The Importance of State Trade Secret Laws in Deterring Trade Secret Espionage

Carl Pacini
Penn State University

Raymond Placid
Florida Gulf Coast University

Follow this and additional works at: https://digitalcommons.law.buffalo.edu/buffaloipjournal

Part of the Intellectual Property Law Commons, and the Litigation Commons

Recommended Citation
Available at: https://digitalcommons.law.buffalo.edu/buffaloipjournal/vol7/iss1/4

This Article is brought to you for free and open access by the Law Journals at Digital Commons @ University at Buffalo School of Law. It has been accepted for inclusion in Buffalo Intellectual Property Law Journal by an authorized editor of Digital Commons @ University at Buffalo School of Law. For more information, please contact lawscholar@buffalo.edu.
THE IMPORTANCE OF STATE TRADE SECRET LAWS IN DETERRING TRADE SECRET ESPIONAGE

CARL PACINI† AND RAYMOND PLACID‡‡

I. INTRODUCTION ................................................................. 102
II. DEFINITION OF A TRADE SECRET ........................................ 104
III. REASONABLE EFFORTS TO PROTECT A TRADE SECRET ......... 107
IV. INDEPENDENT ECONOMIC VALUE ..................................... 115
V. MISAPPROPRIATION OF A TRADE SECRET ............................. 117
   A. Wrongful Acquisition .................................................. 117
   B. Wrongful Use or Disclosure ......................................... 119
   C. Espionage Techniques ................................................ 121
VI. AVAILABLE REMEDIES .................................................. 123
   A. Damages ........................................................................ 123
   B. Injunctive Relief .......................................................... 125
VII. DEFENSES TO LIABILITY ................................................ 127
VIII. INTERNAL CONTROLS TO PROTECT TRADE SECRETS ........ 128
    A. Physical Restrictions .................................................. 129
    B. Employee Restrictions and Monitoring .......................... 129
    C. Other Miscellaneous Controls ..................................... 131
IX. CONCLUSION ................................................................... 131

† Associate Professor of Accounting, Penn State University—Abington, 1600 Woodland Rd., Abington, PA. 19001.
‡‡ Associate Professor of Taxation and Business Law, Florida Gulf Coast University 10501 FGCU Blvd. S. Ft. Myers, FL 33965 Email: rplacid@fgcu.edu.
I. INTRODUCTION

On a per capita basis, American firms produce the majority of the world's intellectual property capital (i.e., patents, copyrights, and trade secrets).\(^1\) Approximately 70 percent of the market value of U.S. firms resides in their trade secrets and other intellectual property.\(^2\) Unfortunately, many firms spend insufficient sums of money to protect such property, making them vulnerable to intellectual property espionage.\(^3\) These vital assets have become the target of increased attacks by current and former employees, competitors, on-site contractors, professional spies, hackers, vendors, business intelligence consultants, and foreign governments.\(^4\)

Precise figures on the amount of trade secret espionage that occurs are not readily available. One study by PricewaterhouseCoopers, sponsored by the U.S. Chamber of Commerce and the American Society for Industrial Security, estimates that theft of intellectual property (including trade secrets), costs American firms about $59 billion per year.\(^5\) The National Counterintelligence Executive claims economic espionage could cost the nation's business community up to $250 billion per year once lost sales are taken into account.\(^6\) Another estimate places annual losses from economic espionage to be between $130 and $330 billion.\(^7\)

Trade secret espionage is practiced by both private firms and foreign governments.\(^8\) Approximately 85 percent of trade secret piracy involves current or former employees.\(^9\) The remainder involves foreign countries.

---

3. Id. at 58.
4. Id.
6. The Enemy Within, Engineer, August 9, 2002.
8. See id. Technically, "economic espionage" refers to the theft of intellectual property assets by a foreign government or an agent of a foreign government. "Industrial espionage or spying" refers to such activity when perpetrated by a domestic or foreign firm or business. We use the term "trade secret espionage" to include the theft or misappropriation of a trade secret by either a foreign government or private firm or individual. Id.
that allegedly commit trade secret piracy against American firms. Such countries purportedly include France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India, and several Scandinavian countries.10

Industries commonly targeted by espionage efforts are aerospace, pharmaceutical, defense, computer/electronics, telecommunications, energy research, financial services, manufacturing processes, and semiconductors.11 The information typically sought out by trade secret pirates include customer lists, design manuals and drawings, financial data, food and dessert recipes, product development data, strategic planning information, manufacturing cost data, formulas, testing data, marketing strategies, installation techniques, product composition, and clustering technology.12

The increase in trade secret espionage activity presents an opportunity for the legal and accounting professions, along with the business community to curb the tide of this growing financial crime. Indeed, it behooves such professionals and the business community to acquire a basic familiarity with the legal and non-legal methods to prevent trade secret espionage.

The purposes of this article are to provide an overview of trade secret law,13 an analysis of reasonable steps to preserve secrecy, an assessment of independent economic value (of trade secrets), an evaluation of misappropriation of trade secrets (including an outline of espionage techniques), an analysis of available legal remedies, a compendium of defenses to liability, and an outline of internal controls to protect an entity’s trade secrets.

---

13 The primary means of enforcement available to victims of trade secret piracy is a civil lawsuit filed under the Uniform Trade Secrets Act (U.T.S.A.) or state trade secret common law. In a civil suit for damages, a claimant must prove: (1) the existence of a trade secret; (2) reasonable steps to preserve secrecy; (3) independent economic value of the trade secret; (4) misappropriation; and (5) actual loss caused by the misappropriation. 18 U.S.C. §§ 1831-1839 (2006) (Another mode of enforcement, in some cases, is a criminal action brought by the Department of Justice under the Economic Espionage Act of 1996).
II. DEFINITION OF A TRADE SECRET

A trade secret encompasses any information that has value because it is not generally known. A trade secret must contain some element not generally known which sets it apart from that which is generally known. Furthermore, trade secret protection does not require that every component of the information in question be completely confidential.

Two or more definitions of “trade secret” exist in the law. Since trade secret protection is primarily addressed by state law, the definition in the Uniform Trade Secrets Act (U.T.S.A.) (currently adopted by 45 states, the District of Columbia, and the U.S. Virgin Islands) is most instructive:

A trade secret is 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 U.T.S.A. does not require that a trade secret be used continuously in business; a secret that has not yet been put to use still may be protected.

In the states that have not adopted the U.T.S.A., a definition of a trade secret is set forth in the Restatement (First) of Torts (Restatement):

A trade secret may consist of any formula, pattern, device, or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know how to use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device,

---

14 Michael Risch, Why Do We Have Trade Secrets? 11 MARQ. INTELL. PROP. L.J. 1, 8 (2007).
16 See id.
19 Risch, supra note 14, at 48.
or a list of customers . . . A trade secret is a process or device for continuous use in the operation of the business. 20

Key differences between the two definitions “are (a) the exception for ‘single use’ information, which can be a trade secret under the U.T.S.A.; (b) the requirement of continuous use in business, which is not necessary under the U.T.S.A.; and (c) less emphasis on efforts to maintain secrecy than under the U.T.S.A.” 21 In sum, the Restatement provides a narrower definition of a trade secret than the U.T.S.A. because it focuses upon business processes and practices actually used by a firm rather than information that could bring economic benefit to a company. 22

Another definition of “trade secret” is found in the Economic Espionage Act of 1996 (E.E.A.). 23 This law is a federal statute that criminalizes the theft of trade secrets by industrial spies and foreign governments. However, the law does not recognize a private cause of action for trade secret piracy. 24 Under this statute, the term “trade secret” includes

... 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, or codes, whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, or in writing . . . 25

