confidential trade secrets. Second, it provides a mechanism for the employer to secure the return of any confidential trade secrets from the employee. Third, it permits the employer to informally discover and investigate the circumstances and conditions of the employee's departure from the company. Corporate and/or outside legal counsel should participate in the exit interview.

Also, the entire employment file, consisting of the employee's resume, job application, detailed job description and any and all agreements or documents executed by the person during employment with the company should be thoroughly reviewed with him or her. Importantly, where applicable, the documents which indicate that confidential trade secret information was received while in the company's employ should be reviewed and acknowledged by the departing employee. Any documentation which demonstrates that the individual did not possess such information prior to entering into the relationship should be highlighted to the employee.

It is important for the employer to properly and completely document the results of the exit interview. It is equally as important to have the employee acknowledge the accuracy of the exit interview report.

2. Post-Employment Documentation

a. Statement Executed by Employee

Upon termination of employment, a written statement should be executed acknowledging that the person had access to certain trade secrets and confidential information during employment and that he or she will return all materials, documentation and computerized materials, and all copies thereof, acquired during employment. This statement should also serve as a reminder of the ongoing obligation not to disclose or use trade secrets in new jobs. Moreover, if a covenant not to compete was executed, the written statement should also acknowledge that the employee will continue to strictly abide by those provisions of the

agreement regarding confidentiality, employee inventions, and non-competition after leaving the company.

b. Correspondence to New Employer

If necessary, the previous employer can deliver a letter to the new employer, if known, informing the company of the obligations, contractual or otherwise, to which the employee is bound. Such a letter may substantiate a potential claim against a subsequent employer for, among other things, tortious interference and conspiracy. Accordingly, not only does the former employer increase the likelihood that the terms and conditions of the covenant not to compete and/or confidentiality agreement will be followed, but also validates a potential defendant in the event that the employee nonetheless violates the terms of the agreement(s) while in a new job.

E. Litigation

The pre-filing preparation, as detailed above, is crucial to the success of a trade secret case. Moreover, if, as a result of the pre-filing investigation, the employer has a reasonable basis to believe that an employee has misappropriated or misused the company's trade secret, the company must make a rapid decision whether to litigate. A number of factors must be considered when deciding whether to institute a trade secret case. Initially, filing suit significantly increases the likelihood that the trade secret will be further exposed during the course of the litigation. This consideration, however, can be significantly controlled through the use of confidentiality agreements and/or protective orders.

Starting litigation also may enhance the company's reputation, among employees and competitors, that it will vigorously enforce its rights to protect its confidential and proprietary trade secret information and that theft or misuse of such information will not be tolerated. Once a decision to litigate has been made, the company must consider a wide array of causes of action which may be available in a trade secret case.

1. Potential Causes of Action

Causes of action in a trade secret case may include misappropriation, breach of contract, breach of fiduciary duty, tortious interference with business relations, tortious interference with contract, unfair competition, unfair trade practice, conspiracy and violation of State or Uniform Trade Secrets Act. Generally, in a trade secret action, the plaintiff should consider suing the misappropriator of the trade secret, as well as the subsequent employer and those who used the information.

2. Discovery

Discovery in a trade secret case must be rapid and precise. Initially, upon beginning the action, the plaintiff should seek a court order compelling limited, necessary discovery, including oral depositions, as well as written discovery. Such expedited discovery requests should be filed simultaneously with the filing of the complaint, and should be tailored and limited to the issues presented in the preliminary injunctive motion. Moreover, the plaintiff should seek an order of court preserving the integrity of documents which may be relevant. A request for immediate, expedited discovery can impress upon the court the urgency of the pending matter, as well as the threat of irreparable harm, which may assist in the issuance of a preliminary injunction.

Almost without exception, obtaining early access to the documents proves to be invaluable to the preparation for the preliminary hearing. Beyond finding copies of plaintiff's secret material in the defendant's possession, documents may be discovered which reflect that the defendant did not independently develop the trade secret information.

3. Injunctive Relief

Injunctive relief is the cornerstone of a trade secret case. Significantly, because a trade secret may be lost once it is disclosed or divulged to the applicable industry, injunctive protection attempts to arrest improper disclosure or further misappropriation of the trade secret.

After the action has been commenced by a verified complaint, the plaintiff may seek injunctive relief through a motion for a temporary restraining order and/or preliminary injunction to stop the misuse and/or misappropriation of the trade secret. A temporary restraining order is used to preserve the status quo for a brief time. A preliminary injunction order is intended to preserve the status quo pending final resolution of the dispute. Importantly, success at the preliminary injunction stage is tantamount to final judgment because the matter is often settled at the conclusion of the preliminary injunction hearing.

In order to obtain a preliminary injunction, the majority of courts require that the plaintiff demonstrate: (1) a reasonable likelihood of success on the merits; (2) that the plaintiff will be irreparably harmed by denial of such relief; (3) the balance of the equities weight in favor of granting preliminary relief; and (4) the preliminary relief is in the public interest.

Ultimately, however, it is critical to draft a comprehensive, yet enforceable, prayer for relief, as well as a proposed order of court granting plaintiff's motion for a temporary restraining order and/or preliminary injunction. Also, because most courts are required to provide a statement of reason why a preliminary injunction was granted, the plaintiff should prepare detailed, and cross-referenced, proposed findings of fact and conclusions of law to facilitate the issuance of the preliminary injunction.

4. Damages

In addition to the significant injunctive relief available to a plaintiff, the court may award monetary damages, reasonable royalties and possibly punitive damages and attorneys' fees. Damages may consist of lost profits, loss of value of the trade secret, cost of developing the trade secret or the cost of remedying the misconduct.

In today's business environment, corporations must address and resolve a plethora of trade secret issues. The following chapters will address many of the issues that were preliminarily discussed in this introduction.

II.

WHAT IS A TRADE SECRET?

A trade secret is any information not generally known in an industry which provides that trade or industry with an advantage over competitors who do not know or use that particular information. Examples of trade secrets that have been protected by the courts are chemical formulas; methods of treating chemicals; methods of doing business, such as the concept for disseminating certain stock quotations; customer lists; credit ratings; recipes; blueprints; architectural plans; designs; marketing and development analyses and plans; new product developments; advertising slogans; and tables of data, such as cost data.

A. Uniform Trade Secrets Act

The most significant national development in trade secrets law is the adoption — by 41 states — of the Uniform Trade Secrets Act (UTSA).[4] The UTSA codifies the common law of trade secret protection. It was first approved by the National Conference of Commissioners on Uniform State Laws on August 9, 1979. Thereafter, on August 8, 1985, four clarifying amendments were approved and also recommended for enactment.

The UTSA provides protection only for "trade secrets." Section 1(4) of the UTSA provides that:

> "Trade Secret" means information, including a formula, pattern, compilation, program, device, method, technique or process, that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

[4] *See* Appendix A, *infra*, for a reference list of these state laws.

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Many of the states that have adopted the UTSA have modified the Act's definition of "trade secret." Illinois, Maine, Virginia and West Virginia, have merely prefaced the listing in the initial paragraph with the phrase "including, but not limited to." In Washington, the Act applies "unless the context clearly requires otherwise." The most common additions made in other states include customer lists (Colorado, Connecticut, Illinois and Oregon), computer data (Montana and Idaho) and drawings (Connecticut and Illinois).

B. Section 757 of the First Restatement of Torts

Those states that have not adopted the UTSA have generally embraced the definition of trade secrets embodied in the RESTATEMENT (FIRST) OF TORTS, Section 757 (1939), and rely upon it to determine whether trade secrets exist. The courts that rely on the Restatement's definition note that there is no precise definition of trade secrets, but nevertheless, courts traditionally look to the six factors listed in Comment b of the Restatement for guidance in determining whether a trade secret exists. *See*, *e.g.*, *Ashland Management Inc. v. C. Christopher Janien*, 624 N.E.2d 1007 (N.Y. 1993); *Colson Co. v. Wittel*, 569 N.E.2d 1082 (Ill. App. Ct. 1991); *Chmura v. Deegan*, 581 A.2d 592 (Pa. Super. Ct. 1990).

Comment b to Section 757 provides that some of the factors to be considered in determining whether information is one's trade secret include:

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

2) The extent to which it is known by the employees and other involved in his business;

3) The extent of the measures taken by him in regard to secrecy of the information;

4) The value of the information to him and to his competitors;

5) The amount of effort or money expended by him in developing the information; and

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

Some courts even go so far as to acknowledge that the Restatement's definition of trade secrets is the "most widely accepted" or "most commonly used" definition. *See Concept, Inc. v. Thermotemp, Inc.*, 553 So. 2d 1325 (Fla. Dist. Ct. App. 1989). Indeed, the Court of Appeals for the District of Columbia has stated that trade secrets were "authoritatively defined" by the Restatement. *Ruesch v. Ruesch Int'l Monetary Serv., Inc.*, 479 A.2d 295 (D.C. 1984).

The Restatement's factors are still followed by some jurisdictions even after adoption of the UTSA. *See*, *e.g.*, *Network Telecommunications, Inc. v. Boor-Crepeau*, 790 P.2d 901 (Colo. Ct. App. 1990).

C. The Economic Espionage Act, 18 U.S.C. §§ 1831-1839

The Economic Espionage Act (EEA) became law in October of 1996. The statute criminalizes the misappropriation of trade secrets. The EEA generally followed and expanded on the Uniform Trade Secrets Act's definition of a trade secret. Section 1831 of the EEA makes it a crime for an individual or an organization to wrongly obtain a trade secret from its owner knowing that the offense will benefit in any way a foreign government or an organization substantially controlled by any foreign government. Section 1832 of the EEA also criminalizes the intentional theft of trade secrets, but is applicable where the theft is not intended as economic espionage for the benefit of a foreign government. The EEA's criminal penalties can be a combination of imprisonment and fines. Under Section 1831,

individuals can be jailed for up to 15 years and fined up to $500,000; organizations can receive up to $10,000,000 in fines. Under Section 1832, an individual can be sentenced for up to 10 years and fined; organizations may be fined up to $5,000,000. In addition, the EEA provides for forfeitures of the proceeds derived from the crime, and to some degree, the offender's private property used to commit the crime.

The EEA regulates conduct outside the United States so long as the offender is either a United States citizen or a permanent resident. It also permits prosecutors to seek civil injunctions before the commencement of the criminal prosecutions to protect trade secrets. The EEA does not preempt other remedies available under state trade secret laws, whether criminal or civil.

D. Requirements of Confidentiality and Economic Value

1. Information Must Be Kept Sufficiently Confidential

The general rule is that an employer must make "reasonable efforts" to preserve the confidentiality of information for it to be eligible for trade secret protection. *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890 (Minn. 1983) (reasonable efforts to maintain secrecy involve combination of physical security and confidentiality procedures that signal the secret nature of the information). *See also Northwest Airlines v. American Airlines*, 853 F. Supp. 1110, 1115 (D. Minn. 1994) (intention to keep information confidential is insufficient basis for trade secret protection; owner must take reasonable measures to guard secret).

In *Amex Distrib. Co. v. Mascari*, 724 P.2d 596, 602 (Ariz. 1986), the court held that knowledge of particular customers could be protected if "truly confidential, and to a substantial degree inaccessible." The court in *Sheets v. Yamaha Motors Corp. U.S.A.*, 657 F. Supp. 319 (E.D. La. 1987), *aff'd in part, rem'd in part*, 849 F.2d 179 (5th Cir. 1988), held that trade secret protection will be extended only if the plaintiff took reasonable efforts to preserve the

secrecy of the alleged information. *See also Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d. 890, 902 (Minn. 1983) (where the court found that the company did not have trade secret because the company did not take enough steps to secure secrecy).

An example where confidential measures were taken is *Peggy Lawton Kitchens, Inc. v. Hogan*, 466 N.E.2d 138 (Mass. App. Ct. 1984). In *Peggy Lawton Kitchens*, the court upheld the trial court's judgment in favor of a food company that sought to stop a former employee from marketing chocolate chip cookies from a secret recipe that the company claimed to be its own. The court noted that since the company stowed its "ingredient cards" in a safe, and the former employee had to develop a strategy to examine the cards, the company used reasonable efforts to secure the confidentiality of the recipe.

Additionally, an employer must be careful to not destroy trade secret protection by inadvertently disclosing the information, especially to third parties, such as customers. Such disclosure can occur through lobby displays, publications, plant tours and insufficient limitations on visitors, failure to identify information, or failure to guard the information's confidentiality.

Trade secret protection was lost through disclosure to customers in *Palin Mfg. Co. v. Water Tech., Inc.*, 431 N.E.2d 1310 (Ill. App. Ct. 1982). In this case, a plaintiff attempted to protect its plans and information concerning paint sludge separation and removal equipment that it installed at a customer's plant. In denying protection, the court said that since the plaintiff provided the drawings of the information, and never told the customer that they were confidential, it was not entitled to trade secret protection. Moreover, the court noted that the customer plant, where the equipment was installed, hosted public tours and was frequently visited by many contractors and former employees.

2. Information Must Derive Economic Value

The information must have economic value in order to be afforded trade secret protection. *See Johns-Manville Corp. v.*

Guardian Indus. Corp., 586 F. Supp. 1034 (E.D. Mich. 1983), *aff'd*, 770 F.2d 178 (Fed. Cir. 1985). In *Johns-Manville Corp.*, the court stated that whether information is protectable depends on the amount of labor and money expended in developing the information. Specifically, the court stated that there must be "sufficient money and time . . . expended . . . to make it 'worthy of court protection.'" *Id*. at 1069-70 (citation omitted). Because the Johns-Manville Corporation had expended more than 150 man-years and $9 million on developing a new fiberglass process, the court determined that "adequate time and money had been expended," and thus granted protection. *Id*. at 1070. *See also*, *Christopher M. Hand's Poured Fudge, Inc. v. Hennon*, 1997 WL 50955 (Super. Ct. Pa. 1997) (where the court observed the value of the information to the owner and competitors and the amount of money or effort spent in developing the secret are factors used to determine whether information will be deemed a trade secret).

Similarly, in *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890 (Minn. 1983), the court analyzed the requirement of "deriving economic value," and stated that competitive advantage may be part of the plaintiff's expense in developing information that is protectable as a trade secret. However, some courts have held that when a competitive advantage exists only if a competitor uses a company's marketing strategy to underbid the company, protection may be denied. *See, e.g.*, *Optic Graphics Inc. v. Agee*, 591 A.2d 578, 587 (Md. Ct. Spec. App.), *cert. denied*, 598 A.2d 465 (Md. 1991).

E. Information That Has Been Afforded Trade Secret Protection

1. Scientific Information

Courts have long recognized that scientific data, including confidential information about machines and devices, chemical processes, and manufacturing methods, may be entitled to trade secret protection. Some examples where courts protected scientific information include: *Henry Hope X-Ray Prods. Inc. v. Marron Carrel, Inc.*, 674 F.2d 1336 (9th Cir. 1982) (machines and devices

relating to film processors); *Felmlee v. Lockett*, 351 A.2d 273 (Pa. 1976) (chemical formulas used to manufacture soft plastic fishing lures); *Syntex Opthalmics, Inc. v. Novicky*, 745 F.2d 1423 (Fed. Cir. 1984), *vacated on other grounds*, 470 U.S. 1047 (1985) (chemical processes and ingredient information used to manufacture contact lens materials); *Ferroline Corp. v. General Analine & Film Corp.*, 207 F.2d 912 (7th Cir. 1953), *cert. denied*, 347 U.S. 953 (1954) (chemical process to manufacture iron pentacarbonyl); and *Surgider Corp. v. Eye Tech., Inc.*, 648 F. Supp. 661 (D. Minn. 1986), *aff'd*, 828 F.2d 452 (8th Cir. 1987) (manufacturing methods used to make medical devices implanted by ophthalmologists to correct vision loss caused by cataracts).

