



PROGRAM MATERIALS

Program #35149

July 23, 2025

Identifying Trade Secrets in Litigation

Copyright ©2025 by

- **Scott F. Gibson, Esq. - Denton Peterson Dunn**

All Rights Reserved.

Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Identifying Trade Secrets in Litigation

Lawyers and judges are smart people who aren't good at math or science.



Scott F. Gibson
Denton Peterson Dunn
SGibson@DentonPeterson.com

Scope of Presentation

- . The Big Picture
- . Important Definitions
- . Identification Process
- . Required Specificity

Part One

The Big Picture

Origins

Unfair Competition

The freedom to engage in business and to compete for the patronage of prospective customers is a fundamental premise of the free enterprise system. .

. . The freedom to compete necessarily contemplates the probability of harm to the commercial relations of other participants in the market.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 1, comment a

“ . . . competition is not a tort.”

Frandsen v. Jensen-Sundquist Agency, Inc.,
802 F.2d 941, 947 (7th Cir. 1986)

Even though competition may be “painful, fierce, frequently ruthless, sometimes Darwinian in its pitilessness, [it] is the cornerstone of our highly successful economic system.”

Speakers of Sport, Inc. v. ProServ, Inc.,
178 F.3d 862, 865 (7th Cir. 1999)

A primary purpose of the law of unfair competition is the identification and redress of business practices that hinder rather than promote the efficient operation of the market.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, comment g

Intangible Assets

Intangible Assets

84% value of
S&P 500

40% in 1980s

17% in 1975

Wisps of air

Selling the Invisible

UNFAIR!

Part Two

Important Definitions

Trade Secrets

“one of the most elusive and difficult concepts in the law to define.”

Lear v. Siegler, Inc. v. Ark Ell Springs, Inc.,
569 F.2d 286, 288 (5th Cir. 1978)

Uniform Trade Secrets Act

- (i) derives independent economic value, actual or potential, from not being generally known to and not being readily accessible 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.

Uniform Trade Secrets Act

- (i) derives *independent economic value*, actual or potential, from not being generally known to and not being readily accessible 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.

Uniform Trade Secrets Act

- (i) derives *independent economic value*, actual or potential, from *not* being *generally known* to and not being readily accessible 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.

Uniform Trade Secrets Act

- (i) derives *independent economic value*, actual or potential, from *not* being *generally known* to and not being readily accessible 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.

Uniform Trade Secrets Act

- (i) derives *independent economic value*, actual or potential, from *not* being *generally known* to and not being readily accessible 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.

Trade secret information must have some novelty
“merely because that which does not possess
novelty is usually known; secrecy in the context of
trade secrets thus implies at least minimal novelty.”

Kewanee Oil v. Bicron Corp., 416 U.S. 470, 476 (1974)

In many cases, the question of whether certain information constitutes a trade secret ordinarily is best “resolved by a fact finder after full presentation of evidence from each side.”

Carbo Ceramics, Inc. v. Keefe,
166 Fed. Appx. 714, 718 n. 1

Misappropriation

The only way to validate a trade secret is through litigation. Absent a court finding that trade secret property rights in information exist, the trade secret status of the information remains alleged but unproven.

R. Mark Halligan and Richard F. Weyand,
Trade Secret Asset Management 2018, 17

The Incredible Morphing Trade Secret

**Confidential
Information**

The rules governing trade secrets are ***still relevant*** in analyzing the reasonableness and enforceability of nondisclosure provisions because, in order to justify the contractual restraint, information subject to non-disclosure provisions must ***share*** at least some of the ***characteristics*** with information protected by ***trade secret statutes***.

Orthofix, Inc. v. Hunter,
630 Fed. Appx. 566, 567 (6th Cir. 2015)

General Skills and Knowledge

Information that forms the general skill, knowledge, training, and experience of an employee cannot be claimed as a trade secret by a former employer ***even when the information is directly attributable to an investment of resources*** by the employer to the employee.

Restatement (Third) of Unfair Competition
§ 42 comment d

Trade secret rights are more likely to be recognized in specialized information unique to the employer's business than in information more widely known in the industry or derived from skills possessed by persons employed in the industry.