There are also differences between the language of the E.E.A. and U.T.S.A. First, the list of potential types of secrets is more expansive in the E.E.A. than in the U.T.S.A. For example, the language of § 1839 of the E.E.A. makes clear that the theft of business or financial information (including perhaps some types of insider trading) falls within the ambit of the statute. 26 Second, the E.E.A. extends the definition of trade secrets to

---

20 Restatement (First) of Torts § 757, Comment b (1939).
21 Risch, supra note 14, at 8.
26 One class of insider trading cases involves persons outside the corporate organization (such as printers working for those engaged in mergers or acquisitions) who take information and trade on it. See Carpenter v. U.S., 484 U.S. 19 (1987); See Sec. & Exch.
involve information in any form "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." This language suggests that not only information stored in electronic form but also data stored in a person’s memory can be the subject of trade secret piracy. For example, in *Allen v. Johar, Inc.*, the defendant worked for Johar, Inc. as a sales manager. Johar was in the business of grinding extruded rubber into handgrips for sporting equipment, motorcycles, and tools. After working for Johar for nine years, Allen developed two grinding machines, allowing him to compete with Johar, and then contacted ten of Johar’s customers. Allen obtained the customer information based on his memory. In holding that the customer list is a trade secret, the Arkansas Supreme Court found that it is immaterial if the customer information involved was written down or memorized. Also, in *Stampede Tool Warehouse v. May*, an Illinois appellate court found that the customer list of a national distributor of auto tools is a trade secret. The court determined that a trade secret can be misappropriated by both physical copying and/or memorization. Third, the E.E.A. modifies the provision in the definition of "secret" regarding the relevant public whose knowledge is tested and changes the relevant person to "the public." However, the question under the U.T.S.A is whether one’s competitors actually knew or could easily discover the secret.

Trade secrets are both similar to and different from patents, copyrights, and trademarks in various ways. “Unlike a patent, [trade secret] information need not be unique, novel, or non-obvious to be protected. In fact, trade secret information need not even be original, allowing for the protection of such items as names and phone numbers that would not be protected under copyright.” Moreover, two or more parties who independently discover the same valuable information may both be entitled


28 Pooley et al., supra note 26, at 189.
30 Id. at 825.
31 Id.
32 Id. at 827.
34 Id. at 217.
35 Pooley et al., supra note 26, at 191.
36 Risch, supra note 14, at 12.
IMPORTANCE OF TRADE SECRET LAWS

The owner of a potential trade secret must take reasonable measures to protect it. The U.T.S.A. requires that the trade secret be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Reasonable secrecy, not absolute secrecy, is required, because:

Without [such] a rule... the amount spent by owners and takers would escalate without any corresponding social benefit. This is why absolute secrecy is not required; the cost of achieving absolute secrecy will often be so high that the value of the secret is spent on ensuring that there can be no possible accidental disclosure without any corresponding social benefit.44
Reasonable measures may be placed in two categories. The first category includes physical methods such as limited access, self-closing and self-locking doors, electrified fences, and guard dogs, and also includes virtual methods such as computer passwords, encryption, and hibernation defaults, and personnel techniques such as background checks and employee seminars.\textsuperscript{45} The second category involves precautions where secrecy is enhanced by information control. Such methods include the dissemination of information on a “need-to-know” basis, rules that restrict copying of sensitive documents, and rules that proprietary information should be stored in a fragmented manner.\textsuperscript{46}

“Reasonable efforts” are a significant component in ascertaining the availability of trade secret protection for the following reasons: the amount of effort corresponds to the value of the secret; (2) the protection is only accorded to things that would not be voluntarily or accidentally disclosed; and (3) protective effort provides evidentiary support to indicate that the information was in fact maintained as a secret, and hence, that the defendant secured the secret through improper means.\textsuperscript{47}

With regard to the first reason, the amount and cost of protective measures required “should be roughly proportional to the value of the secret to prospective appropriators.”\textsuperscript{48} A prospective appropriator will expend effort to gain a competitor’s information based upon its value. Hence, the value of the information to its owner and appropriator will determine the amount of protection required.\textsuperscript{49} Next, trade secret law balances protection of proprietary business data against disclosure of information beneficial to consumers.\textsuperscript{50} The balance struck by trade secret law is that only the most costly or evil means of unmasking a secret are prohibited.\textsuperscript{51} Third, reasonable measures taken to guard proprietary information serves as proof that such information is, in fact, a trade secret. Without protective measures, a business may not be able to prove that information is secret because it would more likely be exposed to the public.\textsuperscript{52}

\textsuperscript{45} Rodgers & Marrs, \textit{supra} note 9, at 26-27.
\textsuperscript{46} \textit{Id.} at 26.
\textsuperscript{49} Grubbs, \textit{supra} note 47, at 426.
\textsuperscript{50} \textit{Id.}
\textsuperscript{51} \textsc{Landes & Posner, supra} note 48, at 364.
\textsuperscript{52} Grubbs, \textit{supra} note 47, at 427; \textsc{U.T.S.A. § 1(4)(ii)}. 
measures indicate to all parties that the business is willing to protect its information.

Some courts and commentators consider measures to protect trade secrets the most important factor in the determination of whether a trade secret exists.\textsuperscript{53} For example, in \textit{Secure Services Technology, Inc. (SST) v. Time and Space Processing, Inc. (TSP)},\textsuperscript{54} the plaintiff SST sold TEMPEST fax machines to American NATO agencies and qualified private government contractors. Defendant TSP decided to enter the TEMPEST fax machine market which meant that TSP’s machines had to send and receive documents from other TEMPEST machines.\textsuperscript{55} TSP achieved interoperability only after the federal government provided the company with an SST fax machine.\textsuperscript{56} Plaintiff SST claimed that the fax handshake protocol was a trade secret. The district court disagreed ruled against SST, finding that the handshake protocol was not a trade secret. The district court noted that the contract for the sale of the fax machines by SST did not reserve any proprietary interest in its machines.\textsuperscript{57} In addition, contract provisions did not exist which prohibited the government from supplying the SST fax machines to third parties.\textsuperscript{58} Further, neither the fax machine nor the operator’s manual contained any restrictive or proprietary legends or any copyright notices.\textsuperscript{59} In granting the defendant’s motion for summary judgment, the district court noted that SST waived trade secret protection by its failure to protect the protocol variations.\textsuperscript{60}

Therefore, a claimant must establish the substantive steps taken to maintain the secrecy of the information that is allegedly a trade secret. The determination of what steps are reasonable under any given set of circumstances is a question of fact.\textsuperscript{61} The secrecy of the information must be maintained in perpetuity by definition; and the claimant will lose trade

\textsuperscript{53} Junkunc v. S.J. Advanced Tech. & Mfg. Corp., 498 N.E.2d 1179, 1183 (Ill. App. Ct. 1986) (the extent of measures that the trade secret claimant takes to guard the secrecy of the information is determinative of whether it is a trade secret); Chally, supra note 41, at 1284.
\textsuperscript{55} Id.
\textsuperscript{56} Id. at 1359.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{60} Id. at 1360.
\textsuperscript{61} Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 666 (4th Cir. 1993) (secrecy is a question of fact); see Injection Research H Specialists, Inc. v. Polaris Indus., L.P., 168 F.3d 1320 (Fed. Cir. Colo. 1998).
secret protection the moment of its dissemination.\textsuperscript{62} Courts assess the totality of the circumstances in order to ascertain whether the measures taken to protect the secrecy of an alleged trade secret were reasonable\textsuperscript{63} and often require measures “rigorous enough to force another to use improper means to discover the information.”\textsuperscript{64}

Factors that a court considers in the evaluation of reasonable measures to protect secrecy include, but are not limited to, the following:

- the existence or absence of a confidential disclosure or non-competition agreement [sic];
- the nature and extent of precautions taken to prevent acquisition of the information by unauthorized third parties;
- the circumstances under which the information was disclosed…;
- the degree to which the information has been placed in the public domain…; and
- how prevalent trade theft is in the industry.\textsuperscript{65}

Many businesses, including small firms, make frequent use of confidential disclosure and non-competition agreements in order to protect its secrets. A confidential disclosure agreement is an important step in protecting trade secrets against disclosure by employees, independent contractors, suppliers, customers, and other third parties. Companies usually disclose confidential information to their employees who have a need to know, however wider dissemination outside the employment relationship (without a confidential disclosure agreement) may defeat a trade secret claim.\textsuperscript{66}

In general, an employee stands in a confidential relationship with his employer with regard to the employer’s trade secrets.\textsuperscript{67} “The nature of the employment relationship imposes a duty on employees and former


\textsuperscript{63} Grubbs, \textit{supra} note 47, at 427; \textit{Secure Services Tech.}, 722 F.Supp. at 1360-61.