As with all protectable information, employers must make reasonable efforts to maintain secrecy. If a company fails to take reasonable efforts to maintain secrecy, the information's otherwise protectable status may be destroyed. For example, failing to follow internal security procedures, publishing papers in scientific journals, and supplying the government with information relating to a scientific process was enough to destroy trade secret protection for a company in *CVD, Inc. v. Raytheon Co.*, 769 F.2d 842, 851-54 (1st Cir. 1985), *cert. denied*, 475 U.S. 1016 (1986).

Similarly, where manufacturing methods for chrome plating were known and used by other businesses in the chrome plating industry, trade secret production was denied for the alleged secret plating process. *Nickelson v. General Motors Corp.*, 361 F.2d 196 (7th Cir. 1966). *See also Weins v. Sporleder*, 1997 WL 539501 Nos. 19307, 19308, 19310 and 19315 (S.D. 1997).

2. Computer Information

While trade secret protection for computer software programs was questionable in the early years of computers, today the law is well established. Indeed, many state statutes and cases include computer programs within the definition of a trade secret. For example, Idaho has expanded the model UTSA statutory language to specifically include computer programs. Idaho Code 48-801 defines a "computer program" as:

> Information used by a computer to perform logical operations which
>
> (i) is contained in any media or format,
>
> (ii) is capable of being programmed into a computer, either directly or indirectly, and
>
> (iii) prominently displays a notice of copyright or other proprietary interest.

Computer software programs are routinely held to be protectable as a trade secret provided that the "secret" is not generally known and that reasonable efforts to maintain its confidentiality are followed. *Cybertek Computer Prods. Inc. v. Whitfield*, 203 U.S.P.Q. 1020 (Cal. 1977). Restrictive confidentiality agreements used in both the employer-employee and business-customer relationships have been routinely held to be a reasonable effort to protect confidentiality. Some jurisdictions have held that a confidentiality notice on documents and computer disks is sufficient to obtain protection. Other courts, however, have not protected computer information where the computer program at issue was not specifically mentioned in the employee's nondisclosure agreement. *See Aries Info. Sys., Inc. v. Pacific Management Sys. Corp.*, 366 N.W.2d 366 (Minn. App. Ct. 1985).

Additionally, courts have routinely enjoined former employees from using a former employer's confidential computer information and trade secrets. *See Alexander & Alexander Benefit Serv., Inc. v. Benefit Brokers & Consultants, Inc.*, 756 F. Supp. 1408 (D. Or. 1991) (Even in the absence of written agreements, the court enjoined four individuals and their new business from using the plaintiff's confidential information and soliciting any of plaintiff's customers finding that the defendants had breached their fiduciary duties to plaintiff and misappropriated its confidential information while still in plaintiff's employ); *LCI Communications, Inc., v. Buonaiuto*, No. C-2-88-1301, 1989 U.S. Dist. LEXIS 18296 (S.D. Ohio 1989) (Court enjoined three individuals from making use of their former employer's technology in the long distance telecommunications industry, including copyrighted software

programs and databases, and prohibited the former employees for a period of one year from engaging in any competing business and soliciting customers in a seven state region); *LCI Communications, Inc. v. Wilson*, 700 F. Supp. 1390 (W.D. Pa. 1988) (Court permanently enjoined a former salesperson of the plaintiff from using confidential information and trade secrets and engaging in a competing business or soliciting customers for one year in the area he had serviced for plaintiff. Further, the salesperson was enjoined from enticing plaintiff's employees to leave plaintiff's employ); *Healthcare Affiliated Servs. v. Lippany*, 701 F. Supp. 1142 (W.D. Pa. 1988) (Court enjoined a former employee from using plaintiffs' methodologies and copyrighted software, developing similar software, and soliciting plaintiffs' customers, and directed the employee to return software developed while in plaintiffs' employ).

3. Business Information

Courts have found that business and strategic plans, pricing and credit policies, marketing plans, financial information, customer lists, and compilations are entitled to trade secret protection.

a. Business and Strategic Plans

For business plans to be protected, they must contain a sufficient degree of particularity. In *AMP, Inc. v. Fleischhacker*, 823 F.2d 1199, 1203-04 (7th Cir. 1987), the court refused to protect business and strategic plans because the plaintiff sought protection of a long list of general business information instead of specifically identifying what particular trade secrets it sought to protect.

b. Pricing and Credit Policies

In theory, pricing or credit policies are protectable under the UTSA. However, in reality, companies attempting to obtain protection face many obstacles. One particular obstacle is reaching a balance between general and specific information.

For example, courts have refused to protect pricing data which is so specific to the manufacturer that the information has no independent economic value. *See Optic Graphics, Inc. v. Agee*, 591 A.2d 578, 586 (Md. Ct. Spec. App.), *cert. denied*, 598 A.2d 465 (Md. 1991). On the other hand, when the pricing information is readily available through means other than misappropriation, it has been held to be "too general" and not entitled to protection. *Cosmos Forms, Ltd. v. American Computer Forms, Inc.*, 596 N.Y.S.2d 862 (N.Y. App. Div. 1993).

Another potential obstacle is the daily, weekly or monthly fluctuations in price changes. These changes make it difficult for a business to assert that its information has independent economic value at particular times. *Schlumberger Well Servs. v. Blaker*, 623 F. Supp. 1310, 1316 (S.D. Ind. 1985), *aff'd*, 859 F.2d 512 (7th Cir. 1988).

c. Marketing Plans

Marketing plans must contain unique information to be protected. Accordingly, if a marketing plan merely uses information readily available in the marketplace, it is not protectable. *See Jillian's Billiard v. Beloff Billiards, Inc.*, 619 N.E.2d 635, 638 (Mass. App. Ct. 1993); *Fleming v. Ray-Suzuki, Inc.*, 275 Cal. Rptr. 150 (Cal. Ct. App. 1990).

d. Financial Information

Financial information must be sufficiently particular to be protected as a trade secret. Although a business must assert what particular form of financial information to protect, the courts will grant protection to very broad categories of information. These include gross sales figures, revenue reports and accounting procedures. *Augat, Inc. v. Aegis, Inc.*, 565 N.E.2d 415, 418 (Mass. 1991); *Jillian's Billiard v. Beloff Billiards, Inc.*, 619 N.E.2d 635, 639 (Mass. App. Ct. 1993); *Centrol v. Morrow*, 489 N.W.2d 890, 894-95 (S.D. 1992).

In addition to common law protection of corporate financial information, some states have added financial

information as a category of information that is expressly protected by their version of the UTSA. For example, Colorado's statute covers "confidential business or financial information," and Connecticut's and Iowa's statutes cover "cost data."

e. Customer Lists

Whether information contained in a customer list or other compilation is a protectable trade secret depends on whether such information is held in confidence, and whether it can be readily obtained by a competitor through legitimate means. Accordingly, a business should take precautions, such as confidentiality measures, to increase the likelihood that its customer lists are protectable trade secrets.

In *Templeton v. Creative Boating Tampa, Inc.*, 552 So. 2d 288 (Fla. Dist. Ct. App. 1989), the Court refused to protect a list of potential advertisers for a magazine because anyone could discover their identity by merely looking at advertisements in past issues of the magazine. The court held in *Western Med. Consultants, Inc. v. Johnson*, 80 F.3d 1331, 1337 (9th Cir. 1996), that the defendant did not use her former employer's trade secrets to start her own business because the information was gathered from "generally known and accessible sources." The court in *ABBA Rubber Co. v. Seaquist*, 286 Cal. Rptr. 518, 527 (Cal. Ct. App. 1991), held that a list of companies in an industry known to use certain products did not have value to that product's manufacturers, and thus, was not protectable. However, the court noted that if the list would have identified only those companies that actually purchased the product, then it would be valuable to the product's manufacturers, for they would know which companies made purchases in the past.

In *Unistar Corp. v. Child*, 415 So. 2d 733 (Fla. Dist. Ct. App. 1982), the court held that a customer list, which was the result of the company's extensive work, considerable effort, knowledge, time and expense, was entitled to protection. *See also Network Telecomms., Inc. v. Boor-Crepeau*, 790 P.2d 901 (Colo. Ct. App. 1990) (list of telephone service customers that was compiled at considerable expense and over a great deal of time was protectable).

A business must also realize that although a customer list may be protected, not all of the individual names on the list are always protected. *Moss, Adams & Co. v. Shilling*, 224 Cal. Rptr. 456, 458-59 (Cal. Ct. App. 1986). In *Moss*, the court stated that "[o]ne may do business with a former employer's customers with whom one became personally acquainted and developed a business relationship while formerly employed." Thus, while the customer list may be a trade secret, a company may not be able to prevent former employees from soliciting business from clients with whom they had personal contact during their employment. *But see Morlife, Inc. v. Perry*, 66 Cal. Rptr. 2d 731, 738 (Cal. Ct. App. 1997), which found "that the distinction *Moss, Adams* makes between former employees who personally dealt with customers and former employees who did not, rests on an unsound premise."

Conversely, in *American Credit Indem. Co. v. Sacks*, 262 Cal. Rptr. 92, 98 (Cal. Ct. App. 1989), the court ruled that "the right to announce a new affiliation, even to trade secret clients of a former employer, is basic to an individual's right to engage in fair competition." Thus, the court recognized that although American Credit's customer list was protectable, former employees could use the list only to announce their new affiliation, but not to solicit business.

f. Compilations of Information

The area of compilations of information is a fact-intensive area of trade secret litigation. A strong argument can be made that compiling a list of information from publicly available sources constitutes a protectable trade secret, provided that the employer generates such a compilation from an expenditure of significant time and expense. *See generally MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); *California Intelligence Bureau v. Cunningham*, 188 P.2d 303, 306-07 (Cal. Ct. App. 1948).

4. An Employee's General Skill and Knowledge

An employee's general skill and knowledge do not constitute a protectable trade secret of an employer. However, where more specific knowledge, such as highly technical information obtained solely through employment is involved, protection may be extended. The ambiguous line between an employee's general skill and knowledge and an employer's proprietary information has led to many disputes in court.

One gray area is when a company conducts its own scientific research and development. *Ingersoll-Rand Co. v. Ciavatta*, 542 A.2d 879, 887 (N.J. 1988). Where businesses encourage and fund research and development, courts have held that the businesses have a protectable interest, albeit narrow, in "highly specialized, current information, not generally known in the industry, created and stimulated by the research environment furnished by the employer, to which the employee has been 'exposed' and 'enriched' solely due to his employment." *Id*.

III.

COVENANTS NOT TO COMPETE IN THE EMPLOYMENT CONTEXT

Almost every employer can benefit from covenants not to compete in the conduct of its business. Although often thought of as offering protection against the theft of trade secrets, covenants not to compete can shield employers from the unfair loss of any competitive advantage held in the marketplace. Just as a computer programmer's skills and knowledge may be invaluable to an employer, so is a salesperson's experience and know-how developed as a result of the employer's investment in training, education, and sharing valuable customer information. Both of these types of employees should be restrained in their ability to use

or abuse their employers' confidential information, trade secrets, and customer goodwill after their employment has terminated.

A covenant not to compete is a contract. It is a promise of the employee to refrain from post-employment use or disclosure of protectable information that the employee has acquired during the term of employment. Covenants may also include provisions prohibiting the employee from engaging in competitive activity or contacting any of the employer's customers, and it usually includes specific confidentiality requirements.

Just as any other contract under the law, a covenant must satisfy certain criteria in order to be valid. The standards for enforceability of covenants differ from state to state, and an employer should be keen to the specifically relevant standards in drafting and enforcing its covenants.[5]

A. Initial Considerations

In contemplating covenants not to compete, an employer's first consideration should be whether the nature of its business and employees warrants post-employment restrictions on unfair competition. Although almost all organizations rely to some extent on confidential information for their competitive advantage in the marketplace, other business considerations may militate against using covenants. For example, in some instances, appropriately trained or experienced employees are hard to come by, and they may wield enough bargaining power to refuse to sign a covenant. In that situation, the employer may determine that it is more important to recruit well-qualified employees than to guard against post-employment competition; perhaps the employer will feel confident in its ability to keep the best employees once they have been recruited. In those instances, it may make good business sense not to require that employees enter into covenants not to

[5]For a comprehensive, nationwide overview of covenants not to compete, *see* COVENANTS NOT TO COMPETE, A STATE-BY-STATE SURVEY, (Brian M. Malsberger et al, eds.) (American Bar Association, 2d ed. 1996 & Supp. 2000).

compete because it is more important to get good employees in the door.

A second important initial consideration is what levels or categories of employees should be required to enter into the covenants. Whenever an employer tries to enforce a covenant in court, it must be prepared to convince a judge that the agreement was necessary to safeguard critical confidential information of the employer. If the employer requires that *every* employee, including support staff, sign the same agreement, it will be difficult to convince any tribunal that the agreement was narrowly tailored and judiciously implemented. Thus, it is advisable that the employer require only those employees with access to confidential information and with ability to cause competitive harm to sign restrictive covenants.

It is important to note that some states prohibit or limit the enforceability of covenants not to compete in the employment context. By contrast, a covenant that is part of the sale of a business is often measured against standards somewhat less stringent than those that govern the employment-related covenant.

Finally, an employer should be aware that the manner in which an employee's services terminate — such as by voluntary resignation or involuntary termination — might affect the enforceability of the covenant.

B. Validity of Covenants Not to Compete

The general criteria governing the validity of covenants not to compete vary from state to state, but most jurisdictions point to a combination of several factors:

(i) Does the employer have a protectable interest and is the restriction that is imposed by the covenant reasonably related to that interest?

(ii) Is the restriction reasonable in time and geographic limitations?

(iii) Does the restriction impose an undue hardship on the employee?

(iv) Is the restriction ancillary to employment, or, is it necessary that the employer grant something of value to the employee in exchange for the employee's promise to abide by the covenant, known in legal terms as "consideration"?

1. How the Protectable Interest and Restriction Relate

The objective of a covenant not to compete is to guard against a former employee's threat to a legitimate protectable business interest. In drafting the covenant, therefore, the employer should first ask itself: what interest am I seeking to protect? The employer must be able to identify the particular concern it seeks to protect because a court is unlikely to define or search for the protectable interest at issue on behalf of the employer. Protectable interests generally include the employer's economic interests, goodwill, and its interest in protecting business secrets disclosed to employees in the course of their employment. A protectable interest can be something tangible, such as a customer list, a patient list, pricing information, a computer program, or a unique formula, or it can be something intangible, such as customer goodwill and client relations. For example, although salespeople often are not the employees who create the employer's products, they are often required to sign restrictive covenants because they are the embodiment of the employer's goodwill with clients. When a salesperson leaves an employer and affiliates with a competing business, the former employer is left exceedingly vulnerable to losing clients because a client's relationship with the employer is its relationship with the salesperson.

At the same time, the technical employees who create the employer's products are most often privy to an employer's trade secrets. These employees can obviously harm an employer by taking their know-how and training to a competitor. Restricting their post-employment competition for a reasonable duration enables the former employer to safeguard its position in the

marketplace both by foreclosing competitors' abilities to garner information from that employee and by hiring and training a replacement by the time the former employee is free to compete.

Not only must the employer be able to define the protectable interest it is trying to protect by the restrictive covenant, but it must also demonstrate that the restriction imposed is necessary and effective in achieving the protection sought. Thus, the restrictive covenant must be carefully tailored to restrict only those post-employment activities that would endanger the employer's competitive advantage while permitting the former employee to use his general skills and knowledge to earn a living. This may take the form of nonsolicitation clauses for salespeople or non-competition clauses in certain industries for technical employees.