Lessner Dental Laboratories, Inc. v. Kidney,
492 P.2d 39, 42 (Ariz. Ct. App. 1971)

Part Three

Identification Process

WHO How WHAT
WHEN ? WHY
WHERE

TRADE SECRET CASE MANAGEMENT JUDICIAL GUIDE

www.fjc.gov

TRADE SECRET
CASE MANAGEMENT
JUDICIAL GUIDE

www.fjc.gov

- *Iqbal and Twombly*

TRADE SECRET
CASE MANAGEMENT
JUDICIAL GUIDE

www.fjc.gov

- *Iqbal* and *Twombly*
- Specificity

TRADE SECRET
CASE MANAGEMENT
JUDICIAL GUIDE

www.fjc.gov

- *Iqbal* and *Twombly*
- Specificity
- General Skills and Knowledge

A person claiming rights in a trade secret bears the burden of defining the information for which protection is sought *with sufficient definiteness to permit a court to apply the criteria for protection . . . and to determine the fact of an appropriation.*

RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 39, comment d

The burden is upon the plaintiff to specify [the bases for its charges], not upon the defendant to guess at what they are.

Xerox Corp. v. International Business Machines Corp.,
64 F.R.D. 367, 371 (S.D.N.Y. 1975)

In any action alleging the misappropriation of a trade secret under the Uniform Trade Secrets Act ... ***before commencing discovery*** relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with ***reasonable particularity*** subject to any [protective] orders that may be appropriate . . .

California Code of Civil Procedure § 2019.210

- Well investigated claims

Advanced Modular Sputtering, Inc. v. Superior Court,
132 Cal. App. 4th 826 (rev. den. 2d Dist. 2005)

- Well investigated claims
- Meritless claims

Advanced Modular Sputtering, Inc. v. Superior Court,
132 Cal. App. 4th 826 (rev. den. 2d Dist. 2005)

- Well investigated claims
- Meritless claims
- Discovery to learn trade secrets

Advanced Modular Sputtering, Inc. v. Superior Court,
132 Cal. App. 4th 826 (rev. den. 2d Dist. 2005)

- Well investigated claims
- Meritless claims
- Discovery to learn trade secrets
- Frame proper scope of discovery

Advanced Modular Sputtering, Inc. v. Superior Court,
132 Cal. App. 4th 826 (rev. den. 2d Dist. 2005)

- Well investigated claims
- Meritless claims
- Discovery to learn trade secrets
- Frame proper scope of discovery
- Complete / well-formulated defense

Advanced Modular Sputtering, Inc. v. Superior Court,
132 Cal. App. 4th 826 (rev. den. 2d Dist. 2005)

Part Four

Required Specificity

In any action alleging the misappropriation of a trade secret under the Uniform Trade Secrets Act ... ***before commencing discovery*** relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with ***reasonable particularity*** subject to any [protective] orders that may be appropriate . . .

California Code of Civil Procedure § 2019.210

A court may require *greater specificity* when the plaintiff's claim involves information that is closely integrated with the *general skills and knowledge* that is properly retained by former employees.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION
§ 39 comment d (emphasis added)

Uniform Trade Secrets Act

- (i) derives ***independent economic value***, actual or potential, from ***not*** being ***generally known*** to and not being readily accessible 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.

Grandpa's Syndrome

Grandpa's Syndrome

Meemaw's Malady

Lake Wobegon

Lake Wobegon

“... all the women are strong, all the men are good looking, and all the children are above average.”

Garrison Keillor
A Prairie Home Companion

Trade Secret Audits

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

Uniform Trade Secrets Act § 5

Important Principles

The Sedona Conference

Principle No. 1: The identification of an asserted trade secret during a lawsuit is not an adjudication of the merits and is not a substitute for discovery.

The Sedona Conference

Principle No. 2: The party claiming misappropriation of a trade secret should identify in writing the asserted trade secret at an early stage of the case.

The Sedona Conference

Principle No. 3: The party claiming the existence of a trade secret must identify the asserted trade secret at a level of particularity that is reasonable under the circumstances.

Show, don't tell

John was scared. The room was really gross and creepy.

Lawyers and judges are smart people who aren't good at math or science.

Quest Solution, Inc. v. RedLPR, LLC

2023 WL 11910450 (D. Utah 2023)

- “proprietary imaging units”
- “pioneering technologies”
- “proprietary imaging units”
- “suite of proprietary software applications”
- “servers, terminals” that are “configured and optimized”
- “technical trade secrets” including “technical know-how, secrets, and other confidential information”

“The allegations swept **broadly and vaguely** across the technical areas of Plaintiff’s business. The allegations include **all** cameras; **all** software, including **all** image processing and management platforms; **all** servers, terminals, and computing devices optimized for the LPR field; **all** technical know-how, etc., and that such **unspecified trade secrets** were incorporated in an **unspecified manner** into the defendants’ products, such that the products were indistinguishable.”