\textsuperscript{64} Grubbs, \textit{supra} note 47, at 427.


\textsuperscript{66} Thomas v. Union Carbide Agric. Prod. Co., 473 U.S. 568, 584 (1985); Smith v. Snap-On Tools Corp., 833 F.2d 578, 580 (5th Cir. 1987); see \textit{generally} Fin. Tech. Int’l., Inc. v. Smith, 247 F. Supp. 2d 397 (S.D.N.Y. 2002) (involving a clause in a consulting agreement prohibiting defendant independent contractor from disclosing or using for its own purposes any of plaintiff’s information which has commercial value in its business and which was not in the public domain).

employees not to use or disclose the employer’s trade secrets." The employer can fortify its claim with regard to employees and trade secrets, however, by advising employees of the existence of trade secrets and limiting their access to the information on a need-to-know basis. "The courts have been clear that this protection applies to an employer’s trade secrets even after the employee no longer works for the employer." There is a limited exception to this general rule that applies to those who have not signed an agreement not to compete. An employee who has not signed such an agreement is free upon leaving employment to engage in competitive employment. Upon leaving employment, a former employee may use general knowledge, skills, and experience acquired under his or her former employer. As one court has noted:

> Our society is extremely mobile and our free economy is based upon competition; one who has worked in a particular field cannot be compelled to erase from his mind all of the general skills, knowledge, and expertise acquired through his experience . . . Restraints cannot be lightly placed upon an employee’s right to compete in the arena of his greatest worth.  

An employer can increase the likelihood of success in a trade secret case against a former employee by using both confidentiality/non-disclosure agreements and non-compete contracts. Various court decisions "recognize the employer’s need for such agreements to promote investment, protect innovation, and promote free competition." A standard

---

68 Ed Nowogroski Ins., Inc. v. Rucker, 971 P.2d 936, 943 (Wash. 1999).
69 Cf. U.S. v. Lange, 312 F.3d 263, 266 (7th Cir. 2002) (ruling that keeping all drawings and manufacturing data in a room protected by a special lock, alarm system, and motion detector were reasonable secrecy measures).
70 Rowe, supra note 67, at 186; see also Air Prod’s. & Chems., Inc. v. Johnson, 215 U.S.P.Q. 547, 552 (Pa. Super. Ct. 1982) (a former employer can reasonably rely upon the obligation of its employees not to disclose trade secrets about which they obtained knowledge while working in an employment relationship).
71 See Nowogroski, 971 P.2d at 941; Canteen Vending Servs. v. Mfrs. & Traders Trust Co., 1998 U.S. Dist. LEXIS 7589, at *5-6 (W.D.N.Y. May 15, 1998) (acknowledging that absent an express agreement or misappropriation of trade secrets, an employee may compete with his former employer after the end of the employment relationship).
72 Cummings v. Dickson, No. EV 88-191-C, 1989 U.S. Dist. LEXIS 17121, at *13 (S.D. Ind. July 27, 1989) ("Although an employer is entitled to protect proprietary interests, she is not entitled to an employee’s use of her knowledge, skill, or general information acquired or increased through experience.").
73 Bendinger v. Marshalltown Trowel Co., 994 S.W.2d 468, 475 (Ark. 1999) (emphasis & citation omitted) (citing AMP, Inc. v. Fleischhaker, 823 F.2d 1199, 1202 (7th Cir. 1987)).
74 Rowe, supra note 67, at 188; see Ticor Title Ins. v. Cohen, 1998 U.S. Dist. LEXIS
nondisclosure or confidentiality agreement states that the employment arrangement creates a relationship of trust with regard to confidential information such as trade secrets, inventions, customer and supplier lists, etc. “Confidentiality agreements are helpful for (1) delineating the confidentiality expectations between employer and employee; (2) showing that the employer takes trade secret protection seriously; and (3) demonstrating the employer’s reasonable efforts to maintain secrecy of its confidential information.”  

Non-compete agreements bar employees from working for competitors or establishing a competing business after leaving an employer. In the majority of states, non-compete agreement enforceability depends on the satisfaction of various criteria. Such agreements: (1) must not be any broader than necessary to protect the employer’s business interests; (2) may not impose undue hardships on the employee; and (3) may not be burdensome to the public interest. However, nondisclosure/non-compete agreements are effective only if employees understand their legal obligations for the protection of trade secrets.

In some states, courts deter the disclosure of trade secrets by former employees through the application of the doctrine of inevitable disclosure. This doctrine “seeks to restrict the transfer of proprietary information through placing limitations on the subsequent professional activities of employees.” The inevitable disclosure doctrine permits courts to prohibit employees from working in other entities where the utilization of trade secrets could harm their former employer’s competitive position. In most cases, application of the inevitable disclosure doctrine requires the existence of a signed non-compete agreement. Only on rare occasions will a court enforce the doctrine in the absence of a non-compete agreement. From a public policy standpoint, the inevitable disclosure

77 Fink, supra note 15, at 231-232.
78 Fitzpatrick et al., supra note 2, at 62.
79 Id.
80 Rowe, supra note 67, at 209.
81 One of those rare occasions occurred in PepsiCo., Inc. v. Redmond, 54 F.3d 1271 (7th Cir. 1995). In that case, the Seventh Circuit Court of Appeals upheld a preliminary injunction against William Redmond, Jr., a former employee of PepsiCo., to prevent him from divulging trade secrets in his new job with Quaker Co. The injunction also prevented Redmond from temporarily going to work for Quaker. Redmond had signed a confidentiality
doctrine requires a court to balance the right of the employer to protect its trade secrets with the right of the employee to earn a living.\(^8\)

Courts also consider the nature and extent of precautions taken to prevent acquisition of information by unauthorized third parties. Still, no single step taken to maintain the secrecy of information will be determinative. If the claimant can establish a consistent approach to keeping information secret it will go a long way toward establishing reasonable precautions. These security measures include the following:

- advising employees that certain organizational information, processes, and/or technologies have been assigned a trade secret designation;
- limiting trade secret access to those persons with a legitimate need to know;
- requiring persons with access to trade secrets to sign confidentiality agreements;
- installing a variety of electro-mechanical and other physical security devices (e.g., locked cabinets, safes, alarms, electronic sensors, security personnel, etc.);
- conspicuously marking proprietary information as confidential; and
- developing corporate security policies which screen external speeches and publications by organizational personnel for the disclosure of trade secrets or proprietary information.\(^8\)

In support of granting a preliminary injunction without a non-compete agreement, the Circuit Court cited Redmond's specialized knowledge of PepsiCo's trade secrets, the fierce competition in the sport drink industry and lack of trust in Redmond. Some legal commentators expressed concern that this decision would lead to a windfall for employers who could benefit from ex post facto non-compete agreements without having negotiated them and prevent affected individuals from earning a livelihood. Matthew Miller, Note, Inevitable Disclosure Where No Non-Competition Agreement Exists: Additional Guidance Needed, 6 B.U. J. SCI. & TECH. L. 9, 39-40 (2000). This has not occurred because most courts require the existence of a legal non-compete agreement to issue an injunction. See Minn. Mining & Mfg. v. Francavilla, 191 F. Supp. 2d 270, 274-75, 282 (D. Conn. 2002); Lumex, Inc. v. Highsmith, 919 F. Supp. 624, 632-34 (E.D.N.Y. 1996).