2. Is the Restriction Reasonable in Time and Geographic Limitations?

States almost invariably require that covenants not to compete contain reasonable time limitations and geographic scope (defined by territory or specific customers). For example, a restrictive covenant that prohibits an employee from working for any competitor in the country for a period of five years is likely to be found invalid unless tied to a limited product line. These analyses are very fact-specific, however, and depend on the nature of the business and the employee's skills and secrets. Most states also allow courts to modify covenants which contain unreasonable time and/or geographic limitations, rather than simply invalidating them.

Certainly the shorter a time restriction in a covenant not to compete the more likely a court will enforce it. Many restrictive covenants run for one to two years, and courts often enforce these time frames without modification. It is helpful to link the term of the covenant to the time necessary to obviate the potential damage caused by the former employee. If the duration is so defined, courts are more likely to enforce the covenant as written because they will understand the necessity of the time frame.

A longer covenant may be necessary in cases in which the employee's technical skills are such that an employer could not hire and train a replacement in less than two or three years. As another example, a commercial real estate broker's covenant might run as long as a standard lease term. That way, a new broker can establish the necessary client relationship in order to renew the lease without competition from the former employee.

Balanced with the time limitation is the geographic restrictions: does the covenant restrict activity within a reasonable distance, county, state, or territory? Specificity in the geographic limitation will lend weight to the overall validity of the covenant. Most states do recognize that a geographic limitation often serves no purpose, particularly for firms who conduct business nationally or internationally. Thus, courts enforce many restrictive covenants where limitations are defined in other terms, such as by certain customers whom the employee is prohibited from soliciting or certain competitors whom the employee is prohibited from serving for a defined period of time.

As with the time restriction, business realities should be the base of geographic limitation. For example, if the competition to be restrained is based on a customer or patient base, it makes sense to define the geographic parameters of the covenant according to the location of the customers. In a highly specialized physician's practice, for example, patients may actually draw from a 200-mile radius; therefore, a 200-mile competition restriction makes sense as a geographic limitation.[6] For a general medical practice, by contrast, patients may come only from a ten-mile radius. In that case, the covenant should restrict competition only in that ten-mile radius. In general, courts will enforce geographic restrictions that are supported by business realities.

[6]Medical employers should be aware that some states prohibit the enforcement of covenants not to compete as against healthcare providers due to the public policy protecting patients' rights to choose any physician at any time.

3. Undue Hardship on the Employee

The basic premise that an employer must overcome in seeking to enforce a covenant not to compete is, simply, the right of a former employee to earn a living. Courts closely scrutinize employment-related covenants not to compete precisely because their effect is to squelch the employee's ability to use his or her talents and skills. The employer who seeks to enforce a covenant often enters the courtroom with "two strikes against him." The employer faces questions such as, "What standing do you have to prevent a former employee from using his or her skills?"; or, "How can you prevent a former employee from dealing with certain customers when such dealings are the customer's desires?"

These questions ultimately turn on the employer's protectable interest. The employer must demonstrate that its protectable interest is legitimate and capable of definition, and that it drafted the covenant as narrowly as possible to protect only that interest and not to punish an employee for leaving his or her job.

For example, chemists can be precluded from post-employment use of special formulae that they developed or used during their employment. However, they generally cannot be prohibited from competing in the field of chemistry altogether. Difficult questions often arise when that chemist seeks to develop a competing but closely related formula.

As another example, a New Jersey court refused to enforce a covenant not to compete against a salesperson because the hardship resulting to the employee was unreasonable.[7] The covenant prohibited the employee from competing for a period of three years "within the existing marketing area of the Employer, or any future marketing area of the Employer begun during the employment under the terms of this agreement . . . ." Relevant facts in this case included the employee's 25 years of experience in the industry, his network of contacts established prior to his employment with the employer, and the employee's status as "little

---

[7] *Coskey's Television & Radio Sales and Serv. v. Foti*, 602 A.2d 789 (N.J. Super. A.D. 1992).

more than a highly-paid indentured servant" as a result of the enforcement of the covenant. *See also Subcarrier Communications, Inc. v. Day*, 691 A.2d 876, 881 (N.J. Super. Ct. App. Div. 1997), *citing Coskey's Television & Radio Sales*, 602 A.2d at 789.

Once again, the overarching concern of courts is that the restrictive covenant serves only to protect the employer's legitimate competitive advantage. If an unnecessary corollary is an undue hardship to the employee, courts will not enforce the covenant as written.

4. Consideration in Exchange for the Covenant

Just as with any contract under the law, covenants not to compete must be supported by consideration. The employer must give the employee something to which he or she was not already entitled in exchange for the promise to abide by the restriction on competition. The form of consideration may vary.

In almost all states where restrictive covenants are enforceable, if the covenant is signed at the inception of employment or at the time of a beneficial change in employment status, the covenant is supported by the consideration of employment or enhanced employment. In some states (*e.g.*, New Jersey, Delaware, Florida, Georgia, Illinois, Massachusetts, and New York), continued employment, in and of itself, constitutes sufficient consideration for the signing of a covenant. Courts in these states have determined that, due to the at-will nature of the employee's employment, the fact that the employer allows employment to continue is the same as providing a benefit to the employee. Some of those states require that employment continue for a "sufficient" period of time beyond the signing of the covenant, although "sufficient" is not uniformly defined.

In states in which continued employment does not constitute sufficient consideration (*e.g.*, Pennsylvania, Connecticut and North Carolina), employers must bestow some specific benefit upon the employee in return for the execution of the restrictive

covenant. Often significant monetary consideration will suffice. Many employers, however, prefer to use non-monetary consideration. Eligibility for stock options, eligibility for pension benefits, eligibility for bonuses, eligibility for a severance package, and eligibility for enhanced commissions have been deemed sufficient consideration by various courts. Additionally, courts have held that gaining an ownership interest in the employer's business constitutes sufficient consideration. A change in an employee's status from, for example, part-time to full-time or from at-will to employment for a definite duration may be good consideration. Some employers have also taken the position that a change in an employee's job duties which entails greater access to confidential information, although no more compensation or benefits, constitutes sufficient consideration.

As is obvious from these examples, consideration can take many forms. The critical component to sufficient consideration is that the employee gain some real or tangible benefit. Illusory promises on the part of an employer will not support a covenant not to compete.

C. Miscellaneous Drafting Considerations

In some states, if a covenant not to compete includes a liquidated damages clause, the employer will not be entitled to injunctive relief in the enforcement of the covenant. In other words, if the agreement contains a clause which sets a specific amount of money an employee will have to pay if he or she breaches the covenant, the employer will not be entitled to ask a court to order that the employee abide by the terms of the agreement. The employer will be entitled only to receive the liquidated damages. Because injunctive relief is often the most effective type of relief in these cases, employers should be careful to avoid this trap in drafting their restrictive covenants.

Also, in some states, restrictive covenants are not enforceable in cases in which the employee's employment ends through no fault of his own. The covenant remains in effect only if the employee chooses to leave his job. In those states, employers

should simply know that they will not be entitled to the protection of the covenant if they choose to fire the employee.

Finally, all restrictive covenants should identify which state's law will govern interpretation and enforcement of the contract. Because each state's law differs, employers may draft a covenant which will pass muster in, for example, New York, but which will be struck down in Pennsylvania. Employers should choose the law of a state with which they have some connection and draft all covenants in the context of that state's laws.

IV.

POST-EMPLOYMENT CONSIDERATIONS: HOW TO PREVENT THE LOSS OF TRADE SECRETS AND CUSTOMERS

Post-employment considerations are an important component in the overall strategy for protecting trade secrets and confidential information. Because the overwhelming majority of trade secret misappropriation and loss of customers occurs when an employment relationship between an employer and employee is terminated, the need for developing effective procedures for maintaining the secrecy of company trade secrets and preventing the movement of business is critical.

Post-employment procedures are often the last opportunity the employer has to ensure the protection of valuable information. Following clear post-employment procedures may also be helpful to prevent the unauthorized use of trade secrets by the departing employee and unauthorized solicitation of the employer's customers.

The exit interview for departing employees, including employees who depart voluntarily or involuntarily, is frequently an optimal time to discuss each employee's continuing obligations to

the employer. Suggested methods are therefore provided for conducting such interviews, in addition to the potential pitfalls to avoid. An exit interview checklist and an employee acknowledgment form are also provided.

One of the purposes of post-employment procedures is to prevent the departing employee from soliciting the employer's customers for the purpose of moving business. This section discusses two methods for preventing erosion of the customer base by departing employees. The first involves protecting customer lists as a trade secret; the second is a practical approach to dealing with customers during the transition phase between the time that the employee leaves the company and the assignment or hiring of another employee by the employer to service the customers' needs.

Notice to the new employer of the former employee's continuing obligations not to disclose the employer's trade secrets and confidential information and to refrain from soliciting customers is another important post-employment procedure to consider. Proper notice to the employee's new employer prevents the new employer from later claiming that the use of the employer's trade secrets and confidential information, or solicitation of its customers, was innocent or inadvertent. Great care, however, must be exercised in drafting these notice letters in order to avoid future allegations against the employer of interference with the contractual relationship between the former employee and his or her new employer.

We will address as well the effect of involuntary termination on the employer's ability to enforce covenants not to compete. The answer to this question varies significantly from state to state.

A. Post-Employment Procedures

Post-employment procedures should complement the employer's overall trade secrets protection strategy. While courts usually evaluate the reasonableness of precautions taken by the employer on a case-by-case basis, the employer's adherence to a uniform protection procedure is important. A well-reasoned and

uniformly applied procedure for conducting exit interviews, protecting customer lists, counseling customers during the transition phase, and providing notification to a new employer when appropriate are all relevant considerations in evaluating the employer's diligence in protecting its trade secrets and confidential information.

1. Effect of Involuntary Termination

As discussed above, a covenant not to compete is an essential tool in preventing the loss of customers to a former employee following the termination of the employment relationship. It must be emphasized, however, that in some states, covenants not to compete will not be enforced where the employer terminates or breaches the employment relationship.

It is essential for the employer to be knowledgeable about the applicable law in its principal place of business. While the employer should consider including a choice of law provision in its employment agreement, such choice of law provision may not be enforceable if the applicable law agreed to by the employer and employee is contrary to the law of the state in which the court hearing the dispute sits.

2. The Exit Interview

The employer should educate its employees, at both the management and non-management levels, about the importance of protecting the employer's trade secrets and confidential information from disclosure. This educational process should start at the beginning of the employment relationship and should continue during the course of employment, as it is generally too late to educate a departing employee for the first time at an exit interview regarding what constitutes "trade secrets." The use of nondisclosure provisions and covenants not to compete in employment agreements, as discussed above, is an ideal method for ensuring employee awareness and compliance from the outset.

The exit interview should ideally satisfy three purposes:

(a) it provides a final opportunity to remind the departing employee of his or her obligation not to disclose confidential information or solicit customers;

(b) it provides an employer with a practical mechanism to secure the return of trade secrets, confidential documents and customer lists, and other documents and information; and

(c) when the employee is leaving voluntarily, it provides the employer with an opportunity to explore the reasons for the employee's departure.

Exit interviews have the potential to become adversarial experiences. Emotions sometimes run deep when a valued employee decides to leave a company and pursue his or her career elsewhere (often in the employ of a competitor) or when an employer terminates an employment relationship with an employee involuntarily. An employer must, however, prevent the exit interview process from breaking down, as it is likely the last opportunity, bar litigation, for the employer to emphasize to the employee what his or her continuing contractual and common-law obligations are to protect company trade secrets and confidential information.

At the exit interview, the departing employee should be clearly reminded of his or her continuing obligation not to disclose confidential information which he or she learned during his or her employment. The employer should review the employee's personnel file with the employee, concentrating on such documents as employment agreements, express written agreements not to disclose trade secrets and confidential information, nonsolicitation agreements, and covenants not to compete. While non-managerial employees are not frequently asked to enter into such agreements at the beginning of their employment, they are still subject to the same common-law obligations applicable to management level employees; namely, to maintain the confidentiality of information

they learn by virtue of their employment and to refrain from competing unfairly with their former employer.

A major advantage of a written employment agreement is that it provides unequivocal proof that the employee, at the outset of his or her employment, was aware of his/her duty to maintain the confidentiality of the employer's trade secrets and confidential information. Such documentation is indispensable for a clear understanding of the employee's obligations both during employment and thereafter.

In situations where an employee has signed a nondisclosure agreement or covenant not to compete at the beginning of the employment relationship, the employer may wish to have the employee re-acknowledge or even re-sign the document that the employee previously signed. After the employee has been given access to the employer's confidential and trade secrets information during his or her employment, the employer may also choose to be more specific by identifying the information which the departing employee is precluded from disclosing and customers subject to a nonsolicitation provision.

In the event that an employee has not entered into a written employment agreement, or where state law does not recognize the agreement because of the employee's involuntary termination, the former employer is still entitled to rely on common-law protection. Most courts recognize that a confidential relationship exists between an employer and its employees. The Restatement (Second) of Agency § 396(b) further provides that:

> After the termination of the confidential relationship, the agent, nonetheless, owes a duty not to disclose the principal's trade secrets, lists of names, or other confidential matters given to the agent.

The employer should bear in mind, however, that the law will enforce an employee's obligation to protect a trade secret only

where an employer has shown that it has taken reasonable precautions to protect the trade secret. It is for this reason as well that a uniform policy for the protection of trade secrets and confidential information should be strictly enforced.

Whenever possible, the presence of legal counsel at the exit interview is advantageous. In-house or outside counsel can best explain to the departing employee the legal ramifications of future disclosures as a breach of an express contractual obligation, and/or their common-law fiduciary duty, and can also clear up any misunderstandings that may arise during the exit interview regarding the employee's continuing obligations. Because litigation is always a possibility, the guidance of legal counsel at this stage may prove to be a worthwhile precaution.

The employer should properly and completely document the results of the interview by use of an exit interview checklist. Also the employer should consider having the employee acknowledge the accuracy of the relevant documents and the content of the exit interview by signing a written statement. Both of these forms, samples of which appear in Appendix B, *infra*, may prove to be valuable documentary evidence in the event of future litigation to establish that the employee was thoroughly advised of his or her contractual and/or common-law obligations upon termination of employment.

3. Protecting the Customer Base

The single most valuable asset of a business is often its "goodwill," which is measured by the positive relationship it has developed with its customers. The employer's source of income, and thus profit, is in most instances directly related to the business relationships it develops and maintains with its customers. For this reason, the employer's need to protect the customer base is critical, as is its need to effectively communicate with its customers during the transition phase following an employee's departure.

a. Protecting the Customer List

Recent years have seen significant litigation in an effort to protect the confidentiality of the "customer list." Employers frequently believe that the identity of their customers, their buying habits, and other customer-specific information constitute trade secrets and are protected from use by former employees. These assumptions, however, are not necessarily accurate.

Customer lists are not automatically protectable as "trade secrets." Where the customer list merely contains names of customers that can easily be collected by any competitor, courts do not generally consider the list to be a trade secret. Where, however, the customer list contains unique information, such as customer buying habits or is particular to the employer's business and cannot be easily reproduced from scratch by a competitor, the customer list may qualify as a trade secret.

In order to persuade a court that a customer list constitutes a trade secret, it is essential that the employer treat it as such by taking reasonable steps to prevent the unauthorized disclosure of the identity of its customers and other relevant information. Even if a customer list is not a trade secret, it is still the employer's "property," and any physical removal of the list or copying of it may justify equitable relief for the employer.