Purchasing Power, LLC v. Bluestem Brands, Inc.

22 F.Supp. 3d 1305 (N.D. Ga. 2014)

- “confidential financial data”
- “credit facilities”
- “credit underwriting matrices”
- “portfolio performance / analysis”
- “customer profiles”
- “sales and marketing information”
- “shipped revenues”
- “repeat buyers”
- “industry concentrations”
- “merchandising trends”
- “product development information”
- “operations and IT”

“unique underwriting process, financing, marketing, industry concentrations to targeted clients, product development, approach to recruiting and supporting brokers, varying margins with respect to specific products, default rate and bad debt expense”

“Additional, ***focused due diligence requests***”

“Information about [Plaintiff's]
recruitment of brokers, underwriting, and
other areas of its business utilizing ***unique***
approaches and processes”

“Aspects” of Plaintiff's business, including
“marketing, merchandising, operations,
finance, credit and tax”

“Intricate details of [Plaintiff's] business model, ***including, but not limited to***, its go-to-market strategies; ways to go through voluntary benefit brokers to reach the heads of human resources departments with a retail product that would allow employees to purchase items; pricing; product offerings; underwriting; and ways to gain acceptance from human resources departments”



\$72 million

Zunum failed to identify any of its alleged trade secrets with sufficient particularity or prove by substantial evidence that its alleged trade secrets derived value from not being generally known to or readily ascertainable by others.

Zunum Aero., Inc. v. Boeing,
2024 U.S. Dist. LEXIS 144978, *14 (W.D. Wash. 2024)

Take Aways

- . Trade secrets v. general skills and knowledge
- . Strike early
- . Show, don't tell
- . Grandpa's Syndrome



Scott F. Gibson
Denton Peterson Dunn
SGibson@DentonPeterson.com

Important Considerations

By Scott F. Gibson

Maintaining trade secrets may seem overwhelming, but you must help your client start now.

Conducting a Trade Secret Audit

Your client's intangible assets are at risk—and its employees pose the greatest threat to those assets. Those intangible assets walk out the door with your client's employees at the end of each work day. If all goes well, they will return

intact the next day. Intangible assets can be downloaded, duplicated, and distributed to competitors, or used to help an employee set up a competing business. They can be posted on the Internet, or transmitted instantaneously around the world with the click of a mouse. Your client's success heavily depends on its ability to protect those assets from misappropriation and misuse.

Intangible assets make up as much as 85 percent of the value of your client's company. *New Ways Needed to Assess New Economy*, L.A. Times, Nov. 13, 2000. Traditional intellectual property law covering patents, trademarks, and copyrights protects many of those assets, but trade secrets make up an increasingly greater portion of intangible assets. If your client wants to protect its business from disloyal employees and from unfair competition, the law requires it to take "reasonable efforts" to maintain the secrecy of its trade secrets.

A trade secret audit is a key component of the "reasonable efforts" to protect the secrecy of trade secrets. Properly done, a

trade secret audit helps a company (1) identify intangible assets entitled to trade secret protection and document the scope of the company's legally protectable interest, (2) segregate and secure the assets, and (3) develop appropriate protocols and procedures to protect the assets. A proper audit addresses every interaction that employees, vendors, customers, and outsiders have with the company's intangible assets, and it identifies appropriate methods for securing the assets from misuse or misappropriation. It allows a company to determine whether it needs restrictive covenants or confidentiality agreements with particular employees who have access to trade secrets and other valuable intangible assets.

Perhaps most importantly, a well-conceived audit helps establish an employer as a "White Hat" and strengthens the likelihood that a company will obtain injunctive relief if litigation becomes necessary to protect its trade secrets or other intangible assets. See Scott F. Gibson, *Protect Your Intangible Assets: Wear a White Hat*, For The Defense, Mar. 2010, at 40 (discussing "white hat" employers).

Value of Intangible Property

In the not too distant past, a company derived its value largely from its hard



■ Scott F. Gibson is the managing partner of the Mesa, Arizona, law firm Gibson Ferrin, PLC, and an adjunct professor at the Sandra Day O'Connor College of Law at Arizona State University. He is a member of DRI's Employment Law, Commercial Litigation, and Trial Tactics Committees.

assets—its land, resources, and inventory. A company's intellectual property and other intangible assets, while valuable, played a secondary role in creating value for the company. As late as the early 1980s, publicly traded companies in the United States derived only 40 percent of their value from their intangible assets. *A Market for Ideas*, The Economist, Oct. 22, 2005.