\(^8\) Fitzpatrick et al., supra note 2, at 58. In Religious Technology Center, v. NetCom On-Line Communication Services, Inc., 23 F. Supp. 1231 (N.D. Cal. 1995), plaintiff sued defendant Dennis Erlich for posting trade secrets of the Church of Scientology on the Internet. Erlich, a former minister of the Church of Scientology, had access to various Scientology writings including published literary works and unpublished confidential materials. According to the plaintiff, Erlich had agreed to maintain the confidentiality of various materials (referred to as Advanced Technology works). Plaintiff argued that Erlich misappropriated trade secrets which had been the subject of elaborate security measures. Protective steps included use of locked cabinets, safes, logging and identification of the materials, availability of the materials at only a handful of global sites, electronic sensors attached to documents, locked briefcases for transporting works, alarms, photo identification, and security personnel. The district court granted a preliminary injunction.
Another factor that courts evaluate in an assessment of measures to protect secrecy is the circumstances under which the information was disclosed. Trade secret law protects the trade secret holder only if the information at issue has been obtained from the holder by means that the law deems inappropriate. Most organizational trade secrets are compromised because of the negligence or dishonesty of people.\textsuperscript{84} One team of researchers reports that about half of those surveyed viewed as appropriate the collection of competitive intelligence through hiring away key employees of competitors, posing as prospective customers, and entertaining the employees of competitors to secure trade secrets.\textsuperscript{85} In another study, a researcher documents that about fifty percent of group members showed no moral qualms in utilizing trade secrets to achieve a competitive advantage.\textsuperscript{86}

Generally, a trade secret plaintiff must demonstrate misappropriation, therefore, no presumption is made against the defendant.\textsuperscript{87} In \textit{Vermont Microsystems, Inc. v. Autodesk, Inc.},\textsuperscript{88} an ex-employee kept certain trade secrets of his employer after cessation of employment while acting as a consulting engineer independently on a software project that closely resembled the trade secrets of Vermont Microsystems (VM). Even though he failed to incorporate those secrets into the project,\textsuperscript{89} the ex-employee admitted that he developed the software using VM’s trade secrets.\textsuperscript{90} VM was able to satisfy its burden of proof because of the ex-employee’s admission.\textsuperscript{91} In general, many courts protect against trade secret misappropriation by any means deemed improper.\textsuperscript{92}

An additional factor relevant to an assessment of trade secret protection measures is the degree to which the information has been placed

\textsuperscript{84} Fitzpatrick et al., \textit{supra} note 2, at 59.
\textsuperscript{88} See Vermont Microsystems, Inc. v. Autodesk, Inc., 88 F.3d 142 (2d Cir. 1996).
\textsuperscript{89} \textit{Id.} at 144.
\textsuperscript{90} \textit{Id.} at 145-46.
\textsuperscript{91} \textit{Id.} at 146.
in the public domain or rendered readily ascertainable by third parties. This factor does not address one’s ability to access or obtain the trade secret from the holder but the likelihood that the proprietary information may be readily ascertainable from a publicly available source. For example, in Sethscot Collection Inc. v. Drbul\(^93\) an intermediate appellate court held that a retailer’s active list of customers compiled from customers who had done business with the retailer and was not available to the public, was a protected trade secret. In Picker International Corp. v. Imaging Equipment Services, Inc.\(^94\) a federal district court found diagnostic software information to be a trade secret because plaintiff did not publicly disclose such data by publishing papers, giving lectures, or providing proprietary information in government reports. In Alan Scott, D.C., P.A. v. Moses,\(^95\) a chiropractor’s patient list was deemed not to be a trade secret because the chiropractor failed to demonstrate that such list could not be obtained by other means. Also, in Leo Publications, Inc. v. Reid,\(^96\) a newspaper’s list of advertising clients was ruled not to be a trade secret because the data on the list was “readily ascertainable” through the use of proper methods and published sources.

IV. INDEPENDENT ECONOMIC VALUE

A trade secret requires proof of “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.”\(^97\) To be valuable, a trade secret must have value not only to its owner, but commercial value to competitors or others who might benefit from its use.\(^98\) Under U.T.S.A., “the definition of trade secret does not require that there currently be competitors, only that there be actual or potential value from information being secret. Thus, potential competition is sufficient.”\(^99\)

Competitors will seek the most valuable trade secrets which grant the original innovator the most extensive monopoly rights. The exclusive

---


\(^96\) 458 S.E.2d 651, 652 (Ga. 1995).


knowledge of a trade secret controlled by the initial innovator may allow that innovator to earn economic rents (i.e., excess profits). Such rents attract competitors and new market entrants to obtain the trade secret from which the innovator profits. If trade secrets did not possess economic value, "then remedies such as injunctions would impose an unjustified social cost by limiting potentially valuable information . . . from those who could use it." \(^{101}\)

The economic value the claimant must establish is objective in nature—not subjective—so the claimant is incompetent to offer any testimony on the issue. \(^{102}\) The plaintiff must submit expert testimony on this point (most likely a forensic accountant who is a business valuation expert). \(^{103}\) The expert witness must show that the value of the information is derived from the fact that it is not generally known and not readily ascertainable. \(^{104}\) Persuasive evidence of not being generally known could come from a competitor or expert in the market who testifies that the information is not generally known. \(^{105}\)

The U.T.S.A. does not prescribe the amount of independent economic value information must possess to be considered a trade secret. The court has ruled that the value need not be great. \(^{106}\) The U.T.S.A. speaks only to "economic" value, any value which is not economic and cannot be quantified is not a component of economic value. \(^{107}\) Hence, a claimant must focus less on the amount of value and more on the "kind" of value to which the U.T.S.A. speaks. \(^{108}\)

---

100 Chally, supra note 41, at 1280-81.
101 Risch, supra note 14, at 38.
102 Gaffney & Ellison, supra note 12, at 13.
103 The expert witness should be qualified under the applicable rules of evidence as a business valuation expert. The individual should possess significant knowledge and experiences in the specific industry in which the information finds its competitive advantage. The expert's opinion should be supported by substantial evidence in the form of receipts, income statements, market analyses, and other financial projections. Id. at n.36.
104 All Pro Sports Camp, Inc. v. Walt Disney Co., 727 So. 2d 363, 368 (Fla. Dist. Ct. App. 1999). The phrase "not readily ascertainable" means the trade secret claimant must establish that the information could not have been discovered by proper means. This issue is addressed infra in the section on misappropriation. Information which is commonly known within a given industry or market and not considered to be unique to the claimant will most likely be considered "generally known." Id.
107 Gaffney & Ellison, supra note 12, at 16.
108 Id. at 17. U.T.S.A. mandates that the information sought to be protected is not known to and is "not readily ascertainable" by those who might use the information for competitive
Trade secret value can be determined using three approaches: the market approach, the cost approach, and the income approach. The market approach is the most difficult to use in the valuation of a trade secret. The method involves the comparison of the sale of similar assets to what is being valued. As a trade secret is unique, finding a comparable asset is quite difficult. The cost method is better suited to the valuation of a trade secret. This technique factors in items such as the cost of replacement. It is important to know how long and how much money it took to create the trade secret. The income approach considers anticipated revenues and future economic benefits to be derived from the trade secret. Using reasonable economic models, this technique is preferable to the market approach.  