Although there is no clear majority rule regarding the trade secret or confidential status of customer lists in the absence of an express agreement between the employer and the employee, an employer can often protect customer lists from disclosure by an employee by utilizing nondisclosure and nonsolicitation provisions in employment agreements. A protectable customer list and the existence of express nondisclosure and nonsolicitation provisions in an employment agreement may significantly assist the employer in maintaining the confidentiality of the customer base.

b. Importance of Communicating With Customers During the Transition Phase

Another important consideration for protecting the employer's customer base is to engage in informative communications with customers with whom the employee had regular contacts during the transition phase, after the announced departure or past departure of the employee. While this consideration appears elementary, its importance cannot be overemphasized. Once a customer enjoys a comfortable and good rapport with an employee, it may be tempted to follow the employee to the competition unless aggressive efforts are made by the employer to retain the customer, thereby protecting its customer base.

To prevent the migration of customers, the employer should write to the customers to whom the employee was previously assigned and advise them that while the employee is no longer with the company, the employer will continue to provide them with the same quality of service they have come to expect. The employer should also tell customers who will be assigned to work with them going forward. The importance of personal contacts, including social outings, visits to the customers' place of business, regular telephone calls, personal notes, and verbal follow-up is critical to encourage customers to keep their business with the employer. The employer should assure its customers that any concerns or questions they may have will be efficiently dealt with and expeditiously handled. The customers should feel comfortable about leaving their business with the employer despite the employee's departure.

The content of these communications with customers must avoid the possibility of a future civil action for defamation by the departing employee. The employer should refrain from mentioning the circumstances under which the employee left the company, and should concentrate instead on assuring the customer that quality service will not be interrupted.

4. Whether to Provide Notice to the Employee's New Employer

The well-established rule concerning the rights of an employer with respect to the protection of trade secrets is that an owner of trade secrets may protect them from unauthorized disclosure or use by a third party only when the third party has actual or constructive notice: (1) that the information is considered to be a trade secret and (2) that the information was disclosed to the third party through a breach of duty arising from an express contract or a common-law fiduciary duty to the trade secret owner. The employer bears the burden of demonstrating that the third party received notice.

The most common and effective method of providing notice to a former employee's new employer is by means of a letter from the employer. This letter should be signed by the president of the company or by in-house or outside counsel. The new employer should be advised that the employee had access to trade secrets and confidential information and that he or she has a continuing contractual and/or common-law duty not to disclose such information to third parties. Where the former employee signed an employment agreement containing a covenant not to compete, nonsolicitation and nondisclosure provisions, the employer should also reference these provisions in the letter.

New employers will occasionally initiate contact directly with the former employer. Typically, the new employer may write a letter to the former employer acknowledging the employee's former employment and provide written assurance to the former employer that it does not intend to induce or permit the use or disclosure of the former employer's trade secrets or confidential information or the solicitation of its customers. Such letters are an effective means of establishing clear lines of communication and often have the desired effect of preventing litigation.

a. A Word of Caution Regarding Interference With Contractual Relations

The employer should exercise caution when drafting letters to a former employee's new employer. Such communications may cause the new employer to revoke offers of employment they have extended to the former employee or otherwise cause them to sever their new employment relationship with the former employee. Should this occur, potential civil liability may arise for intentional interference with contractual relations.[8] Such letters should be drafted with extreme caution to ensure that they are accurate, based on fact, do not overstate the employer's legal rights, and are not defamatory in nature. Caution should also be exercised to avoid reference to threatened litigation unless a clear basis exists for such assertion.

V.

ENFORCEMENT OF TRADE SECRET RIGHTS

If an employer's confidential business information, proprietary technology or know-how becomes known in the industry, then the property loses its trade secret status and the protections afforded under the law. Therefore, the primary goal of an employer seeking to enforce its trade secret rights usually is to prevent the dissemination or misuse of such property. Given this objective and the difficulty in placing a monetary value on the loss

[8]The Restatement (Second) of Torts § 766 delineates three elements to the tort of intentional interference with contractual relations:

(1) intentional and improper interference;
(2) with the performance of a contract between another and a third person; and
(3) inducement of one of the parties to the contract not to perform.

of intellectual property, the trade secret case is typically litigated in the context of a preliminary injunction proceeding.

As time is of the essence to achieve the employer's objective, preparation and strategic planning up-front are key to success in a trade secret case. This chapter explores factors to consider in deciding whether to commence litigation, important initial tactical decisions, fact-finding and initiation of the litigation.

A. To Sue or Not to Sue

Weighing the pros and cons of a lawsuit prior to commencing litigation is highly advisable. First consider what is at stake. How valuable is the information, technology, know-how or other asset such as customer goodwill to the employer's business? Some information may have only temporary value, quickly becoming outdated, while other information may be of critical importance to the viability of the business. Similarly, evaluate the nature of the competitive threat. If, through a former employee or other individual entrusted with or having access to proprietary data, it ends up in the hands of a principal competitor, the ramifications in the marketplace may be substantial.

Litigation can have an impact on the employer's public image and on employee morale, in both positive and negative ways. It can have the constructive effect of sending a strong signal to the work force and to the marketplace that the employer will take legal action to enforce and protect its rights — whether those be contractual rights under a covenant not to compete or proprietary rights in trade secret information. A consistent policy and enforcement of such rights can serve as a strong deterrent to others who may be considering leaving to unlawfully compete. It may likewise discourage competitors from hiring employees subject to restrictive covenants or nondisclosure agreements.

On the other hand, litigating against a former employee may create the image of a corporate "bully." Labor problems may develop as a result of litigation, particularly if the dispute involves a member of a labor union. Some employees may view litigation as an effort on the part of the employer to deprive an individual of

making a living and to restrict competition. Effective public relations can minimize these perceptions. Getting the right message out — that the objective is to protect proprietary information and know-how that are critical assets of the business — can dispel the "anti-competitive" misperception of such litigation.

Another business consideration is whether a lawsuit will drag the employer's customers into the dispute.

Because litigation is a public process, there is the risk of disclosure of trade secret information. Publicized litigation may pique a competitor's interest in the information. Care has to be given to establishing procedures such as protective orders and "in camera" review of evidence, to safeguard the confidentiality of proprietary information throughout the proceeding.

Consider the likelihood of prevailing in a lawsuit. The plaintiff in a trade secret case will be required to prove that the information or technology at issue is proprietary to the employer and not generally know in the industry or available to the public at large. The employer must show that it has taken reasonable measures to maintain the confidentiality of the information or know-how. Proper security measures, including well-drafted employment agreements containing nondisclosure covenants and covenants not to compete, are important — not only to protect the proprietary nature of the data or technology, but also to prevail in litigation.

A preliminary injunction action seeking to bar the use of trade secrets and confidential information or the breach of a restrictive covenant is an action in equity. Given the nature of the relief sought, courts will weigh equitable considerations such as how much time has passed since the employer knew or should have known of its claims and commencement of the litigation. A court may be less inclined to grant injunctive relief to a litigant who has "sat on his rights." Failure to respond promptly and appropriately to the actual or threatened misappropriation of trade secrets may create the impression that the information is not truly that valuable and, thus, discredit a claim of irreparable harm. Delay in

responding to the misappropriation of trade secret information may also affect the "balance of the equities." Few equities, if any, lie initially with a disgruntled employee who has jumped ship, joined a competitor and taken confidential information or know-how with him in order to gain an unfair competitive advantage over his prior employer. However, with the passage of time, particularly if the competitor expends time, money and manpower to develop a new product line or technology using the misappropriated information or know-how, the equities arguably may begin to shift.

A court of equity will look to whether an employer has "clean hands," which raises the question of the employer's conduct. If the employer has engaged in wrongdoing with respect to the matters at issue, such as violation of antitrust laws or breach of any employment agreement with a departed employee/defendant, such conduct may be an obstacle to obtaining equitable relief. Other equitable considerations may factor in, such as the circumstances of a former employee's termination. An employer who summarily discharges an employee for poor performance may have a difficult time establishing how it will be irreparably harmed if that individual is permitted to compete in violation of a restrictive covenant.

A preliminary injunction case is usually an expedited proceeding. As such, it can place significant time demands on management and other employees in terms of fact-finding, discovery and trial. The activities will be compressed into a short period of time, disrupting normal schedules and diverting time from regular business activities.

B. Fact-Finding

Thorough initial fact-finding is critical to preparing for and succeeding in litigation. Employers must promptly investigate suspected misappropriation of trade secrets, particularly if injunctive relief is sought. Under such circumstances, a search of a departed employee's office is advisable and may indicate whether company files or other information maintained by the departed employee is missing. If the individual used a computer, those computerized files should be checked. Certain software programs

enable one to recover information that has been "deleted" from a computer. Records of computer usage may reveal recent unusual activity, such as the printing out of a large volume of information or access to computer files not normally used by the departed employee in the course of job performance. Likewise, records of duplicating activity should be checked. Interviews of a former employee's staff and co-workers may disclose important information. Telephone records, calendars, phone slips, expense reports and travel logs are other good sources of information. Records showing access by the departed employee to the employer's offices during off-hours may also be significant evidence.

Information about the new entity with which the departed employee has associated, such as the date of incorporation, location of business offices and financial status as shown in Dun & Bradstreet reports, should also be obtained.

C. Initial Tactical Decisions

1. Whether to Send a Warning Letter

A question frequently asked is whether it is advisable to send a warning letter prior to initiation of a lawsuit. A letter may be appropriate in some cases, such as when a competitor may not be aware that a new hire is subject to a covenant not to compete with his prior employer. A letter also may serve the purpose of heightening a competitor's sensitivity to the proprietary concerns of another. Sending a warning letter prior to initiating legal proceedings also conveys to the court that the trade secret owner has made an effort to find a business solution to the problem before resorting to litigation. It may diminish or eliminate any negative inference that might otherwise be drawn from a delay in responding to a threatened misappropriation of trade secrets. The downside risk of such a communication is that it places the competitor on notice, enabling it to prepare for the possibility of litigation and possibly leading to the destruction of important evidence.

2. Where to Sue

Selecting the proper forum for bringing the lawsuit is another important tactical decision. If a contract is involved, there may be a forum selection clause which may dictate where and how disputes are to be resolved. Furthermore, an employment contract may include an arbitration clause requiring that disputing parties submit to arbitration.

Nonetheless, jurisdiction and venue rules may permit a choice of forum. A plaintiff usually wants to sue close to "home" in order to maximize the chances of success and reduce litigation expenses. Liberal long-arm statutes may facilitate the selection of a favorable forum.

Because time is of the essence in trade secret and restrictive covenant litigation, the differences in court dockets and calendar systems may be a significant factor in choosing a forum. An individualized calendar, where one judge decides the case and all preliminary matters, may be preferable to court systems that divide those functions. Similarly, a court with a fast-moving docket is usually preferable to one with a backlog of cases when seeking preliminary injunctive relief.

If there is diversity among the parties (i.e., the plaintiff is a resident of a state different from that of the defendants) and the amount in controversy exceeds $75,000, the federal courts will have jurisdiction over the case. Federal court dockets in some states are less crowded than state court dockets, and discovery procedures are more established. Usually in federal court one judge will be assigned to hear the entire case. In state court different judges may preside over different phases of the litigation.

Some trade secret/restrictive covenant cases also involve violation of federal laws such as the Copyright Act or unfair competition under the Lanham Act. Such violations may provide another basis for bringing the lawsuit in federal court. In addition, owners of trade secrets can seek to prosecute under the Economic Espionage Act, 18 U.S.C. §§ 1831-39 — a criminal federal statue.

Once a decision is made to sue, counsel should act fast to select the forum. There is always the risk of the adverse party initiating litigation first — for example, by filing a declaratory judgment action seeking to void a covenant not to compete. By suing first, the adverse party may be able to control selection of the forum.

3. Whom to Sue

Potential defendants in a trade secret/restrictive covenant case include the departed employee(s); any new competitive company or entity established by the departed employee(s); the competing company who hired the departed employee(s) and/or was the recipient of trade secret information; and financial backers, "silent" partners or others acting in concert with the former employee(s).

D. Temporary or Preliminary Injunctive Relief

While the grant of a preliminary injunction is not dispositive of the case, practically speaking, it accomplishes the primary objective of the plaintiff, which is to stop the disclosure or use of proprietary information. In addition, success at the preliminary injunction hearing provides significant leverage and often leads to a resolution of the entire action. Conversely, if the preliminary injunction stage is unsuccessful, the trade secret may be lost, and chances of obtaining permanent injunctive relief at a final hearing on the merits, absent the discovery of new evidence, is diminished. The hearing on the motion for a preliminary injunction is therefore a crucial phase in the litigation.

In order to prevail in an action for preliminary injunctive relief in either federal court or state court, the moving party must show: 1) a likelihood of success on the merits of his or her claim; 2) irreparable harm to the moving party absent the injunctive relief; 3) that the balance of the equities weighs in favor of granting preliminary injunctive relief; and 4) that preliminary injunctive relief is in the public interest. Federal Rule of Civil Procedure 65, entitled *Injunctions*, governs preliminary injunctions and

temporary restraining orders in federal court. Usually a party in a trade secret/restrictive covenant case pursues a preliminary injunction after expedited discovery.

In some cases, however, the misappropriation of trade secrets may present such a threat of irreparable harm that a temporary restraining order ("TRO") without notice to the other side is necessary. While a court can issue a TRO based on affidavits alone if it appears that immediate and irreparable harm may result before the adverse party can be heard in opposition, the entry of such an *ex parte* TRO will accelerate the proceeding under the rules of most courts. For example, under the federal rules, a temporary restraining order expires within ten days unless extended by the court or by the consent of the parties. Thus, such immediate relief is short-lived and may result in a prompt hearing before much, if any, discovery can be taken.

As a practical matter, courts are reluctant to issue TROs without notice to the other side. The moving party must therefore be able to articulate a compelling reason why written or oral notice cannot be given and the nature of the harm that the moving party will sustain if notice is given. The federal rules require counsel to provide this information in federal court.

A party obtaining a preliminary injunction or temporary restraining order must file a bond with the court in an amount set by the court, which bond is for payment of damages suffered by any party who is found to have been wrongfully enjoined or restrained as a result of the entry of the injunction.

E. Initial Pleadings

A party may initiate a trade secret/restrictive covenant case by filing a complaint in the appropriate court. The complaint can be either verified or accompanied by affidavits setting forth facts sufficient to establish the plaintiff's entitlement of the relief being sought. The complaint should set forth the nature of the proprietary business interest at issue — whether technology or know-how, confidential business information, such as customer lists, pricing or goodwill; the investment made by the plaintiff to

develop the know-how, information or goodwill developed over the years and the measures taken to maintain the information in confidence; the manner in which the defendant gained access to the information, whether through employment in a position of trust and confidence or some other confidential relationship or through improper means; and the irreparable harm that the plaintiff will suffer if the information is used or disclosed or if customer goodwill is diverted.

Causes of action typically available in trade secret/restrictive covenant cases include:

(1) breach of employee's contract;

(2) breach of employee's fiduciary and common law duties;

(3) misappropriation of trade secrets and confidential information;

(4) tortious interference with the former employer's contractual and business relations with the ex-employee (if a new employer is involved) and/or between the former employer and its customers or suppliers; and

(5) unfair competition.

Another cause of action to include, if the facts warrant, is a count for civil conspiracy. Prevailing on such a cause of action may offer recovery in addition to what one may recover for the underlying torts; e.g., joint liability, increased monetary damages and expanded injunctive relief. The courts have uniformly recognized four basic elements of a cause of action for common law civil conspiracy:

(a) a combination of two or more persons/entities;

(b) to establish an unlawful object or to accomplish a lawful object by the use of unlawful means;

(c) overt acts in furtherance of the conspiracy; and

(d) resulting injury to the plaintiff.

In terms of the prayer for relief, the complaint should seek injunctive relief, preliminary and then permanent, as well as damages and costs.