Those days are long gone. The American economy has undergone a transition from a manufacturing economy to a service economy; technological advances have emphasized ideas and innovations. During the dot-com era, companies transformed an idea to a publicly traded company without ever selling a product. Patent portfolios and licensing agreements have become key components determining a company's financial standing. Companies conduct business through cyberspace without any tangible physical presence, and they prosper because of their ideas. As Alan Greenspan, former chairman of the Federal Reserve, noted, "The economic product of the United States [has become] predominantly conceptual." *Id.*

Intangible assets—ideas and innovations—have become your client's most valuable resources. Those intangible assets take many forms, ranging from traditional intellectual property—patents, trademarks, and copyrights—and electronic data, to branding strategies and financial profiles, to customer good will and secret formulas. Intangible assets help a company differentiate itself from its competitors and establish the foundation for the company's marketing niche. No matter the industry, every company has valuable intangible assets that it must leverage and protect.

At the same time that intellectual property has become more central to the financial viability of companies, employees have become more mobile, regularly changing jobs from one company to another. Current and former employees constitute the greatest threat to intangible assets. ASIS Int'l, *Trends in Proprietary Information Loss*, Aug. 2007, at 29, <http://www.asisonline.org/newsroom/surveys/spi2.pdf> (last visited Dec. 29, 2010). Technological advances have made it increasingly easier for thieves to walk off with that intellectual property, often unnoticed by the companies that they fleece.

As bad as the risk of theft is, losses from careless or untrained employees are worse. Employees often inadvertently compromise their employer's intangible assets by misdirecting e-mails or faxes, observing information without authorization, or by exposing them in written communications or in oral presentations at trade shows. *Id.* at 29. One recent study disclosed these shocking facts:

- One of every 50 files on file shares and desktops contain exposed confidential data.
- One of every 400 outbound e-mail messages contains confidential data.
- 95 percent of data loss incidents are unintentional. Most breaches are the result of careless or untrained employees, or legacy automated processes,
- 41 percent of violations contained intellectual property, insider information, or trade secrets.
- 58 percent of violations may be subject to review under state and federal regulations.
- The average number of data loss incidents per year per employee is four.

Vontu Report: Data Security Trends 2005, at 8 (Vontu, Inc. 2006).

The losses associated with the theft of trade secrets are staggering. For example, a recent survey of Fortune 1000 companies and 600 small and mid-sized companies belonging to the U.S. Chamber of Commerce estimates that the companies suffered between \$53 billion and \$59 billion in losses of proprietary information and intellectual property in 2001. ASIS Int'l, *Trends in Proprietary Information Loss*, Sept. 2002, at 1. Some 40 percent of the companies participating in the survey reported incidents of known or suspected losses of proprietary information. *Id.*

If your client wants to avoid becoming part of these staggering statistics, it must take appropriate steps to protect and safeguard its intangible assets. Your job as counsel is to help your client do so.

Defining a Trade Secret

Part of the challenge of protecting trade secrets is that, well, they are intangible and, therefore, difficult to define and conceptualize. Indeed, a trade secret "is one of the most elusive and difficult concepts in the law to define." *Lear Siegler, Inc. v.*

Ark Ell Springs, Inc., 569 F.2d 286, 288 (5th Cir. 1978).

To successfully protect those ethereal assets, you must first understand how the law protects ideas and innovations. The law of trade secrets initially developed through the common law. Two major sources of law—the Uniform Trade Secrets Act and the Restatement of Torts—outline the legal

No matter the industry,
every company has valuable
intangible assets that it
must leverage and protect.

principles primarily used to secure and protect trade secrets.

Trade secret protection "arises automatically, the scope is extremely broad, and it allows independent development of similar ideas by innocent third parties." Henry H. Perritt, Jr., *Trade Secrets: A Practitioner's Guide*, 1 (Practicing Law Institute 1994). In the words of one court, "at bottom, trade secret protection is itself but a branch of unfair competition law." *Balboa Ins. Co. v. Trans Global Equities*, 218 Cal. App. 3d 1327, 1341, 267 Cal. Rptr. 787, 785 (Cal. Ct. App. 1990).

Trade secrets are particularly well suited for the Information Age: "Machinery and mechanisms were the brainchildren of the Industrial Age, and patent law was designed to protect them. In the Information Age, trade secret protection is better suited to the fast-moving and unpatentable confidential information we need to run our companies." R. Mark Halligan and Richard F. Weyand, *The Sorry State of Trade Secret Protection*, <http://www.thetso.com/Info/sorry.html> (last visited Dec. 29, 2010).