V. MISAPPROPRIATION OF A TRADE SECRET

The U.T.S.A. establishes a statutory cause of action for two different types of misappropriation—one for wrongful acquisition and a second for wrongful disclosure. The first is defined by the U.T.S.A. as the “acquisition of a trade secret of another by a person who knows or has reason to know that the secret was acquired by improper means.”

Misappropriation by wrongful disclosure is:

[D]isclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (1) derived from or through a person who has utilized improper means to acquire it: . . .

“Thus, a plaintiff can state a claim for misappropriation simply by demonstrating that the defendant acquired its trade secret by improper means, even if the plaintiff cannot show use of that trade secret.”

A. Wrongful Acquisition

Wrongful acquisition under the U.T.S.A. requires the plaintiff to demonstrate that (1) the defendant acquired the trade secret; and (2) he or she knew, or had reason to know, that the information was acquired through
“improper means.”113 Under the U.T.S.A., “improper means includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”114 Improper methods or means “constitute intentional conduct involving some sort of stealth, deception or trickery.”115 In many cases, “improper” means includes acts that are actionable in and of themselves—trespass, breach of contract, conversion of physical property, and the misuse of computer networks.”116 One court has held that improper means includes obtaining “knowledge of a process without spending the time and money to discover it independently . . . unless the holder voluntarily discloses it or fails to take reasonable precautions to ensure its secrecy.”117

The U.T.S.A.’s list of “improper means” is not exhaustive and includes a catchall for espionage. The Restatement states that “improper means” are those that fall below the generally accepted standards of commercial morality and reasonable conduct.118 The jury must determine improper means under a particular set of facts.119

The fluidity of the concept of “improper means” is illustrated by the question of whether dumpster diving—surreptitiously searching through the trash of another to discover trade secrets—constitutes improper means. The means may be improper when conversion or trespass occurs but what about discarded trash that has been removed from the owner’s property? In Tennant Co. v. Advance Machine Co.,120 a state appellate court held that an owner of trash retains a reasonable expectation of privacy in its contents until it becomes mixed with trash elsewhere. However, in Frank W. Winne

113 U.T.S.A. § 1(2)(i).
114 U.T.S.A. § 1(1).
115 Systems, 8 F. App’x at 200.
117 E.I. duPont de Nemours & Co., Inc. v. Christopher, 431 F.2d 1012, 1015-16 (5th Cir. 1970).
118 RESTATEMENT (FIRST) OF TORTS § 757, Comment f at 10 (1939). Comment 1 to section 1 of the U.T.S.A. contains a partial listing of proper means:
1. Discovery by independent invention;
2. Discovery by “reverse engineering”, that is, by starting with the known product and working backward to find the method by which it was developed;
3. Discovery under a license from the owner of the trade secret;
4. Observation of the item in public use or on public display; and
5. Obtaining the trade secret from published literature.
119 DSC Commc’ns Corp. v. Pulse Commc’ns, Inc., 170 F.3d 1354, 1364 (Fed. Cir. 1999).
IMPORTANCE OF TRADE SECRET LAWS

and Son, Inc. v. Palmer, a federal court ruled that there is no reasonable expectation of privacy in trash set out for collection.

Most trade secret misappropriation claims involving wrongful acquisition have been asserted "either against a defendant who had a confidential relationship with the trade secret owner or against a former employee who becomes hired by a competitor." Such cases involve a claim that the defendant breached a duty of secrecy or confidentiality. An employee’s "duty . . . not to disclose the secrets of his employer may arise either from an express contract, or may be implied from the confidential relationship existing between employer and employee" and an employee may not use this information to the detriment of the employer.

The trade secret claimant must demonstrate that the saboteurs were made aware that the information was secret and not to be divulged. For example, in Tedder Boat Ramp Systems, Inc. v. Hillsborough County, a federal court held that by clearly marking information given to the defendant as "confidential" the latter was made aware that the information was not to be disclosed. Also, in Aries Information Systems, Inc. v. Pacific Management Systems Corp., the Minnesota Supreme Court found that by reading and signing confidentiality agreements that employees knew they were under a duty to maintain secrecy of trade secret data.

The E.E.A. provides a more detailed list than the U.T.S.A. of acts deemed to involve wrongful acquisition. The E.E.A. sanctions one who "steals, or without authorization, appropriates, takes, carries away, or conceals, or by fraud, artifice or deception obtains [a trade secret]." Also, whenever one knowingly "receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization," he has illegally acquired the trade secret.

B. Wrongful Use or Disclosure

Wrongful use or disclosure of a trade secret under the U.T.S.A. is somewhat more complex than wrongful acquisition. The claimant must

124 54 F. Supp. 2d 1300, 1305 (M.D. Fla. 1999).
establish that the defendant actually used the trade secret or disclosed the information to another.\textsuperscript{128} The U.T.S.A. does not define the terms “use” or “disclosure” nor does the U.T.S.A. appear to require a certain level of activity to impose liability. Once the claimant establishes that the trade secret saboteur did not consent to use or disclose the trade secret he or she must establish that the defendant (1) used improper means to acquire knowledge of the trade secret; (2) knew or had reason to know that the trade secret had been obtained from one who used improper means (or breached a duty of confidentiality);\textsuperscript{129} or (3) used or disclosed accidentally acquired information and knew or had reason to know it was a trade secret.\textsuperscript{130} The U.T.S.A. does appear to create a safe harbor for defendants who accidentally obtain trade secret information but neither know nor have reason to know of its protected status or how it was acquired illicitly.

Also, any person who obtains trade secret knowledge in a confidential capacity is under an obligation not to reveal the secret or use it for his or her own advantage.\textsuperscript{131} Third parties may be held liable if they induced another to misappropriate a trade secret or knowingly or negligently acquired a trade secret from or through one who had acquired or revealed it illegally.\textsuperscript{132}

The E.E.A. defines wrongful use or acquisition more broadly than the U.T.S.A. The E.E.A. punishes one who “without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret.”\textsuperscript{133} The inclusion of transmitting and delivering will permit legal action against one who merely discloses the secret without using it.

The E.E.A.'s description of stealing and unauthorized copying of

\textsuperscript{128} Liability may not arise from every “use” of a trade secret. In some cases, the use must affect a party’s competitive market position. Omnitech Int'l, Inc. v. Clorox Co., 11 F.3d 1316, 1325 (5th Cir. 1994).
\textsuperscript{129} The U.T.S.A. provides that the claimant must show that “at the time of disclosure or use, [the defendant] knew or had reason to know that his or her knowledge of the trade secret was: (a) derived from or through a person who had utilized improper means to acquire it; (b) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (c) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.” U.T.S.A. § 1 (2)(ii)(B) (1985).
\textsuperscript{130} Gaffney & Ellison, supra note 12, at 32.
\textsuperscript{131} Healthcare Affiliated Servs., Inc. v. Lippany, 701 F .Supp. 1142 (W.D. Pa. 1988) (employment agreement whereby defendant agreed to preserve the confidentiality of employer’s techniques).
\textsuperscript{132} Saunders, supra note 122, at 147.
\textsuperscript{133} 18 U.S.C. §§ 1831 (a), 1832 (a)(2) (2006).
trade secrets covers all types of new and future technologies. The federal trade secret statute “makes it a crime to deprive the rightful owner of trade secrets in any way, as long as this creates an economic benefit for the thief or a third party. This . . . indicates that the thief or third party need not gain a direct benefit from the information as long as he gains a relative benefit by depriving the rightful owner of the information.”