F. Motion for TRO and/or Preliminary Injunction

It is usually advisable to file a motion for a TRO and/or preliminary injunction with the complaint. The motion and proposed order should spell out the specific type of temporary or preliminary injunctive relief being sought. For example, in a trade secret case, a plaintiff may seek a preliminary injunction barring an individual or entity from further work in a particular field or competitive business, or development of a certain product line or technology for a specific time period; barring the use or disclosure of certain information, know-how or technology; and requiring the return of all proprietary information of the plaintiff in any tangible form. In a restrictive covenant case, a plaintiff may seek a preliminary injunction barring a former employee from breaching the terms of a covenant not to compete; barring the solicitation of customers; and requiring notification to all customers of the injunction. An accounting is additional equitable relief that should be considered. The injunctive relief sought in the complaint should parallel the relief sought in the motion for the TRO and/or preliminary injunction and proposed order.

G. Motion for Order of Court Directing Preservation of Documents, Software and Things

An order requiring the preservation of relevant information from destruction or alteration is a useful tool. Such an order does not impose on a defendant any duty or burden beyond what is required by the rules of court and therefore is usually granted. It is a vehicle for conveying to the court the severity of the matter

and possibly highlighting defendant's conduct to date, showing the reason why a bona fide concern exists that evidence of wrongdoing may be destroyed. The entry of such an order may deter a defendant from altering or destroying evidence such as computer-based data which can easily be deleted.

H. Motion for Expedited Discovery and Proposed Order Setting Specific Dates for Depositions and Production of Documents

Typically under the rules of court, discovery may not be taken for 30 to 45 days after the complaint has been filed by a plaintiff. An employer may need expedited discovery to develop facts for a preliminary injunction hearing. Discovery may be expedited only by order of court. Taking discovery quickly also realizes the advantages of surprise. If the defendant is forced to comply with discovery by way of giving testimony at a deposition and producing documents, it diverts time the defendant might otherwise devote to unlawfully competing with the former employer.

I. Protective Orders

Before discovery or trial, the former employer should ask for a protective order to ensure the continued confidentiality of any trade secrets or proprietary information. Such an order often creates a presumption or impression of the existence of confidential information. It also eliminates any objections to discovery based on the existence of trade secrets or confidential information.

Consider how restrictive the protective order should be — should information produced in discovery be available to the parties only, for designated representatives of the parties or for "attorneys eyes only"? One approach is to have a "two-tier" protective order providing for two different classifications of confidential information.

The protective order should address what is to be done at the end of the case with the confidential information produced by each side (usually such information is returned to the producing party or destroyed).

VI.

DISCOVERY IN A TRADE SECRET/COVENANT CASE

A. Discovery Goals and Objectives

As in all litigation, the plaintiff's foremost goal in discovery is to glean as much pertinent information as possible as quickly as possible to support its claims. Given the time-sensitive nature of trade secret/covenant cases, however, the pressure to achieve this goal can be intense and critical sources of information may be overlooked. It is essential, therefore, to have a clear picture of the elements of proof necessary to prove each claim and to focus discovery efforts on the most likely sources of information and documents to support those claims. Use of a written discovery plan, which outlines the elements of the various causes of action and the proof needed to support them, may be extremely helpful.

B. Likely Motions

Trade secret/covenant cases frequently require the immediate filing of a number of motions designed to speed the discovery process, to preserve evidence and to protect the confidentiality of information produced. The most common motions are: (1) to expedite discovery; (2) to preserve evidence; and (3) for a protective order.

1. Motion to Expedite

Given the urgent nature of trade secret/covenant litigation, much discovery is likely to be conducted on an expedited basis.

This, of course, will generally require the filing of a motion to expedite, either with or shortly after the filing of the complaint and injunction papers. Although many employers view such a motion as an afterthought, this is a mistake. A well-crafted motion to expedite can not only provide the court with a concise view of the events surrounding the litigation, but can also convey the urgency of the situation.

A motion to expedite should contain the following:

- a brief recitation of the pertinent facts surrounding the litigation;
- an explanation as to why discovery should be expedited and suggested time frames for the production of documents and the taking of depositions;
- a proposed form of order; and
- attached copies of proposed document requests, deposition notices and third-party subpoenas.

Before filing a motion to expedite, a company should have carefully considered and determined the types of information that it will seek and the sources of that information so that the request can be as specific as possible. The types and sources of information are discussed more fully in Part C, *infra*.

2. Motion to Preserve Evidence

It is generally advisable to file a motion for preservation of evidence as soon as possible. This is particularly true where a company has reason to believe that information that has been stolen from it may be destroyed. It is also effective in casting doubt upon the motives and behavior of the defendants.

A motion for preservation simply asks the court to order that no relevant documents, computer data or other information in the possession or under the control of the defendants be destroyed,

changed or altered during the period of time pending the litigation. This may prove to be particularly critical in cases involving theft or misuse of computer or other electronic data which can be easily modified or deleted.

3. Motion for Protective Order

Trade secret/covenant cases usually involve the entry of a protective order governing the treatment of documents produced during the course of discovery, either by agreement or motion. This is necessary because of the confidential and sensitive nature of the information involved. Moreover, a plaintiff company seeking relief against the misuse of its stolen confidential information will itself often be required to produce other business information that is also confidential. Similarly, courts may require defendants to produce not only the allegedly stolen information, but also other confidential information about business operations, and strategies, customers, processes and financial condition.

A protective order will outline the procedures for identifying and maintaining documents that are deemed to be confidential, as well as portions of deposition transcripts and court filings. It will also typically limit the persons who can see the documents produced. For example, it may allow only the outside attorneys and experts for the parties to see the documents, or it may provide for a slightly broader group, perhaps adding a specific number of business people and corporate counsel on each side. The identity of the persons permitted to see the documents should be carefully considered. There is a need to balance the danger of allowing key business people on the opposing side to see a plaintiff company's confidential information against the need for a plaintiff company's own knowledgeable executives to review the information produced to evaluate the degree of the opponent's wrongful conduct.

Once a motion for protective order has been entered, plaintiff companies must follow its terms to avoid inadvertent waiver of a claim of confidentiality. All documents that a company wishes to designate as confidential should be clearly marked as such. Court papers that include confidential documents

or deposition excerpts should be filed under seal. Filing under seal also lessens the chances of disclosure of confidential information through the media's review of court filings.

C. Sources and Types of Information

Documents and information to support a plaintiff company's claim in a trade secret/covenant case may come from many sources. A critical one which is sometimes overlooked is the plaintiff company itself. Others include: (1) the ex-employee; (2) the new employer; and (3) any recruiter who may have been involved.

1. The Plaintiff Company

A company that has been victimized by the theft of trade secrets or the violation of a covenant is frequently so anxious to exact revenge on the opposition that it fails to focus on a fertile ground for support for its claims — its own files, which may provide potent ammunition.

Among the types of information that should be carefully gathered and reviewed are the following:

(a) **Documents and information that show the high level of trust and confidence placed in the ex-employee**. This would include, for example, job descriptions or internal memos outlining the employee's duties and responsibilities; any documents reflecting the employee's security level or degree of access to confidential information; and documents showing the employee's personal involvement in the development of the plans, strategies, products or customers in question.

(b) **Documents and information that show the ex-employee's agreement not to disclose confidential information, solicit employees or solicit customers**. Included in this category are confidentiality agreements or covenants that the

ex-employee may have signed; personnel manuals that the ex-employee may have received outlining the company's policies and expectations regarding the confidentiality of information; and the ex-employee's signed acknowledgment of receipt of the personnel manual.

(c) **Documents and information that may show pre-leaving wrongful conduct**. The ex-employer should carefully review the ex-employee's expense and business records to determine whether he or she used company time or money to solicit employees or clients. These records may show, for example, that the employee interviewed for a position with the defendant competitor and charged travel expenses back to the plaintiff employer, or that he or she entertained clients for the purpose of having them switch their business to the new employer. In addition, remaining employees should be thoroughly interviewed to determine if there was improper solicitation.

2. Ex-Employee and New Employer

Among the categories of documents and information which should be sought from the defecting employee and his or her new employer are the following:

(a) **Documents or materials taken by the ex-employee from the plaintiff company**. It is critical to determine the extent and timing of the removal of all confidential information from the plaintiff employer. Documents may reveal a gradual pre-planned misappropriation, which would tend to support a conclusion of bad motive. In cases involving more than one defecting employee, there may have been agreement and collaboration regarding the information to be taken and the method of taking it, as for example where a high-ranking employee who is subject to

a covenant or confidentiality agreement attempts to have a lower-level employee not subject to the same restrictions steal the information or solicit the clients.

(b) **Documents or materials showing concerted action among ex-employees**. In cases involving the defection of more than one employee to a competitor, it is often possible to establish the existence of a common plan or scheme to steal information, clients or other employees. Documents that may be relevant to this area of inquiry include calendars or date books which may show the timing of meetings and communications among the defecting group, simultaneous or closely timed offer letters, and internal documents of the new employer showing that the defectors were considered a "package deal."

(c) **Documents or information showing participation/agreement by the new employer**. This would include such items as offer letters, employment contracts, file memos or correspondence which may tend to show that the new employer began negotiating with the ex-employee long before he or she actually left the employ of the plaintiff company. In addition, there may be documents which show that the prospective new employer discussed the existence of the confidentiality agreement or covenant with the employee and knew of its contents, or that there was prior discussion of moving specific pieces of business or clients.

(d) **Documents or information showing the new employer's own efforts to protect its trade secrets, customers or market position**. It is quite common for the new employer itself to use confidentiality agreements or covenants, which

can often be used to undermine its position that it did not believe that there was any problem in hiring the ex-employee in question. These agreements often contain language similar or identical to that used by the plaintiff employer. In addition, the new employer's personnel manuals may contain language emphasizing that its own employees have access to confidential information and agree not to disclose it.

(e) **Documents or information showing the illicit use made of the stolen information**. This category includes all files of the new employer that reveal new clients or pieces of business added as a result of the use of the stolen information, as well as any solicitation efforts in which the new employer may be engaged. It also includes such seemingly mundane items as date books and calendars, which may note client lunches or meetings at which ex-employees tried to solicit clients.

3. Recruiters

If the competitor used a recruiter or headhunter to solicit the ex-employee, whether or not the recruiter is named as a defendant, the plaintiff company should seek discovery to the extent, nature and timing of the contacts between and among the recruiter, the ex-employee and the competitor. Also, the plaintiff company should search for the fees paid to the headhunter, information and objectives conveyed by the competitor to the headhunter regarding the position in question, the extent and nature of the headhunter's knowledge of any confidentiality agreement or covenant to which the ex-employee is subject, and whether the headhunter has been engaged to solicit other employees of the plaintiff company, which may support the concept that the competitor is engaging in a raid.

D. Discovery of Computer and Electronic Data

Misappropriating information that is stored on computer or using a computer to misappropriate information, is extremely common in trade secret/covenant cases. While the discovery of computer and electronic data is generally governed by the same rules applicable to other types of discovery, it often takes on an entirely new dimension given the nature of the information sought. In this regard, plaintiff companies should note the following points:

1. Internal Investigation

It is often possible to develop a highly accurate road map of a defecting employee's misappropriation of computer data, or misuse of computer access rights, by performing an immediate internal investigation of the ex-employee's computer usage preceding the departure. An individual (either within the company or hired from outside) with expertise in systems management should perform this investigation and thoroughly document all aspects of the following:

(a) **Accessing files not usually used**. While most companies limit access to files by the use of passwords, it is not uncommon for certain employees (especially in smaller companies or who are relatively high-ranking) to have broad access rights. Under these circumstances, determine whether the ex-employee has accessed files which are not generally required for his or her daily work.

(b) **Unusually frequent computer usage**. Determine whether the ex-employee has been accessing the network at an unusually frequent rate or at unusual times, as for example after hours.

(c) **Transferring files via modem**. Determine whether the ex-employee has been transferring

files from the computer network to a personal server and/or to a home computer via modem, especially for long periods of time and at unusual hours.

(d) **Laptop and home computer inventory**. If the ex-employee has been provided with a laptop computer (or has had access to one), make sure that it is returned and immediately inventory its contents. Determine if there are any unusual files or signs of activity. In addition, it may be possible in discovery to require the ex-employee to produce any home computer for examination and analysis.

2. Discovery of Computer Data From Defendants

In addition to determining the extent of any misappropriation of information via computer by means of an internal investigation, it is also critical to ascertain the extent to which the stolen computer data has been placed upon the system of, or used by, the competitor. In this regard, focus on the following:

(a) **Copying/transfer of stolen data to competitor's system**. All of the competitor's pertinent computer records should be reviewed to determine whether and when any of the stolen data was copied or transferred onto its own system.

(b) **Destruction of data**. In some instances, stolen data is copied onto a competitor's system or network and later deleted. Such deletion may evidence knowledge of the impropriety of having the data in the first place. It is important to ascertain whether and when any deletions occurred, again by reviewing pertinent records and by deposing the competitor's director of management information systems.

(c) **Back-up systems**. The existence and functioning of the competitor's computer back-up system should be carefully studied to determine whether any of the stolen information still remains available to the competitor and how it can be retrieved.

(d) **E-mail**. Like computer data bases, e-mail messages are also discoverable to the extent permitted by the rules that govern discovery generally. Because e-mail messages tend to be written informally and the writer often does not realize that they are potentially discoverable, e-mail messages often include information that would never be included in a formal memorandum. In addition, e-mail messages may remain on a company's data base even after they have been "deleted" by the reader.

Thus, a plaintiff company should specifically request the production of all e-mail messages (including deleted ones) pertaining to the litigation, since these may contain valuable information not found elsewhere. Conversely, a plaintiff company should recognize that its own e-mail messages may be subject to scrutiny.

VII.

RELIEF AVAILABLE IN TRADE SECRET MISAPPROPRIATION CASES

Following the misappropriation of a trade secret, a trade secret owner wants to limit the damage caused by the misappropriation. First, a trade secret owner will attempt to stop a misappropriator by seeking an injunction. If circumstances render the injunction an inadequate remedy, a trade secret owner will also seek monetary relief. A trade secret owner will attempt

to recover the profits lost from the misappropriation as well as any profits that the misappropriator made from the trade secret.

The Uniform Trade Secrets Act ("UTSA"), the Lanham Trade-Mark Act, and common law provide trade secret owners with a variety of claims and theories upon which to obtain relief. Unfortunately, deciding upon an appropriate claim for damages, choosing the theory of liability, and proving damages are the some of the most difficult aspects of trade secret litigation. Trade secret misappropriation, unlike other causes of action, does not give rise to easily quantifiable damages. Rather, courts in trade secret misappropriation cases have great discretion in determining damage amounts.

First, this section will note the types of relief that a trade secret owner has available against a trade secret misappropriator. Usually, a trade secret owner will seek relief under several different theories of relief. It will also review the nature of these relief theories and when they are appropriate. Second, this section will explain the three primary theories under which trade secret owners seek monetary relief: legal, equitable, and market share theories as well as the method of proving entitlement to such relief.

A. Overview of Available Relief

1. Injunctive Relief

Injunctive relief provides trade secret owners with the greatest protection against trade secret misappropriators. An injured trade secret owner should first seek injunctive relief because monetary relief does not protect the trade secret owner's information. The trade secret owner must protect the trade secret to maintain the viability and competitiveness of the trade secret owner's business. Yet, if a misappropriator causes general dissemination of a trade secret, then an injunction is not effective and monetary relief is appropriate.

Because injunctions frequently serve as the only effective remedy, courts generally swiftly enjoin actual or threatened trade secret misappropriation. *See* Unif. Trade Secret Act § 2(a).

However, the UTSA provides that "an injunction shall be terminated when the trade secret has ceased to exist." *Id*. In other words, courts terminate injunctions when the misappropriator could have developed the trade secret apart from the misappropriation.