In 1934, the Restatement of Torts outlined the definition of a trade secret:

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

Restatement of Torts §757, cmt. b (1934).

The Restatement definition quickly became the most common legal approach to handling trade secrets. The law did not develop consistently and uniformly under

sonable under the circumstances to maintain its secrecy.

Unif. Trade Secrets Act §1(4) (emphasis added).

This definition of a trade secret raises two critical points. First, as the name suggests, a trade secret must actually be a secret. Information that is commonly known or used in an industry cannot have trade secret protection. Rather, “a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information.” Restatement of Torts §757 cmt. b. Courts frequently consider a number of factors to determine whether information constitutes a trade secret, including those factors first identified in the Restatement, which noted the necessity of secrecy:

- The extent to which the information is known outside of a business;
- The extent to which it is known by employees and others involved in a business;
- The extent of the measures taken by a business to guard the secrecy of the information;
- The value of the information to the information’s owner and to its competitors;
- The amount of effort or money expended by the business in developing the information;
- The ease or difficulty others would have properly acquiring or duplicating the information.

See, e.g., *Lee v. Cercoa, Inc.*, 433 So. 2d 1, 2 (Fla. Dis. Ct. App. 1983).

Second, to constitute a trade secret the owner must take appropriate steps to protect the secrecy of the information. In other words, information that otherwise might constitute a trade secret—for instance, information that provides an economic benefit to its owner because it is not commonly known in the industry—may lose its status as a trade secret if its owner does not take “reasonable” steps to protect its secrecy. As noted by one court, “Indeed, the most important factor in gaining trade-secret protection is demonstrating that the owner has taken such precautions as are reasonable under the circumstances to preserve the secrecy of the information.” *Enterprise Leasing Co. of Phoenix v. Ehmke*, 197 Ariz. 144, 150 ¶22, 3 P.3d 1064, 170 ¶22 (Ariz. Ct. App. 1999).

The UTSA has received widespread acceptance, with 44 states and the District of Columbia adopting statutes based on it. The other six states—Massachusetts, New Jersey, New York, Pennsylvania, Texas, and Wyoming—protect trade secrets either under the common law or through a state-specific statutory scheme. The Restatement definition plays a vital role in the states that have not adopted the UTSA. See, e.g., *Ashland Mgmt v. Janien*, 82 N.Y.2d 395, 407, 624 N.E.2d 1007, 1013 (N.Y. 1993).

Wear a White Hat

If all goes well, your client will never have to file suit to protect its intangible assets. It will faithfully implement the plan that you have developed to protect its trade secrets. Employees will care for and guard the company’s trade secrets, former employees will respect the legal boundaries placed on them through restrictive covenants and the common law, and competitors will stay within the limits of fair competition. Life is wonderful when things work the way they were designed.

But real life is often messier than it should be. When people fail to honor their commitments, you must litigate to protect your client’s trade secrets.

A court likely will first consider the merits of your client’s case in a preliminary injunction hearing. Preliminary injunction hearings are abbreviated and fast paced. You may not have time to fully develop the evidence supporting the virtue of your client’s case. What can you do to increase your odds of success? The answer is simple: wear a white hat.

The old black and white Western movies use visual clues to help an audience distinguish the “good guys” from the “bad guys.” The “good guys” wear white hats; “bad guys” wear black hats. This simple dress code allows even the least attentive patron to determine where to place his or her allegiance.

In similar vein, judges look for clues to determine which party should prevail on a claim for injunctive relief. If your client is a White Hat—that is, if it has behaved ethically and fairly—the court will reward your client with the injunctive relief it desperately needs. If not, the court will deem it to be a Black Hat, and allow those critical intangible assets to dissipate away.

Your challenge is to make the intangible tangible, to give substance to the ephemeral, and to help a court visualize the invisible.

the Restatement definition, however, and when the American Law Institute published the Restatement (Second) of Torts in 1977, it failed to discuss liability for misappropriation of trade secrets.

In 1979, the National Conference of Commissioners on Uniform State Law approved the Uniform Trade Secrets Act as a means of protecting intangible assets. In doing so, the commissioners noted that while trade secret law had considerable commercial importance, “this law has not developed satisfactorily.” Unif. Trade Secrets Act, Commissioners’ Prefatory Note. The UTSA was designed to resolve the “uneven” development of the law and the “undue uncertainty concerning the parameters of trade secret protection, and the appropriate remedies for misappropriation of a trade secret.” *Id.*

Because a trade secret is difficult to define, the UTSA broadly defines it as 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 rea-

The challenge with intangible assets is that, as mentioned before, they are intangible and difficult to conceptualize. Judges are reluctant to protect that which they cannot see or comprehend, particularly when the putative owner can only vaguely describe the asset and has difficulty proving that he or she actually owns it. Your challenge is to make the intangible tangible, to give substance to the ephemeral, and to help a court visualize the invisible. You must clearly show a judge that your client deserves the relief that he or she seeks.