E.E.A. language is not limited to secrets obtained by improper means. Even legally acquired trade secrets can be misappropriated under the E.E.A. because it serves as an incentive against waste. The E.E.A. discourages wasteful behavior and motivates the internalization of options by sanctioning punishment despite the use of legal alternatives to discover trade secrets.

One troublesome aspect of the E.E.A. is how it treats reverse engineering. While reverse engineering is not expressly prohibited under the E.E.A., it is not expressly permitted. Some types of reverse engineering, such as observing or tasting a lawfully acquired product to determine its contents, are not prohibited by the E.E.A. The legality of reverse engineering under the E.E.A. appears to be a function of whether the actor engages in any acts outlawed under the statute.

C. Espionage Techniques

Tools used in the perpetration of trade secret espionage include but are not limited to scanning trade show floors, combing through websites, eavesdropping in airline terminals and on airline flights, reviewing filings with regulatory agencies, taking photographs of factories and businesses, using data-mining software to search databases on the internet, stealing laptop computers, dumpster diving, and application of the MICES

---

135 Id. at 292-93. Harm to the original owner is important in the E.E.A., not just benefit to the thief. The issue is what the owner has lost and not only what the taker has gained. Id.
136 Risch, supra note 14, at 51.
137 Id.
138 Pooley et al., supra note 26, at 195.
principle.\textsuperscript{143} MICES is an acronym describing agent recruitment methodologies based on money, ideology, compromise, ego, and sexual entrapment.\textsuperscript{144} Money is often employed to enlist the assistance of employees in illicitly obtaining the trade secrets of firms. Individuals who are under severe financial strain are offered bribes to reveal trade secrets.\textsuperscript{145} The theft of trade secrets related to the Kodak 401 filmmaking process illustrates this espionage technique.\textsuperscript{146} The ideology aspect of MICES is applied to encourage individuals to turn over employer trade secrets due to loyalty to a foreign nationality or philosophical values that differ from those of the employer.\textsuperscript{147} Compromise techniques extort employees into betraying trade secrets by threatening to disclose personally or professionally damaging information.\textsuperscript{148} Ego techniques try to isolate employees possessing low- or bruised self-esteem or a disgruntled attitude to yield proprietary information.\textsuperscript{149} Lastly, sexual entrapment is employed to generate photographs, video recordings or sound tapes that can compel employees to disclose trade secrets through threats of blackmail or extortion.\textsuperscript{150} The application of the MICES principle costs American


\textsuperscript{144} Fitzpatrick et al., supra note 2, at 59.

\textsuperscript{145} \textit{Id.;} FINK, supra note 15, at 265-70.

\textsuperscript{146} The 401 process was a research and development program to enhance the speed and quality of film-making at Kodak. One Kodak employee, Harold Worden, possessed knowledge of the whole manufacturing process, anticipated early retirement, and had authority to recommend what aspects of the 401 technology would be patented. Before retirement, Worden used his position to secretly acquire documents outlining details of the 401 process. After departing Kodak, he sold the 401 process technology to Kodak competitors. Worden was apprehended in an FBI sting operation. In 1997, he pled guilty to selling trade secrets to Kodak officials who were working undercover, posing as Chinese agents. Having agreed to cooperate in a continuing investigation, he was able to negotiate a plea bargain that resulted in a one-year prison sentence and a $30,000 fine. Desmet, \textit{supra} note 24, at 99; Fitzpatrick et al., \textit{supra} note 2, at 59-60.

\textsuperscript{147} Fitzpatrick & Burke, \textit{supra} note 143, at 85-6.

\textsuperscript{148} \textit{Id.;} see HUGO CORNWALL, \textit{THE INDUSTRIAL ESPIONAGE HANDBOOK} (Century 1991).

\textsuperscript{149} Fitzpatrick et al., \textit{supra} note 2, at 60. A noteworthy instance involving this facet of MICES principle is \textit{United States v. Martin}, 228 F.3d 1 (1st Cir. 2000). In that case, Caryn Camp, an employee of IDEXX, Inc., stole trade secrets related to veterinary diagnostic kits. She was a disgruntled employee (eager to find a new job). In her job search, she commenced e-mail correspondence with Dr. Stephen Martin. The latter was CEO of WDV, a competitor of IDEXX. Martin reinforced Camp’s damaged ego by discussing job opportunities, the nature of her discoveries, and general corporate gossip about IDEXX. She eventually disclosed through e-mail proprietary information, software, and computer files containing IDEXX trade secrets.

\textsuperscript{150} Fitzpatrick et al., \textit{supra} note 2, at 61.
A successful trade secret claimant under the U.T.S.A. is entitled to recover damages from a misappropriation. Damages can include both the actual loss caused by the misappropriation\(^{151}\) and unjust enrichment that is not considered in computing actual loss.\(^{152}\) Punitive or exemplary damages may be awarded in some circumstances.\(^{153}\) "Recovery of actual damages is proper only for the period in which the information is entitled to trade secret protection, plus any additional period during which the defendant has a competitive advantage . . . ."\(^{154}\) An examination of authority from across the U.S. indicates that the proper method of computation is on the basis of net profit, whether lost by the injured party or gained by the wrongdoer.\(^{155}\) The trade secret claimant is entitled to that which affords greater relief.\(^{156}\) A party seeking damages must supply a reasonable basis for the computation of those damages.\(^{157}\)

The U.T.S.A. also permits recovery for unjust enrichment or the misappropriated profits, as long as the amounts are in addition to the trade secret owner's fees.\(^{158}\) Plaintiffs have been permitted to seek an accounting of the profits made by the defendant because of the wrongful appropriation.
of the trade secret and then recover such profits. Recovery of the misappropriator’s profits (or prevention of unjust enrichment) reduces the competitor’s incentive to focus more resources on appropriation. The importance of preventing unjust enrichment trade secret cases is aptly reasoned as follows:

If the competitor values the trade secret in an amount more than the owner will lose or if the court undervalues the amount of the trade secret owner’s loss, then the competitor will have an incentive to spend more on appropriation. In turn, this will cause the owner to spend more on protection than it otherwise might need to if it had the remedy, leading to the same “arms race” without a commensurate gain in expected social value.

If the facts of a case are insufficiently precise to justify a damage award based upon lost profits or unjust enrichment, then courts prefer to use the “reasonable royalty theory” for a defendant’s unauthorized disclosure or use of a trade secret. “A reasonable royalty award tries to measure a hypothetically agreed upon value of what the defendant wrongfully obtained from the plaintiff.” The court computes what the parties would have agreed to as a fair licensing price at the time the misappropriation occurred. “[M]ost courts adjust the measure of damages to accord with the commercial setting of the injury, the likely future consequences of the misappropriation, and the nature and extent of the use the defendant put the trade secret to after misappropriation.”

A court may also award “exemplary damages” under the U.T.S.A. where the misappropriation is “willful and malicious.” The amount may not exceed twice the amount of any award for actual loss or unjust enrichment. One example of “willful and malicious” behavior occurred in Smith v. Snyder. In Snyder, former employees of Lectron Corporation covertly started a competing business, used fraudulent means to misappropriate the plaintiffs’ most productive and efficient machine, discouraged the plaintiffs’ existing customers by overquoting jobs,

---

160 Risch, supra note 14, at 59.
161 Kline & Floyd, supra note 87, at 339-41.
165 Gaffney & Ellison, supra note 12, at 33.
166 839 A.2d 589 (Conn. 2004).
IMPORTANCE OF TRADE SECRET LAWS

Winter 2009

125

disrupted the plaintiffs’ cash flow by not sending out bills, and solicited the plaintiffs’ customers and diverted them to their own business venture.167 However, the defendants did not dispute the trial court’s finding that their conduct was willful and malicious, resulting in punitive damages being awarded. Another example of such conduct transpired in Boeing Co. v. Sierracin Corp.168 In that case, the trial court found that “Sierracin misappropriated Boeing’s drawings for replacement cockpit windows for Boeing 707s, 727s, and 737s.169 The trial court record indicated that Sierracin knew its actions to be of dubious legality and engaged in a massive effort to disguise its copying of Boeing’s drawings.”170 The appellate court ruled that the evidence justified the imposition of punitive damages.