Additionally, courts may continue a temporary injunction for a reasonable time. A reasonable extension period is the amount of time necessary to eliminate any commercial advantage that the misappropriator might otherwise derive from the trade secret. *See K-2 Ski Co. v. Head Ski Co., Inc.*, 506 F.2d 471, 474 (9th Cir. 1974). Thus, an injunction may last forever or for the length of time that the misappropriator would have taken to develop or figure out the trade secret on its own. *See id*. (concluding that the court appropriately enjoined the company for the time period that it would need to develop its own product without the misappropriated trade secret information).

Another type of injunction involving a royalty payment may also be granted for the period during which use of the trade secret could have been prohibited. *See* UTSA § 2(b) commentary at 450 (1990). In certain exceptional circumstances,[9] courts may grant this injunction allowing the misappropriator continued future use of the trade secret in exchange for reasonable royalty payment. This special situation arises when the misappropriator's future trade secret use will damage a trade secret owner but an injunction against future use is inappropriate. For example, if a third party reasonably relies in good faith upon acquisition of a misappropriated trade secret without reason to know of its prior misappropriation, then an injunction prohibiting future use would prejudice that third party.

[9]The official commentary of the UTSA § 2(b) envisions the following two exceptional circumstances: (a) an overriding public interest and (b) third party's reliance in good faith upon its acquisition of the trade secret without knowledge of the secret's prior misappropriation.

2. Royalties[10]

The trade secret owner may request royalties where injunctive relief is not appropriate or as an alternative to quantified monetary damages for unauthorized use of a trade secret. *See* UTSA § 3(a). A "reasonable royalty"[11] differs from monetary damages because it is not a simple percentage of actual profits; rather, the fact finder determines the actual value of what the violator has appropriated. *Metallurgical Industries, Inc. v. Fourtek, Inc.*, 790 F.2d 1195 (5th Cir. 1986) (calculating the reasonable royalty based on what the parties would have agreed to as a fair price for licensing the misappropriated trade secret). Methods for determining royalty amounts include reference to existing royalty agreements with other parties, existing license agreements, and hypothetical negotiations in an open market.

3. Unjust Enrichment

A claim for unjust enrichment is frequently appropriate as a supplemental claim for relief and generally is included along with other claims. *See* UTSA § 3(a); *see generally Reingold v. Swiftships Inc*., 210 F.3d 320 (5th Cir. 2000) (holding that courts may grant unjust enrichment in addition to relief for plaintiff's actual loss and that a general remedy law does not preclude unjust enrichment). Unjust enrichment is defined as "any quantifiable unjust benefit that is realized by the misappropriation and is not accounted for in the monetary damages or reasonable royalty calculations." *See General Clutch Corp. v. Novikov*, 10 F. Supp. 2d 124, 130-31 (D. Conn. 1998) (holding that the jury could reasonably find that a former employee was unjustly enriched in the amount of $100,000 when he appropriated trade secrets).

---

[10]The official comment to UTSA § 3(a) explains that a reasonable royalty serves as a general option, awarding monetary relief because of the misappropriator's past conduct. *See* UTSA commentary at 456 (1990).

[11]Courts require the trade secret owner to support the royalty amount demanded by competent evidence. *See* UTSA § 3 commentary at 456 (1990).

4. Exemplary Damages

Courts grant exemplary or punitive damages when the misappropriator's conduct is willful or malicious. *See* UTSA § 3(b). Such damages are limited to twice the amount awarded under a claim for monetary damages. *See id.* An award of punitive damages is within the trial court's discretion and the amount of the award will not be reversed unless clearly erroneous. *See* UTSA § 3(b) commentary at 459 (1990) (noting that courts use clearly erroneous as the standard of review).

5. Attorneys' Fees

The Uniform Trade Secret Act provides that attorney's fees may be awarded to the prevailing party[12] in three specific circumstances: "(i) a claim of misappropriation is made in bad faith; (ii) a motion to terminate an injunction is made or resisted in bad faith; or (iii) willful and malicious misappropriation exists." UTSA § 4. The official commentary to the UTSA notes that courts determine whether to award attorney's fees as well as the amount of such award even if a jury has heard the case. UTSA § 4 commentary at 460 (1990).

6. Prejudgment Interest or Lost Opportunity Costs

A claim for damages may include prejudgment interest or lost opportunity costs. These damages consist of not only the royalty payments and monetary loss but also the foregone use of such monies between the time of misappropriation and the date damages are paid. Whether courts implicitly incorporate such costs into relief awards and whether courts will begin to include expressly these costs remains to be determined.

---

[12]Either the plaintiff or defendant may recover attorney's fees depending on who acted wrongfully in causing the lawsuit. UTSA § 4 commentary at 460 (1990). For example, attorney's fees may be awarded for reasons ranging from specious claims of misappropriation to a misappropriator's specious efforts to terminate injunctive relief. *Id*.

7. Tort Recovery

In the case of a competitive tort such as trade secret misappropriation, the wrongdoer must answer for all consequences naturally resulting from the wrongful act whether or not they were anticipated or contemplated. *See Broan Mfg. Co. v. Associated Distribs., Inc.,* 923 F.2d 1232, 1235 (6th Cir. 1991) (citing *Aladdin Mfg. Co. v. Mantle Lamp Co. of Am.,* 116 F.2d 708, 716 (7th Cir. 1941). Trade secret owners may recover compensation for all injury to their businesses which are naturally and proximately caused by the tortious act. *See id.* Business injuries include reputation, goodwill, loss of business, expenses incurred because of such tort, and all other elements of injury to the business.

B. MONETARY RELIEF

Courts may award only legal damages in trade secret cases or they can couple such damages with equitable relief. *See* UTSA § 3. However, if a trade secret owner seeks a monetary judgment only, courts will treat the claim as exclusively legal and grant a jury trial absent imperative circumstances. *Dairy Queen, Inc. v. Wood*, 369 U.S. 469, 479-80, 82 S. Ct. 894, 900-01 (1962) (holding that damages for trademark infringement claim required legal issues to be tried before a jury prior to the court deciding equitable remedy of injunction and noting that using the equitable terms of "accounting" rather than "damages" did not effect jury trial right). However, courts and juries can seldom measure damages with any assurance of accuracy and may not adequately compensate for loss. *See Vermont Microsystems, Inc. v. Autodesk, Inc.,* 88 F.3d 142, 151 (2d Cir. 1996) (noting that trial courts receive great deference for their factual findings regarding damages because of the degree of uncertainty associated with establishing damages).

1. Relief Theories

Although most courts associate trade secret litigation with equitable relief because injunctions generally serve as the most useful remedy, trade secret owners frequently seek relief based on multiple theories, and courts no longer make a rigid distinction between these theories. Whether courts discuss monetary relief in

terms of a legal, equitable, or market share theory, courts generally assess amounts based on the circumstances of the case in view of both trade secret owner's losses and the misappropriator's profits. *See generally*, Joel Eichengrun, *Remedying the Remedy of Accounting*, 60 IND. L.J. 463 (1985) (discussing how most courts grant restitution for wrongdoer's profits without addressing the law-equity distinction).

a. Legal Damages

Courts calculate the trade secret owner's lost profits through methods that range from relatively straightforward to extremely complex. Courts often consider the following factors: (a) the nature of the misappropriated trade secret, (b) the businesses and degrees of competition of the trade secret owner and the misappropriator, (c) the length of time each has produced the goods which incorporate the trade secret, (d) research and development costs, and (e) size of the market as well as many other factors difficult to quantify. *See Vermont Microsystems, Inc.*, 88 F.3d at 152 (noting that courts usually consider many factors when adjusting damages, such as the nature and extent of the misappropriator's use of the trade secret).

Because determining the amount of profits that the trade secret owner lost is so difficult, courts often consider more than just the traditional common law remedy of what damages the victim sustained. *Tri-Tron Int'l v. A. A. Velto*, 525 F.2d 432, 437 (9th Cir. 1975). Even in a legal action, the courts may measure damages based on the secret owner's lost profits by looking to the benefit conferred on the misappropriator. *See id*. (awarding $35,000.00 in actual damages and noting that the court should not only calculate the victim's lost profits but also the misappropriator's profits); *see also Metallurgical Indus., Inc. v. Fourtek, Inc.,* 790 F.2d 1195, 1208 (5th Cir. 1986) (noting the importance of calculating the actual value of misappropriation of the trade secret and awarding a reasonable royalty). The benefits to the misappropriator can include direct profits on sales of products incorporating the misappropriated trade secret, reduced research and development costs, or other saved costs. *See Int'l Indus., Inc. v. Warren Petroleum Corp.,* 248 F.2d 696, 699 (3d Cir. 1957)

(analogizing trade secret misappropriation to patent infringement and using the comparison method to calculate defendant's actual advantage). Despite the difficulty in calculating the trade secret owner's lost profits, courts can more easily measure monetary damages when the trade secret owner directly competes with the misappropriator. *See Metallurgical Indus., Inc. v. Fourtek, Inc.,* 790 F.2d 1195, 1208 (5th Cir. 1986) (recognizing competitive posture as an important factor).

Courts allow trade secret owners to recover damages for the time period when the courts find the trade secret protected, plus any additional period when a misappropriator retains an advantage over good faith competitors because of the misappropriation. *See* UTSA § 3(a) commentary at 456 (1990); *see also Carboline Co. v. Jarboe,* 454 S.W.2d 540, 555 (Mo. 1970) (limiting the damages to the time period that the misappropriator could have discovered the trade secret).

Although a claim for actual damages and lost net profits can be combined with a claim for injunctive relief, if both claims are granted, the injunctive relief will ordinarily preclude a monetary award for the period during which the injunction is effective. *See* UTSA § 3(a) commentary at 456 (1990). *Cf. Whiteside Biomechanics, Inc. v. Sofamor Danek Group, Inc.,* 88 F. Supp. 2d. 1009, 1020 (Mo. 2000) (holding that an injunction against defendant's future sales would be redundant because the lower court already granted monetary relief). Although courts do not allow double counting, courts generally permit recovery for both trade secret owner's actual losses and the misappropriator's unjust benefit to the degree the two do not overlap. *See* UTSA § 3(a) commentary at 456 (1990) (citing *Tri-Tron Int'l*, 525 F.2d at 437 (noting that courts asses damages according to wrongdoers' profits and victims' losses)).

b. Equitable Damages

The equitable counterpart of an action for damages at law is an accounting for profits. Courts should grant an accounting in the following circumstances: (1) the misappropriator was unjustly enriched; (2) the trade secret owner was injured by the

misappropriation; or (3) if an accounting could have a deterrent effect upon the misappropriator. *See Monsanto Chem. Co. v. Perfect Fit Prods. Mfg. Co., Inc.,* 349 F.2d 389, 394-96 (2d Cir. 1965); *see generally W.E. Bassett Co. v. Revlon, Inc.,* 305 F. Supp. 581 (S.D.N.Y. 1969). However, an order for accounting is properly denied if an injunction alone will satisfy the equities. *See Champion Sparkplug Co. v. Sanders,* 331 U.S. 125, 132, 67 S. Ct. 1136, 1140 (1947).

In order for the trade secret owner to prove entitlement to an accounting for profits, the trade secret owner must first establish his injury by showing that a nexus exists between his losses and the misappropriator's gains. He must then show that the misappropriator actually made sales which involved the stolen trade secret. After proving the misappropriator's profits, courts presume that the trade secret owner's losses occur as a result of the misappropriator's gains. Once this prima facie case is made, the misappropriator carries the burden of proving there was no causal connection between his profits and his unlawful conduct. If the misappropriator is successful, the trade secret owner will be denied recovery of the defendant's profits. An unsuccessful misappropriator may be required to disgorge not only the profits of his wrongdoing, but may also be required to provide sales information or the names of customers to the wronged owner. Profits owed by the misappropriator are net profits, after deduction of actual costs and other expenses.

In general, courts account for profits and grant equity awards under three theories: the compensation theory, the deterrent theory, and the unjust enrichment theory. *See Basch Co., Inc. v. Blue Coral, Inc.*, 968 F.2d 1532, 1537-40 (2d Cir. 1992) (discussing how courts award equitable relief based on the three theories); *see also, Bundy Corp. v. Teledyne Industries Inc.*, 748 F.2d 767, 772 (2d Cir. 1984); *Ideal World Marketing, Inc. v. Duracell, Inc.*, 997 F. Supp 334, 337 (E.D.N.Y. 1998). Courts have great discretion in determining the award of profits based on these theories and may adjust the award if profits prove to be inadequate or excessive. *See Burger King v. Weaver,* 169 F.3d 1310, 1321 (11th Cir. 1999). In fact, courts may make awards greater than what the court finds would adequately compensate the

trade secret owner because of the deterrent and unjust enrichment theories. *See id*. However, a limit exists as to the amount courts may award after compensating the trade secret owner since awards cannot be remote or purely speculative. *See Broan Mfg. Co. v. Assoc. Distribs.*, 923 F.2d 1232, 1235 (6th Cir. 1991).

Additionally, some courts hold that trade secret owners must meet further requirements to receive an accounting for profits under the deterrence and unjust enrichment theories. For example, some courts have held that deterrence alone does not justify an award of the misappropriator's profits. *See Alpo Pet Foods, Inc. v. Ralston Purina Co.,* 913 F.2d 958, 968 (D.C. Cir. 1990) (stating that damages should not be awarded "for their sheer deterrent effect"). Therefore, these courts require a showing of (a) damage to the trade secret owner or (b) willfulness or bad faith on the part of the misappropriator. *See id*. Likewise, in order to recover under the deterrent or unjust enrichment theories, some courts require the trade secret owner to prove that the misappropriator willfully deceived the owner when the owner cannot show actual damages to support an accounting of the misappropriator's profits on a compensation theory. *See Basch Co. v. Blue Coral, Inc.,* 968 F.2d at 1532, 1539-40 (2d Cir. 1992).

c. Market Share Damages

Market share theory of damages emerged relatively recently out of antitrust litigation and offers a new method of assessing damages based on business torts. It relies on the proposition that courts should evaluate the real injury sustained from the business tort by considering the company's position in the marketplace. Under this theory, courts measure damages by finding what the trade secret owner could reasonably have expected to attain absent the misappropriation based on the share of total market sales. In particular, the market share theory proves useful when the tort forecloses the trade secret owner from entering a new market or where sales fall below their reasonable expectations. Courts require trade secret owners to prove the fact that damage occurred only with reasonable, not absolute, certainty. *See Broan Mfg. Co. v. Associated Distribs., Inc.*, 923 F.2d 1232, 1235 (6th Cir. 1991). Thus, the trade secret owner need only show

the amount of damages with as much certainty as the nature of the tort and the circumstances of the case permit. *See id*.

2. Proof of Damages

a. Actual Damages

Courts assess damages at their discretion. *But see* UTSA § 3 commentary at 459 (1990) (stating that trial court has discretion to award up to twice the amount of actual damages and will not be reversed unless clearly erroneous). Courts classify the damages attributable to unfair competition, loss of goodwill, damage to reputation, and the like as unliquidated and calculate theses damages based on the evidence presented on the business' prior experience and industry knowledge. To determine what the trade secret owner's financial position would have been absent the misappropriation, courts look to the following: (a) trade secret owner's business records prior to and after the misappropriation; (b) experience of comparable businesses not otherwise affected by the misappropriation; or (c) expert opinion based on either. Although it may not be possible to make such estimates with any degree of precision, courts cannot base damages on guess, speculation, or conjecture. However, the owner's inability to prove actual damages does not preclude recovery in an accounting of profits realized from the misappropriator's unlawful sales.