A trade secret audit helps establish your client as a White Hat by allowing it to identify and document, segregate and secure, and develop the appropriate procedure and protocols to protect its trade secrets.

White Hats document and inventory their intangible assets early and often. They show that they value their trade secrets by taking reasonable steps to protect those assets. They can demonstrate how their trade secrets differ from an employee's general knowledge and skills, which courts do not consider proprietary. White Hats vali-

date their trade secrets before these valuable assets have been compromised.

Conducting an Audit

The specific scope of a trade secret audit varies depending on a client's industry and the nature of its intangible assets. Regardless of the industry, however, an audit locates assets and establishes the restrictions placed on the people who have access to the assets, including job applicants, employees, former employees, vendors, and business partners.

Trade Secrets Audit Checklist

Identify categories of potential trade secrets.

- Technical information
 - Proprietary technical information
 - Research and development
 - Formulas
 - Compounds
 - Prototypes
 - Processes
 - Lab notebooks
 - Experiments and experiment data
 - Analytical data
 - Calculations
 - Computer programs
 - Business know-how, including negative know-how
 - Drawings
 - Design data and manuals
 - Vendor and supplier information
- Production and processing information
 - Cost or pricing data
 - Proprietary information concerning production and processes
 - Special production machinery
 - Processing or manufacturing technology
 - Specifications for production processes and machinery
 - Production know-how and negative know-how
 - Business methodologies
 - Distribution sources

- Vendor and supplier information
 - Cost and price data
- Quality control information
 - Quality control procedures, manuals, or records
 - Maintenance know how and negative know how
- Sales and marketing information
 - Sales and marketing plans
 - Sales forecasts
 - Proprietary information about sales and marketing
 - Sales-call reports
 - Customer lists and databases
 - Customer needs and buying habits
 - Proprietary sales and marketing information
- Financial information
 - Proprietary financial information
 - Internal financial documents
 - Budgets and forecasts
 - Computer printouts
 - Product margins
 - Product costs and pricing
 - Operating reports
 - Profit and loss (P&L) statements
- Internal administrative information
 - Proprietary administrative information
 - Internal organization
 - Information about key personnel

- Strategic business plans
- Internal computer software

Document trade secrets.

- Identify storage media
 - Electronic
 - Physical documents
 - Human memory
- Identify storage systems and devices.
 - Filing cabinets
 - File server
 - Workstations
 - Voice-mail system
 - Portable objects
 - Lap tops
 - PDAs
 - Flash drives
 - CDs and other electronic media
- Identify trade secrets storage locations.
 - Company headquarters
 - Satellite offices
 - Work sites
 - Offsite locations
 - Employee homes
 - Subcontractors
 - Clients, customers, vendors, and business partners

Restrict access to confidential information.

- Security procedures
 - Premises
 - Network
 - Backup of network
 - Access
 - Authorization
 - Portability
 - Espionage

- Review and update company policies on a regular basis.
- Conduct regular audits of policies and procedures used to protect confidential information. Update and amend policies as needed.
- Develop procedures for correcting inadvertent disclosure.
- Establish a policy of pursuing theft of trade secrets and other confidential information.
- Develop an appropriate document-retention policy.

Protect information based on the way it's classified.

- Location
- Segregate information
- Restrict access to the information.
- Assign a specific employee the responsibility for managing the confidential information.
- Determine which type of storage system or device is appropriate for the information.
- Determine where the company should store the information.
- Documents
 - Clearly identify documents as confidential.
 - Transmit trade secrets through secure means.
 - Develop an appropriate policy for destruction of documents.

Identify and Document

The first step of a trade secret audit will identify the trade secrets and other intangible property a company needs to protect. That analysis should cover every aspect of a company's business, including research and development, manufacturing, production, sales, marketing, and human resources. The Trade Secrets Audit Checklist on page 39 identifies key components of an audit.

To determine whether your client's information qualifies for trade secret protection, focus on three key questions: (1) Is the information commonly known in the industry? (2) Does the company receive economic value from the information because it is not commonly known in the industry? (3) Has the company taken reasonable steps to protect the secrecy of the information?