B. Injunctive Relief

The U.T.S.A. authorizes a court to issue an injunction to prohibit an actual or threatened misappropriation of a trade secret.171 The usual standards for injunctive relief apply to trade secret situations. The trade secret claimant must show: (1) a likelihood of success on the merits; (2) irreparable injury; (3) such injury outweighs any harm to the defendant; and (4) the injunction would not harm the public interest.172 The first factor is often considered the most important.173 The trade secret claimant may prove a likelihood of success on the merits by establishing the existence of a trade secret and by making a prima facie case that the defendant misappropriated that trade secret.174 The second element is usually automatically satisfied because the loss of a trade secret is generally found to constitute irreparable harm.175 Also, the claimant must convince the court that the harm it will incur will outweigh any harm to the defendant if it is granted and show how the “public interest” will be served by the

167 Id. at 593.
169 Id. at 670.
170 Id. at 680.
court’s exercise of its equitable powers. One “public interest” consideration cited by some courts is the need to enforce contracts, such as non-disclosure agreements and non-compete clauses.

A court may issue an injunction to prohibit an actual or threatened misappropriation of a trade secret. The injunction should be in place for only “as long as is necessary . . . to eliminate the commercial advantage or ‘lead time’ with respect to good faith competitors that a person has obtained through misappropriation” and “should terminate when a former trade secret becomes either generally known to good faith competitors or generally knowable to them because of the lawful availability of products that can be reverse engineered to reveal a trade secret.”

Under “exceptional circumstances,” the court may condition future use of the trade secret on payment of a reasonable royalty for the time period during which the defendant’s use could have been prohibited. Under appropriate circumstances, a court may order that affirmative acts be undertaken to protect the trade secret. However, a court must terminate an injunction upon a showing that the trade secret no longer exists “but it may be continued for a ‘reasonable period of time’ to eliminate any commercial advantage which may have been derived from the misappropriation.”

A court may also enjoin threatened misappropriation of a trade secret. The U.T.S.A. does not define the term “threatened misappropriation” so it is not clear what conduct or circumstances would justify an injunction under such language. In some courts, the existence of a real and present danger of disclosure is enough. Mere suspicion of injury is not sufficient to constitute an actionable threat. The possibility of disclosure does not, by itself, rise to the level of inevitability of disclosure. In sum, “the

---

176 Am. Red Cross v. Palm Beach Blood Bank, Inc., 143 F.3d 1407, 1410 (11th Cir. 1998); Church v. City of Huntsville, 30 F.3d 1332, 1342 (11th Cir. 1994).
179 U.T.S.A. § 2 Comment.
180 U.T.S.A. § 2(b).
181 U.T.S.A. § 2(c); See also Phillips v. Corporate Express Office Prods., Inc., 800 So. 2d 618, 621 (Fla. Dist. Ct. App. 2001).
182 Gaffney & Ellison, supra note 12, at 34.
185 See FMC Corp. v. Cyprus Foote Mineral Co., 899 F. Supp. 1477, 1481 (W.D.N.C. 1995) (explaining that the “mere possibility of misappropriation” is insufficient grounds for
exact nature and duration of an [injunction] must be tailored to fit the facts of the case and that an injunction should generally be only as broad as is necessary to protect the rights of the plaintiff."186

VII. DEFENSES TO LIABILITY

One of the most popular defenses includes challenges to the trade secret plaintiff's substantive elements of proof.187 Each one of the substantive facts that the claimant offers to satisfy the elements of the U.T.S.A. should be carefully assessed, and, if required, rebuttal evidence proffered.188 The trade secret defendant should pursue factual weaknesses in any facet of the claimant's case, especially the areas of value, secrecy, and accessibility.189

Other defenses are also available. A trade secret misappropriator may avoid liability by demonstrating that the same information (as the trade secret) could have been derived by independent discovery or reverse engineering.190 Others besides the trade secret claimant are free to obtain the same data as the trade secret and use it so long as they gain their knowledge through independent efforts.191 "Reverse engineering is a method of industrial engineering in which one begins with a known finished product and works backward to divine the processes and specifications involved in the product's development and manufacture."192 It also may involve "looking at or tasting a lawfully acquired product in order to determine its content."193 Independent discovery involves the creation or discovery of a trade secret as a result of one's own effort.194

Another defense for the alleged trade secret misappropriator is the statute of limitations. Actions for trade secret misappropriation must be brought within three years "after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered."195 One

---

187 Gaffney & Ellison, supra note 12, at 37.
188 Id. at 38.
189 Id.
190 Henry Hope X-Ray Prods., Inc. v. Marron Carrel, Inc., 674 F.2d 1336, 1341 (9th Cir. 1982).
192 Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 91 F.3d 914, 917 n.3 (7th Cir. 1996).
193 Pooley et al., supra note 26, at 195.
195 U.T.S.A. § 6 (1985); See also Ashton-Tate Corp. v. Ross, 916 F.2d 516, 523-24 (9th
thorny issue here is whether or not an ongoing misappropriation constitutes a continuing wrong or a single claim. This issue is important because it either triggers the statute of limitations period or tolls the statute of limitations as long as the misappropriation continues. The U.T.S.A. states that a continuing misappropriation constitutes a single claim. Among U.T.S.A. jurisdictions, a conflict of authority exists as to whether misappropriation is a continuing wrong.

The U.T.S.A. also provides an exception to the right to sue for damages for trade secret misappropriation. A trade secret claimant is not entitled to damages if the defendant demonstrates that (1) it made a material and prejudicial change in its position prior to acquiring knowledge of the misappropriation, which has (2) rendered monetary relief inequitable.

VIII. INTERNAL CONTROLS TO PROTECT TRADE SECRETS

The key steps in the protection of trade secrets are to identify company information that may constitute a trade secret and to implement reasonable controls to ensure this information is kept confidential. "Within a very wide band of discretion, the trade secret owner must have considered the value of the secret, the nature of the threat to disclosure, and the cost of any particular security mechanism." The avoidance of significant expenditures on physical controls or security is consistent with the goal of encouraging investment in trade secret research.

The most effective way to prevent trade secret fraud and show "reasonable efforts" is to implement a comprehensive trade secret compliance plan. Such a program should be designed for the specific organization and the actual risks it faces. The various factors that should be considered in its design are: (1) the size of the company (the larger the entity, the more formal the plan); (2) the risks inherent in the business; (3) past history of either security problems or trade secret piracy; and (4) any applicable industry or government standards related to information security. Such a compliance plan includes numerous elements.

---

197 Saunders, supra note 122, at 148.
200 Pooley et al., supra note 26, at 217.
201 Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).
A. Physical Restrictions

"First, trade secrets should be kept in restricted areas. For instance, confidential processes, devices, or information can be performed or kept in sectioned-off or locked areas or receptacles to which only appropriate personnel have access." Physical restrictions include restricted access to premises (key cards, receptionists, building security), file cabinet locks, trash security (to prevent dumpster diving), surveillance equipment, control of prototypes, and control of writings and presentations by scientists and others. An entity should consider using "employee/visitor identification badges, "DO NOT ENTER" or "RESTRICTED ACCESS" signs for confidential areas, simple sign in/out sheets," computer passwords, physical barriers, and policies to keep visitors away from trade secret information.