Ordinarily the burden is on the trade secret owner, as plaintiff, to prove the amount of actual damages or unjust enrichment. *See Weight Watchers Int'l v. Stouffer Corp.,* 744 F. Supp. 1259, 1288 (S.D.N.Y. 1990) (requiring plaintiff to prove defendant's sales). However, when sales information is under the control of the misappropriator, the burden is shifted to the misappropriator, as defendant, to prove the sales amounts. *See Wesco Mfg., Inc. v. Tropical Attractions of Palm Beach, Inc.,* 5 U.S.P.Q.2d 1190, 1192 (11th Cir. 1987). A misappropriator may be accountable for profits even though the trade secret owner was not doing business in a particular market, particularly if the misappropriator, by his act, prevented the trade secret owner from competing in that market.

b. Deductions

Generally, courts require the misappropriator to account for net profits, which are the difference between gross income and the costs properly incurred in generating that gross income. Once the trade secret owner demonstrates the amount of gross profits, courts assume those profits are the result misappropriator's activity. The misappropriator then bears the burden of showing which portion of the profits is not attributable to the misappropriation.

For each particular cost or expense deducted from the wrongdoer's net profits, the misappropriator must prove (a) it was paid and (b) it is attributable to the unlawful sales. Allowable deductions may include the actual cost of materials, services, and labor incurred in producing the goods, reasonable waste, certain taxes, insurance premiums, building repairs, depreciation, allocated percentages of overhead costs, and promotion and advertising costs. The cost of defending the suit is not deductible.

VIII.

FEDERAL PROTECTION OF TRADE SECRETS: UNDERSTANDING THE ECONOMIC ESPIONAGE ACT OF 1996

The Economic Espionage Act of 1996 ("EEA"), Pub. L. No. 104-294, §§ 1831-1839, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839), gained considerable media attention when it was enacted on October 11, 1996. The EEA's potentially severe criminal penalties — imprisonment for up to 15 years and fines of up to $500,000 for individuals and $10 million for corporations or organizations — and several high-profile FBI sting operations leading to federal prosecutions under the EEA focused the business community's attention on both the new law and on trade secret protection in general. In recent years, the media seems to have lost interest in the EEA, and the law has simply become another weapon in the arsenal available to prosecutors attempting to stop commercial piracy. Accordingly, many people may have heard of

the EEA, but are unclear as to its scope, purpose and practical application. This chapter will: (1) provide an overview of traditional trade secret law; (2) describe the EEA's legislative background; (3) analyze the specific provisions of the EEA; and (4) provide guidance to individuals and companies regarding issues likely to arise in connection with the application of the EEA to a specific instance of actual or suspected trade secret misappropriation.

A. Trade Secret Law: An Overview

The common law and non-federal statutory underpinnings of trade secret law are important to any discussion of the EEA, for the EEA does not preempt but rather presumes and builds upon the law of trade secrets as it developed in the states. 18 U.S.C. § 1838. Accordingly, a brief overview of classical trade secret law is the first step in understanding the EEA.

1. Common Law

The use and protection of trade secrets was traditionally governed by common law. Under the common law, a trade secret is defined as any information not generally known or readily ascertainable through proper means, developed at the claimant's expense, which provides a competitive business advantage, and which the claimant attempts to keep confidential. Such information may include techniques, processes, plans and designs, compilations, policies, codes and, under certain circumstances, lists and other information about customers.

2. Restatement of Torts

The Restatement of Torts, first published in 1939, attempted to summarize the trade secret concepts that evolved from the common law. Comment b to Section 757 of the Restatement identified the following factors as relevant to a determination of whether one's information constitutes a trade secret:

> (1) the extent to which the information is known outside of his business;

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

(3) the extent of measures taken to guard the secrecy of the information;

(4) the value of the information to him and to his competitors;

(5) the amount of effort or money expended by him in developing the information; and

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

These factors have been cited by courts in most states, and continue to inform disputes over the disposition of alleged trade secrets.

3. Uniform Trade Secrets Act

Since its initial proposal in 1979, the Uniform Trade Secrets Act ("UTSA") has been adopted, sometimes with slight modification, by over 40 states and the District of Columbia. The UTSA's uniform definition of trade secret is as follows:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> > (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

As the Judiciary Committee's September 16, 1996 Report to the House of Representatives notes, the EEA's definition of "trade secrets" is "based largely on the definition of that term in the Uniform Trade Secrets Act." As discussed below, the EEA's definition of trade secrets varies from the UTSA definition in several respects; however, the UTSA definition (which the Judiciary Committee also stated should "be read broadly"), along with the common law trade secret concepts discussed above, supplies the legal context within which the EEA was drafted.

Historically, federal law has protected intellectual property through patent and copyright laws, but no federal statutes provided similar protection for trade secrets. The EEA now extends federal protection to trade secret rights, recognizing that intangible assets are enormously valuable to American businesses, and that the value of such assets depends upon their secrecy.

B. Legislative Background of the Economic Espionage Act

Congress began seriously considering the issue of foreign economic espionage during the early-1990s. By 1994, the Government Accounting Office had characterized foreign economic espionage as a "real and growing problem," and in May of 1994, the newly created National Counterintelligence Center was charged with, among other things, reporting to Congress on foreign economic intelligence gathering activities.

In January of 1996, then-Senator William Cohen introduced a bill creating a specific criminal offense for engaging in foreign state-sponsored economic espionage. On February 10, 1996, legislation sponsored by Senator Jon Kyl requiring the Executive Branch to develop a national policy to protect the "national information infrastructure" against foreign intelligence

and economic espionage agents became law when the President signed the Defense Authorization Act.

Also in February of 1996, Senators Arlen Specter and Herb Kohl introduced bills requiring stiff jail terms and financial penalties for individuals and/or corporations engaged in the theft of proprietary economic information from a U.S. owner for the benefit of a foreign government or corporation. Congressional hearings on the Senate bills established a growing threat of foreign economic espionage resulting in potential losses for American industry totaling as much as $63 billion per year. Notwithstanding that threat, federal prosecutors lacked appropriate criminal statutes to investigate and prosecute the theft of proprietary information; instead, they relied primarily upon decades-old statutes intended to prevent the movement of stolen property across State lines, and wire and mail fraud laws.

On June 26, 1996, Congressman Bill McCollum introduced the Industrial Espionage Act of 1996, the bill that would eventually become the EEA. Consistent with the prevailing anxiety over foreign economic espionage, Congressman McCollum's bill criminalized such activity, but the bill also applied to domestic theft of trade secrets. A legislative compromise led to the foreign and domestic provisions being split into two sections (what are now sections 1831 and 1832 of the EEA); however, the definitions and other provisions of the bill are unified and equally applicable to foreign and domestic misappropriation of proprietary information.

Congress's desire to bolster trade secret protection is warranted, for intellectual capital and the intangible assets of knowledge, skill and information are arguably the most valuable resources in today's economy, exceeding by many times the value of physical assets appearing on a company's balance sheet. Converting individuals' intellectual capital into structural assets such as formalized procedures, information systems and customized applications creates a type of property with enormous actual or potential value that, if not legally protected, can easily be taken, copied or communicated to others. Given the importance of these proprietary assets in the new economy, legislators have good

reason to enact specific legal protection against theft of trade secrets.

C. Analysis of the Economic Espionage Act

1. Definition of "Trade Secret" Under the EEA

The EEA defines "trade secret" as:

> 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 memorized physically, electronically, graphically, photographically, or in writing if –
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) 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). The three irreducible elements of the EEA's definition of "trade secret" may thus be summarized as follows. The information: (1) must belong to the general class of information that bears "trade secret" characteristics; (2) must be guarded through "reasonable measures" designed to keep the information secret; and (3) must derive independent economic

value through not being known or readily ascertainable through proper means by others.

a. Types of Trade Secrets

Although the legislative history expresses Congress's intent to define "trade secret" in a way that tracks the Uniform Trade Secrets Act definition of "trade secret," the EEA definition is actually broader than the UTSA definition in several respects.

i. *The EEA Expands the UTSA's List of Representative Trade Secrets*

The UTSA definition of trade secrets contains a representative list of potential categories of trade secrets as information, "including a formula, pattern, compilation, program, device, method, technique, or process" that otherwise satisfies trade secret criteria. The EEA expands the UTSA's list of representative trade secrets by adding "all forms and types of financial, business, scientific, technical, economic, or engineering information," including plans, formulas, designs, prototypes, procedures, programs, or codes. 18 U.S.C. § 1839(3).

This statutory definition will likely be interpreted in light of existing trade secret principles; however, Congress's enumeration of additional representative categories of trade secret information provides a number of new statutory bases upon which an EEA prosecution may proceed.

In addition to expanding the UTSA's list of representative categories of trade secrets, the EEA casts a very broad net in terms of the *type* of information that is protected by federal criminal law. Currently, twenty-five states have criminal statutes relating to misappropriation of trade secrets.[13] For the most part, those state

[13]The states and territories that have criminal statutes relating to theft of trade secrets are: Alabama, Arkansas, California, Colorado, Florida, Georgia, Illinois, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, New Mexico, New York, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Virgin Islands,

criminal statutes apply only to theft of scientific and technical information.[14] The EEA, by contrast, also prohibits the misappropriation of financial, business and economic information, providing considerably broader federal protection of trade secrets than that afforded by most state criminal statutes.

ii. *The EEA Expressly Protects Intangible Information*

Whereas the UTSA does not expressly include intangible information, such as "know-how" or "negative know-how,"[15] in its definition of trade secret, the EEA does expressly protect such information. 18 U.S.C. § 1839(3). While intangible information has traditionally been afforded protection by courts under the UTSA, the EEA's explicit codification of such protection represents another subtle extension of state trade secret laws.

iii. *The EEA Protects Information Existing In Any Form Without Regard to the Means by Which It Is Stored*

Whereas the UTSA is silent on the issue, the EEA expressly extends federal protection of trade secrets to information in any form, "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." 18 U.S.C. § 1839(3). That language is significant because it demonstrates Congress's appreciation that certain information is valuable and worthy of protection whether or not it has been memorialized or otherwise

---

Wisconsin and Wyoming.

[14]As representative examples, the criminal statutes of New Jersey, Ohio, Pennsylvania and Texas relating to theft of trade secrets are all applicable only to misappropriated technical and scientific information. Florida is one of the few states whose criminal statute defines "trade secret" so as to include "commercial" information.

[15]"Negative know-how" refers to the knowledge of what does *not* serve to advance a business goal.

reduced to a tangible record capable of being physically stored or transmitted. The EEA therefore protects trade secrets that "exist" only in the mind, and prohibits the misappropriation of such information through memorization.

b. Trade Secrets Must Be Protected by "Reasonable Measures"

Much of the early commentary on the EEA has focused on the law's requirement that the owner of proprietary economic information take "reasonable measures" (an undefined phrase) to protect the secrecy of such information in order to obtain the protections of the EEA. 18 U.S.C. § 1839(3)(A). Some have suggested that the only way a business can be sure its trade secrets are protected under the EEA is to adopt every possible means of guarding the secrecy of such information.

In its Report to the House of Representatives, the Judiciary Committee took pains to discourage this extreme construction of the "reasonable measures" requirement, stating: "The fact that the owner did not exhaust every conceivable means by which the information could be kept secure does not mean that the information does not satisfy this requirement. Rather, a determination of the 'reasonableness' of the steps taken by the owner to keep the information secret will vary from case to case and be dependent upon the nature of the information in question."

In civil litigation, parties seeking judicial protection of trade secrets are generally expected to guard the secrecy of such information through means commensurate with the information's estimated value. Businesses may take any number of steps to protect proprietary economic information, including the use of nondisclosure and confidentiality agreements; covenants not to compete; employee and visitor access controls; computer passwords and firewalls; implementation of document protection and retention policies; vigilant training concerning the importance of confidentiality; and exit interviews during which departing employees are reminded of their continuing duties with respect to the use and/or disclosure of confidential information. Whether any combination of these measures will be deemed "reasonable" as a

means of protecting certain confidential information will depend upon the value and competitive sensitivity of the information, the nature of the threat of disclosure, and the relative cost of implementing particular security measures. It is clear, however, that the EEA establishes a fact-based test of reasonableness, and not an inflexible rule requiring maximum security.

In *U.S. v. Krumrei*, 2001 WL 837939 (6th Cir., July 26, 2001), the U.S. Court of Appeals for the Sixth Circuit rejected a constitutional challenge to the EEA. The defendant agreed that because the phrase "reasonable measures" is an elastic concept, the EEA's definition of trade secret is unconstitutionally vague, and does not allow defendants to adequately assess what constitutes a "trade secret." The court explained that the EEA is not unconstitutionally vague merely because it invokes the "reasonable" standard, and in the particular facts of that case, the defendant was well aware that he was attempting to sell confidential information to which he had no claim.

c. Trade Secrets Derive Value Through Not Being Known or Readily Ascertainable by Others

Under the UTSA, confidential information constitutes a trade secret if, among other things, it derives value by virtue of its not being known to, or readily ascertainable through proper means by, "other persons who can obtain economic value from its disclosure or use," i.e., competitors in the marketplace. By contrast, the EEA prescribes a larger universe of persons whose ignorance of certain information may result in that information acquiring trade secret status.

The EEA defines trade secret information as that which derives value by virtue of its not being known to, or readily ascertainable by, "the public." 18 U.S.C. § 1839(3)(B). Of course, it will generally be easier to demonstrate that "the public" lacks knowledge of certain valuable information than it is to prove that one's competitors lack such knowledge; by definition, one's competitors would be expected to possess knowledge about alleged

trade secrets with respect to which "the public" is utterly ignorant.

On its face, this change may appear to increase the amount of information that constitutes trade secrets under the EEA; however, Congress apparently did not intend to make such a radical change by this language, and it is likely that courts will continue to view the universe of relevant persons who can obtain economic value through the use or disclosure of confidential information as those having an economic interest in obtaining such information, i.e., competitors.

2. Conduct Prohibited by the EEA

The EEA contains two operative sections describing the conduct that is prohibited by the law. Section 1831 applies to actors engaged in foreign economic espionage, and requires that the theft of trade secrets benefit a foreign government, instrumentality or agent. Section 1832 is a general criminal trade secrets statute, applicable to anyone engaged in the common misappropriation of trade secrets.

While sections 1831 and 1832 are directed at different actors, the provisions contain identical language regarding the theft or misappropriation of trade secrets. Both sections punish one who knowingly:

(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), and one or more of such persons do any act to effect the object of the conspiracy.

18 U.S.C. §§ 1831(a) and 1832(a). The EEA's prohibited acts thus include (1) theft or misappropriation of trade secrets, (2) receipt of misappropriated trade secrets, and (3) conspiracy to misappropriate trade secrets. The territorial scope of the EEA is very virtually limitless: it criminalizes both acts conducted within the United States and foreign acts, provided the actor is a United States resident or any "act in furtherance of the offense was committed in the United States." 18 U.S.C. § 1837(1)-(2).

3. Some Possible Ambiguities

a. Reverse Engineering

Subsections 1831(a)(2) and 1832(a)(2) prohibit, among other things, the copying, duplication, replication, sketching, altering and drawing of trade secrets. By their terms, these subsections arguably reach reverse engineering activity that traditionally has not been proscribed by civil trade secret laws. For example, reverse engineering of computer programs, chemical products and mechanical devices will, in many cases, involve replication, sketching, altering and other activities that may fit within the range of conduct expressly prohibited by subsections 1831(a)(2) and 1832(a)(2).