Once you have identified the relevant trade secrets, prepare a confidential list of them. The list should identify each trade secret with reasonable particularity, and it should outline how the trade secret was developed.

Work with company representatives to identify specifically *why* the information is valuable to the company. One of the primary rules of marketing is that, to succeed, a company must differentiate itself from its competitors in ways that are meaningful to its customers. The same rule applies to trade secrets and other intangible assets. You must be able to demonstrate and communicate how each asset differs from industry standards, and why that difference is meaningful in your client's industry.

If you are required to go into court to protect a trade secret, you will need an

articulate witness who can explain both the value of that trade secret and the efforts that its owner has taken to develop and protect it. Most companies do not begin gathering information on their trade secrets until a disloyal employee has walked out the door with one. Don't make that mistake. As part of an audit, begin preparing a company representative to testify about the trade secret during a trial. If things go well, you will never need to finalize that direct examination. You will find, however, that contemplating the scope of testimony will help you better understand the information that your client wants to protect and will allow your client to more effectively protect and secure its intangible assets than otherwise.

One of your main objectives is to help your client make its intangible assets substantial and real. You can do so by mani-

Trade Secrets and Employee Relations Protocols

Prehiring

- Have a written job description for every position that
 - identifies the essential job functions of the position;
 - identifies the interactions that the employee will have with trade secrets, confidential information, and intangible assets;
 - identifies the types of agreements that the employee must sign with the employer—confidentiality agreements, trade secrets agreements, non-compete agreements, and other restrictive covenants; and
 - has been reviewed and updated within the last 12 months.
- All job postings should identify the essential job functions for the position.
- All candidates should complete a standard application form that
 - states that the company protects the trade secrets, confidential information, and intangible assets of others;
 - states that the company protects its own trade secrets, confidential information, and intangible assets;
 - requires a candidate to disclose any agreements that would impact his or her ability to perform the essential job functions of the position—confidentiality agreements, trade

- secret agreements, non-compete agreements, and restrictive covenants;
 - requires a candidate to affirm in writing that he or she will abide by any agreements with his former employers;
 - requires a candidate to affirm that he or she will not disclose any trade secrets or confidential information of any current or former employer as part of the application and interview process; and
 - requires the candidate to identify in general terms the types of trade secrets and confidential information that he or she holds.
- All candidates should submit a resume.
- A capable human resources specialist should screen all applications and resumes.
- The company should adopt and follow an approved policy for reviewing the candidate's job history and references.
- Candidates should sign an approved Non-disclosure Agreement (NDA) if they will be exposed to any confidential information during the interviewing process.
- A candidate should receive a copy of the completed application.
- A candidate should receive a signed copy of the NDA.
- A candidate should receive a copy of any confidentiality agreements or restrictive

covenants that he or she will be required to sign as a condition of employment.

- The company should design and use a standard protocol for interviewing applicants.
 - The interviewer should take notes on a standard form identifying key points to be covered during the interview.
 - The interviewer reiterates key points about confidential information:
 - The company respects and protects the trade secrets and confidential information of others.
 - The company protects its own trade secrets and confidential information.
 - The candidate should not disclose any trade secrets or confidential information of others during the interview process.
 - The company expects the candidate to abide by all agreements with any current or former employers.
 - The interviewer explains the types of agreements that the successful candidate will be expected to sign to protect the company's trade secrets, confidential information, and intangible assets.
- Before a candidate is asked to return for a second interview, the company should receive and review copies of all

festing intangible assets through a physical means. For example, you can explain an intangible idea in writing, marking the writing “confidential,” and storing it in a secure location with limited access. Likewise, a process becomes tangible when you document and name it, as well as when employees receive ongoing, systematic training on how to properly perform the process. As you help your client identify its trade secrets and other intangible assets, consider how you can best give that intangible property form.

Segregate and Secure

Once you have identified and documented your client’s intangible assets, you must next segregate and secure that property. Segregate trade secret materials from intangible assets that are not. When appropriate, label the information confidential

and move it to a secure location. Assigning a location to confidential information partly will depend on its format. The following security methods may be appropriate to secure the property:

- Mark documents as “Confidential” or “Trade Secret,” and specifically restrict copying of the documents.
- Limit access to sensitive information on a “need-to-know” basis.
- Create physical security barriers.
- Use password-protected computer files.
- Develop segregated portions of a hard drive.
- Monitor the number of physical copies that document a trade secret.
- Disable the USB ports or other methods of downloading information to storage devices.
- Maintain logs documenting the nature and scope of a trade secret.