An entity should consider the use of unnamed or coded components or ingredients. For example, in Mangren Research & Development Corp. v. National Chemical Co., the court found that removing supplier labels from ingredients used to manufacture a product and replacing said labels with company-coded labels were sufficient for establishing reasonable protection efforts. The method used by KFC Corporation to protect its secret recipe fried chicken seasoning is to have one supplier provide one part of the recipe and another vendor supply the other with neither having knowledge of the ingredients supplied by the other.

B. Employee Restrictions and Monitoring

An employer should address trade secret protection issues from the moment a prospective employee applies for a job and should conduct criminal background checks on prospective employees. From the start, prospective employees should know what is required of them, such as a high degree of responsibility in maintaining the confidentiality of specified information. If potentially damaging information must be revealed during the job interview process, the applicant should sign a pre-employment confidentiality agreement.

Once hired, the employee should be informed of the trade secrets that

---


203 Morton v. Rogers, 514 P.2d 752, 754 (Ariz. Ct. App. 1973) (blending directions and formulae kept locked up with only limited employee access upheld as trade secrets); See Dicks v. Jensen, 768 A.2d 1279, 1285 (Vt. 2001) (customer list which was not locked and was available to any employee held not a trade secret).

204 Rodgers & Marrs, supra note 9, at 27.

205 87 F.3d 937, 943 (7th Cir. 1996).

he or she is bound to protect. He or she should be asked to sign a non-disclosure or non-compete agreement, which often includes various confidentiality provisions. Upon starting work, the employee should be monitored for compliance with the rules regarding trade secrets, especially those involving computer usage and telecommunications. This type of monitoring can be implemented through the installation of keystroke logging software/hardware and/or packet sniffers on computer systems/networks. "Keystroke logging software/hardware creates encrypted log files that store a record of the keystroke or typing activities of a computer user. These files are stored in a manner invisible to the computer user. . . . An example of these monitoring technologies is the Spy Agent software package."208

The education of employees on the confidential nature of trade secrets is another important aspect of a trade secret compliance plan. Employees should be informed about their duties to guard trade secrets and the consequences of failing to do so. The viability of many businesses is tied directly to the protection of trade secrets. For example, employees should be taught not to discuss confidential information "in the presence of third parties, such as in elevators, at restaurants, at the airport, and in personal emails."209 In addition, employees should be taught to discern between general information and sensitive data that should not be disclosed to unauthorized persons.

An exit interview should be conducted before an employee departs a firm. The purposes of such an interview are to identify compromises in security perceived by the departing employee and stress that proprietary information must not be disclosed. Also, legal forms should be signed by the departing employee acknowledging her understanding of the firm's trade secret policies, and the continuing obligation of non-disclosure. In some cases, the new employer should be notified in writing of the employee's obligation not to disclose or use trade secrets. "Such precautions will make it difficult, if not impossible, for the employee to later claim that he or she had no reason to know that such was a trade secret or acquired by improper means."210

---

208 Fitzpatrick et al., supra note 2, at 66-67.
209 Rodgers & Marrs, supra note 9, at 26.
210 Halan, supra note 202, at 26. Accord Hexcomb Corp. v. GTW Enters., Inc., 875 F. Supp. 457, 467 (N.D. Ill. 1993) (finding that defendant knew of the trade secret status of a machine because he had been put on notice of such during exit interviews).
C. Other Miscellaneous Controls

An entity should conduct systematic audits or inventories of its trade secret portfolio. As noted, trade secrets may include formulas, prototypes, processes, customer lists, analytical information, marketing campaigns and strategies, scientific notebooks, computations, chemicals, equations, cost information, quality control procedures, revenue information, budgets and forecasts, and other internal data or information. It is incumbent upon management to learn what information gives the firm a competitive advantage.

Firms should enter agreements with suppliers, consultants, independent contractors, vendors, and others to protect all types of proprietary information. Often such agreements include both a pledge to refrain from using the company's trade secrets and also a promise not to compete. Refusal of a third party to enter into an agreement vital to the protection of trade secrets raises a serious question about whether the company should be doing business with that entity. A company owning trade secrets must protect them during any negotiations with third parties including prospective customers and those interested in buying products, technology, or other company assets.

Another critical dimension of a firm's trade secret compliance plan is document protection, retention, and destruction. Scientific and technical information should be in notebook form and "confidential" identification should be stamped on documents. Moreover, documents should not be copied without control—an inventory should be kept of all copies, identifying their location. Special permission should be required to remove documents from the premises and should be granted only for compelling reasons. Also, documents and other items containing trade secret information should be labeled with legends or stamps denoting such to be proprietary trade secret data.\(^<sup>211</sup>\) Documents should be discarded only after supervising or legal personnel have been consulted. Discarded documents should be destroyed by burning, shredding, or other means of destruction.

IX. Conclusion

Trade secret espionage activities are conducted by current and former employees, competitors, foreign governments, independent contractors,
vendors, business intelligence analysts, and others. The information sought out in trade secret fraud activities includes customer lists, pricing strategies, formulas, compilations, financial information, processes, design manuals, strategic and marketing plans, and other proprietary information.

The primary means of civil enforcement available to victims of trade secret espionage is a lawsuit filed under the U.T.S.A. or state trade secret common law. In a civil suit, a trade secret claimant must prove the following elements: (1) the existence of a trade secret; (2) reasonable steps to preserve secrecy; (3) independent economic value of the trade secret; (4) misappropriation; and (5) actual damage.

The Restatement, U.T.S.A., and the E.E.A. can be used to determine if a trade secret exists. The Restatement provides a narrower definition than the U.T.S.A. because it focuses upon business processes and practices. Under the E.E.A., the list of potential types of trade secrets is more expansive than under the U.T.S.A. The U.T.S.A. establishes statutory causes of action for both wrongful acquisition and wrongful disclosure of a trade secret. Wrongful acquisition means that the information was acquired through improper means. Improper means includes numerous illegal acts and obtaining knowledge of a process without spending the time and money to discover it independently. For wrongful disclosure, the claimant must establish that the defendant actually used the trade secret or disclosed the information to another.

The owner of a trade secret must take reasonable measures to protect it. Such measures include physical methods and the fragmentation of information. Some courts consider means to protect trade secrets the most important factor in the determination of the existence of a trade secret. The issue of what steps are reasonable under a particular set of circumstances is a question of fact.

A trade secret claim also requires proof of independent economic value. The trade secret claimant must demonstrate that competitors or others attach value to the trade secret. Competitive value communicates to the courts that the legal protection for trade secrets is justified. The value of protected information is derived from the fact that it is not generally known and not readily ascertainable. Economic value can be determined using the cost, market, and/or income approaches.

A successful trade secret plaintiff may recover damages from and/or obtain an injunction against an offender. Damages can include both actual losses (computed on the basis of net profit) and unjust enrichment not considered in actual losses. If the facts are not precise enough to warrant a damage award based upon lost profits or unjust enrichment then courts use the "reasonable royalty theory." Exemplary damages may also be awarded
where the misappropriation is willful and malicious. An injunction may be issued to prevent an actual or threatened trade secret misappropriation.

One of the main defenses to liability under the U.T.S.A. is challenges to the claimant’s evidence for each of the required statutory elements. A trade secret misappropriator may also negate liability by proof that the secret could have been derived by independent discovery or reverse engineering. The statute of limitations is also an acceptable defense to trade secret misappropriation.

Finally, the most effective way to prevent trade secret fraud is to implement a trade secret compliance plan. The elements of such a compliance program include physical restrictions, employee restrictions and monitoring, systematic audits or inventories of trade secrets, agreements with suppliers, consultants, independent contractors, vendors, and others, and document protection, retention, and destruction.