The EEA does not directly address reverse engineering, but the legislative history indicates that legitimate reverse engineering is not within the scope of the Act: "If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent, or this law, then that form of 'reverse engineering' should be fine." 142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl).

b. The EEA Only Protects Trade Secrets Related to Products Produced for or Sold in Interstate/Foreign Commerce

Section 1832 criminalizes the theft of trade secrets that are "related to or included in a product that is produced for or placed in interstate or foreign commerce. . . ." 18 U.S.C. § 1832(a). Accordingly, the EEA appears to contain two enforcement gaps not found in civil trade secrets law. First, if the stolen trade secret relates to a service, rather than a product, the EEA may be inapplicable. Second, if the stolen trade secret relates to a product that is still being developed or is otherwise in a "pre-launch" stage, the protections of the EEA may be unavailable because the product is not yet actually "in interstate or foreign commerce."

c. Criminal State of Mind

Under section 1831, an individual must act with the intent or knowledge that his theft of trade secrets will benefit any foreign government, instrumententality or agent, in order to be liable under the EEA. The foreign economic espionage section is therefore broad enough to include the acts of individuals who do not act with the "intent to benefit" a foreign government, so long as they know or have reason to know that their activities will benefit a foreign government. However, section 1831 is narrowed by its requirement that the actor intend or know that his theft of trade secrets will benefit only foreign *governments*, as opposed to foreign corporations.

Because of its emphasis on domestic misappropriation of trade secrets, section 1832 (domestic misappropriation of trade secrets) does not share the government/corporation distinction embodied in section 1831 (foreign economic espionage). However, section 1832 is applicable only to those who act "with intent to convert a trade secret." Therefore, the EEA arguably does not protect against disgruntled employees or former employees, or to computer hackers, who act out of ill-will, perverse satisfaction, or for some other non-commercial purpose.

d. Criminal Penalties

i. *Fines and Prison Terms*

Individuals who violate section 1832 (domestic misappropriation of trade secrets) face penalties of up to ten (10) years in prison and unspecified fines.[16] 18 U.S.C. § 1832(a). Corporations or other organizations that violate section 1832 may be fined up to $5 million. The penalties for engaging in foreign economic espionage in violation of section 1831(foreign economic espionage) are even greater: the maximum organizational fine is increased to $10 million and the maximum prison term is raised to fifteen (15) years.

ii. *Criminal Forfeiture*

Section 1834 of the EEA provides for forfeiture of a defendant's property during sentencing. The types of property subject to the forfeiture provision include: (1) property obtained directly or indirectly as a result of the actor's criminal violation, 18 U.S.C. § 1834(a)(1); and (2) property that was used or intended to be used to commit the criminal violation. 18 U.S.C. § 1834(a)(2). Curiously, the proceeds of a defendant's criminal activity are forfeited to the United States rather than, as would seem more appropriate, to the victim of the crime. 18 U.S.C. § 1834(a). (However, victims may seek restitution from the United States.)

D. Handling an Economic Espionage Act Violation

The EEA is a federal criminal statute. As such, it is enforced by the United States Department of Justice and its United States Attorneys' offices located in each federal judicial district

[16]The general maximum fine for felonies is $250,000. 18 U.S.C. § 3571(b)(3).

across the country.[17] *The EEA does not provide for a private civil right of action.* Accordingly, a victim of trade secret theft seeking redress must persuade the federal prosecutor in its judicial district that the particular case is worthy of prosecution. Scarce resources have led many United States Attorneys' offices to establish monetary thresholds ($100,000 or more) for prosecution in cases involving white collar criminal activity. Prosecutors will likely be more inclined to prosecute trade secret misappropriation involving scientific and technical information than business information (which is harder to value), and where there is independent evidence of misappropriation and criminal intent. Prompt reporting of the misappropriation is crucial, as it demonstrates a sense of urgency and reduces the defendant's ability to argue that he obtained the trade secret through reverse engineering or parallel development.

In making a referral to the federal prosecutor, it is advisable to describe with maximum specificity exactly what was taken and its approximate value. The trade secret owner should also be prepared to articulate how it has taken reasonable steps to protect the misappropriated information, and to disclose any negative or embarrassing information concerning the matter. The victim's outside counsel should be an integral part of the referral decision and process, particularly if parallel civil proceedings are contemplated.

The benefits of criminal referral include cost savings (since the government will incur all direct investigation and litigation costs), swift justice, and the message that the trade secret owner sends to its competitors and to the public regarding its willingness to vigilantly protect its valuable proprietary information.

---

[17]Attorney General Reno issued an internal rule providing that the United States may not file charges under the EEA, or use a violation of the EEA as a predicate offense under any other law, "without the personal approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General in charge of the Criminal Division. The rule is effective for a period of five years from the enactment of the EEA, or until October 11, 2001. 62 Fed. Reg. 63,453 (Dec. 1, 1997) (codified at 28 C.F.R. § 0.64-5).

However, trade secret owners should also weigh the risks of criminal referral. Once the case is in the prosecutors' hands, the trade secret owner has relinquished full control of the litigation process, including settlement. Moreover, victims of trade secret theft should consider the impact that a criminal proceeding will have upon any parallel civil action. Should the defendant invoke his Fifth Amendment right against self-incrimination in the criminal case, discovery in the civil lawsuit could grind to a halt, effectively staying the case and delaying the entry of injunctive relief or an award of damages. However, pursuant to section 1836 of the EEA, the government may seek appropriate injunctive relief from a United States District Court against any violation of the EEA. 18 U.S.C. § 1836.

In addition, there is a risk that the victim's confidential information will become public during the course of the criminal proceeding. Pursuant to section 1835, courts must enter confidentiality orders and take other action as may be necessary to preserve the confidentiality of trade secrets (consistent with the Federal Rules of Evidence, the Federal Rules of Criminal Procedure and other applicable laws), and it is expected that prosecutors will routinely invoke section 1835 to protect the secrecy of confidential information and trade secrets. However, persons or firms who view trade secrets as the lifeblood of their commercial activities should consider that even the requirements of section 1835 and the advocacy of an aggressive prosecutor will not necessarily protect their sensitive information from disclosure during a criminal trial.

In *U.S. v. Kai-Lo-Hsu*, 982 F. Supp. 1022 (E.D. Pa. 1997), a case involving defendants who attempted to purchase the formulae and processes for the manufacture Bristol-Myers Squibb Company's anti-cancer drug, Taxol, the United States unsuccessfully sought a strong protective order pursuant to section 1835. The protective order sought by the government would have prevented the defendants from reviewing Bristol-Myers' Taxol technology for any reason. The court rejected the government's request (but entered a less restrictive protective ordered that permitted the defendants, their attorneys, outside experts and prospective witnesses to review Bristol-Myers' confidential

information) because: (1) permitting the government to protect all such information would effectively relieve the prosecution of the burden of proving before the jury one of the essential elements of its case, the existence of a trade secret; (2) restricting the defendants' access to the confidential documents would interfere with their Sixth Amendment right to cross-examination at trial; and (3) the defendants needed to have the exact processes and formulae for Taxol in order to develop their defense that the alleged trade secrets were actually available through technical journals and other publications. The court also rejected the prosecution's argument that it needed full protection in order to prevent defendants from "graymailing" the government by threatening to disclose Bristol-Myers' sensitive information unless the government dropped its charges, stating that such activity would be subject to the court's contempt power. (However, the court also noted, somewhat helplessly, that the defendants were linked to foreign wrongdoers "far removed from the borders of our contempt power.") The district court's decision was overturned on interlocutory appeal. *See United States v. Kai-Lo Hsu*, 155 F.3d 189 (3d Cir. 1998).

E. CONCLUSION

The Economic Espionage Act of 1996 is a significant development in the law of intellectual property, as Congress has now extended meaningful federal protection to another form of proprietary economic information — trade secrets. In light of the new legislation, trade secret owners and those engaged in competitive intelligence may wish to review their procedures regarding the treatment of commercially valuable confidential information. Careful and effective use of the EEA by federal prosecutors should contribute to the vitality of America's increasingly information-based economy.

APPENDIX A

States Adopting Uniform Trade Secrets Act

The UTSA, with modifications which vary from state to state, has been adopted in the following states:[18]

- Alabama Code 1975, §§ 8-27-1 to -6 (effective August 1 2, 1987)
- Alaska Statutes §§ 45.50.910 to .945 (effective September 2, 1988)
- Arizona Revised Statutes §§ 44-401 to -407 (effective April 11, 1990)
- Arkansas Statutes Annotated §§ 4-75-601 to 4-75-607 (effective March 12, 1981)
- California Civil Code §§ 3426 to 3426.10 (effective January 1, 1985)
- Colorado Revised Statutes §§ 7-74-101 to -110
- Connecticut General Statutes §§ 35-50 to -58 (approved June 23, 1983)
- Delaware Code Annotated tit. 6, §§ 2001-09 (effective April 15, 1982)
- District of Columbia Code 1981, §§ 48-501 to -510 (effective March 16, 1989)
- Florida Statutes §§ 688.001 to .009 (effective October 1, 1988)

---

[18] *See* Melvin F. Jager, TRADE SECRETS LAW, Appendix A2 (Clark Boardman Callaghan, 1994).

- Georgia Code Annotated 1981, §§ 10-1-760 to -767 (effective July 1, 1990) (1991 Supp.)
- Hawaii Revised Statutes §§ 482B-1 to 482B-9 (effective July 1, 1989)
- Idaho Code §§ 48-801 to -807
- Illinois Compiled Statutes Annotated §§ 765 ILCS 1065/ 1 to 1065/9 (effective January 1, 1988)
- Indiana Code §§ 24-2-3-1 to -2-3-8 (effective September 1, 1982)
- Iowa Code Annotated §§ 550.1 to 550.8 (effective April 27, 1990)
- Kansas Statutes Annotated §§ 60-3320 to -3330 (effective July 1, 1981)
- Kentucky Revised Statutes §§ 365.880 to 365.900 (effective April 6, 1990)
- Louisiana Revised States §§ 51:1431 to :1439 (approved July 19, 1981)
- Maine Revised Statutes Annotated tit. 10, §§ 1541 to1548 (effective May 22, 1987)
- Maryland Commercial Law Code §§ 11-1201 to -1209 (effective July 1, 1989)
- Minnesota Statutes §§ 325C.01 to .08 (effective January 1, 1981)
- Mississippi Code 1972, §§ 75-26-1 to -26-19 (effective July 1, 1990)
- Montana Code Annotated §§ 30-14-401 to -409 (effective October 1, 1985)

- Nebraska Revised Statutes §§ 87-501 to -507 (effective July 7, 1988)
- Nevada Revised Statutes §§ 600A.010 to .100 (effective July 1, 1987)
- New Hampshire Revised Statutes Annotated §§ 350-B:1to -B:9 (effective January 1, 1990)
- New Mexico Statutes Annotated 1978, §§ 57-3A-1 to -3A-7 (effective April 3, 1989)
- North Carolina General Statutes §§ 66-152 to 66-157
- North Dakota Century Code §§ 47-25.101 to -08 (effective July 1, 1983)
- Oklahoma Statutes tit. 78, §§ 85 to 95 (effective November 1, 1986)
- Oregon Revised Statutes §§ 646.461 to .475 (effective January 1, 1988)
- Rhode Island General Laws ch. 41, §§ 6-41-1 to -41-11 (effective July 1, 1986)
- South Carolina Code tit. 39, ch. 8, §§ 39-8-1 to 39-8-9 (effective June 15, 1992)
- South Dakota Consolidated Laws §§ 37-29-1 to -29-11 (effective July 1, 1988)
- Texas (Vernon's Texas Business and Commercial Code tit. 2, ch. 15E, §§ 15.50-15.51 (effective 8/28/89))
- Utah Code Annotated 1953, §§ 13-24-1 to -24-9 (effective May 1, 1989)
- Virginia Statutes §§ 59.1-336 to -343 (effective July 1, 1986)

- Washington Revised Code §§ 19.108.010 to .108.940 (effective January 1, 1982)
- West Virginia Code §§ 47-22-1 to -22-10 (effective July 1, 1986)
- Wisconsin Statutes §§ 134.90; 893.51(2) (effective April 24, 1986)

APPENDIX B

Exit Interview Sample Forms

Employee Exit Interview Checklist

Employee _____

File Number _____

Interviewer _____

Date of Termination _____

Yes/No

_____ 1. Did employee attend the interview?
If yes, was the employee hostile or did the employee make any adverse comments?

_____ 2. Were all secrecy provisions of the employment agreement and corporate trade secret policy reviewed?

_____ 3. Any comments by employee? If yes, set forth on reverse side.

_____ 4. Does employee have any corporate documents, software, material, hardware, etc. at home or elsewhere outside of the office?
If yes, detail the items and how and when they will be returned.

_____ 5. Did employee mention the name of any attorney or future employer?
If yes, please identify:

_____ 6.Were the materials returned by the employee inspected? If yes, set forth what was taken, the location from which documents were taken, who

conducted the inspection, the circumstances of the escort where applicable, and all other relevant details.

_____ 7. Obtain address to which the employee's personal mail and outstanding pay and commission checks should be forwarded.

Date_____ Signature of Inspector_____

Date_____ Signature of Interviewer_____

Acknowledgment of Exit Interview

I [name of employee] acknowledge that the undersigned representative of [name of company] has conducted an exit interview with me.

At this interview, my employment obligations to protect the trade secrets and to refrain from soliciting customers of [name of company] as set forth in my employment agreement were reviewed.

I acknowledge that I have been privy to [name of company]'s trade secrets and confidential information during my employment and that if I have any doubt as to whether a particular item of information is considered by [name of company] to be a trade secret, I will treat it as a trade secret.

I further acknowledge that I have returned confidential information and all trade secret material that I obtained during my employment with [name of company] that I may have had at my home or elsewhere, including any and all copies thereof.

Date_____ Employee _____
Date_____ [Name of company] _____

_____
[Name of individual representative and job title]

WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Avenue, N.W.
Washington, D.C. 20036
(202) 588-0302
www.wlf.org

WLF'S LEGAL STUDIES DIVISION

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by producing and distributing substantive, credible publications targeted at educating policy makers, the media, and other key legal policy outlets.

WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other policy centers.

First, the Division deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to: federal and state judges and their clerks; members of the United States Congress and their legal staffs; Government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life--from law students and professors to federal judges and senior partners in established law firms--in its work.

The key to WLF's Legal Studies publications is the production of a variety of readable and challenging commentaries with a distinctly common sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. Each piece is written to reach an intelligent reader who has no use for academic jargon. The publication formats include the provocative *Counsel's Advisory*, compact and succinct *Legal Opinion Letters*, concise *Legal Backgrounders*, in-depth *Working Papers*, legal outline-length *Contemporary Legal Notes*, law review-length Monographs, and occasional books.

WASHINGTON LEGAL FOUNDATION

The Washington Legal Foundation was established in 1977 as a nonpartisan public interest law institution organized to engage in litigation and the administrative process in matters affecting the broad public interest. An independent, nationwide corporation not associated or affiliated with any other organization, the Foundation devotes a substantial portion of its resources to defending individual rights, challenging regulations which impede economic security, and to working with our friends in government and our legal system to maintain balance in the Courts and help strengthen America's free enterprise system.

The Foundation is classified as a Section 501(c)(3) organization under the Internal Revenue Code of 1954. Individuals, corporations, companies, associations, and foundations are eligible to support the work of the Foundation through tax-deductible gifts. Background material will be provided to substantiate tax-deductibility. The Foundation neither solicits nor accepts government funding or court-awarded (taxpayers') fees for its operation.

To receive information about previous Washington Legal Foundation publications, contact Glenn G. Lammi, Chief Counsel, Legal Studies Division. Materials concerning WLF's other legal programs and activities may be obtained by contacting Daniel J. Popeo, Chairman, Washington Legal Foundation, 2009 Massachusetts Avenue, N.W., Washington, D.C. 20036.

WLF PUBLICATIONS AVAILABLE ON LEXIS/NEXIS®

Washington Legal Foundation on the World Wide Web:

http://www.wlf.org

WLF PUBLICATIONS AVAILABLE ON LEXIS/NEXIS®