- Develop appropriate protocols and procedures for hiring, training, and terminating employees.
- Require employees to sign nondisclosure agreements or confidentiality agreements.
- If authorized by state law, require employees to sign limited restrictive covenants.
- Create a detailed training program, and regularly train employees consistent with that program.
- Develop procedures for employees to follow when discussing trade secrets and other confidential information with outsiders.

The UTSA requires that owners of trade secrets make “efforts that are *reasonable under the circumstances*” to protect the secrecy of their trade secrets. What is “rea-

Trade Secret, continued on page 76

Trade Secrets and Employee Relations Protocols. *cont.*

agreements that the candidate has signed with current or former employers.

- The company human resources department should maintain all applications, resumes, agreements, and interview notes in individual files for each candidate.

Extending a job offer

- The interviewer should take notes on a standard form identifying key points to be covered during the second interview.
- A candidate should receive copies of all agreements that he or she will be expected to sign if he or she accepts the job and is encouraged to review the agreements with counsel and with family members before signing them.
- The candidate should receive a copy of the company’s employee handbook and confidentiality policies.
- The interviewer should instruct the candidate to remain loyal to the current employer and caution the candidate
 - to refrain from removing original records from that employer;
 - not to advise clients of departure prior to resignation;
 - not to advise coworkers of departure prior to resignation;
 - not to solicit customers;
 - not to solicit coworkers to leave that employer;

- to work with employer to return coordinate the return of all confidential information; and
- to cooperate with the employer in training the candidate’s replacement.

Employee relations

- As part of an annual employee evaluation, review the company policies on trade secrets, confidential information, electronic services and communications, among other policies and procedures, with each employee. Have each employee sign an acknowledgment that the person conducting the evaluation meeting reviewed the policies.
- Protect confidential information from employees’ access from remote locations.
- Restrict access to sensitive information on a need-to-know basis. Incorporate appropriate training and agreements with those who have a “need to know.”

Create a culture of confidentiality in the work place.

- Regularly discuss the obligations of confidentiality in employee meetings, at least two times per year.
- Review obligations of confidentiality as part of employees’ annual review.
- Document independent development of trade secrets and other confidential information.
- Keep confidential information off of

the company’s website and make sure it is not in other marketing materials. Avoid disclosing confidential information through electronic communications.

- Follow the company’s policy on confidentiality

Employee departures

- Determine the type of information the company is most concerned about losing with the departure of the employee.
- Inventory sensitive documents to which the employee has had access.
- Inventory any electronic materials to which the employee has had access, including software source code. Note the “last edit” dates and the “edited by” information.
- Review the status of the employee’s agreements with the company, including the annual acknowledgment of the company’s policies. If any acknowledgments are missing, ask the employee to sign an acknowledgment during the exit interview.
- Schedule an exit interview with a human resources representative and with the employee’s manager upon confirming the employee’s departure.
- If management suspects theft of trade secrets or confidential information, immediately arrange for forensic imaging of the hard drive of the employee’s computer.

Trade Secret, from page 41

sonable” depends on the nature of the trade secret, the value the information holds, and the size and sophistication of the business. The definition of “reasonable” is not static. An owner may need to take increasingly more sophisticated efforts to protect a trade secret as a company grows or as the information takes on greater value to the company.

Regularly evaluate the “reasonableness” of the efforts made to protect a trade secret. Your client should audit at least annually, reviewing trade secrets already covered in previous audits, as well as new trade secrets, and regularly should update efforts to segregate and secure them.

Protocols and Procedures

This is where the rubber meets the road. It is easy to talk about trade secrets, but unless your client develops and fully implements appropriate protocols and procedures, your efforts have been in vain. Indeed, if your client does not faithfully implement its trade secrets protocols and procedures, they may serve as evidence against the company’s interests. After all, if a company identifies certain procedures as being “reasonable” to protect its trade

secrets and then fails to follow those procedures, it has not taken “efforts that are reasonable under the circumstances” to protect the trade secrets.

Trade secret protocols and procedures will center primarily on a company’s interactions with its employees. “Trade Secrets and Employee Relations Protocols” on pages 40–41 identifies a number of protocols that a company will want to develop for its pre hiring, hiring, employment, and postemployment interactions with its employees.


In addition, a company should develop different procedures for handling corporate information based on the nature of the information involved. For example, some information is available for *public disclosure*, such as press releases, website postings, and marketing materials. Other information is for *internal company use* only, such as organizational charts and disaster recovery plans. Still other information is sensitive and *confidential* and employees should access it only on a “need-to-know” basis. This information includes marketing plans, business plans, and financial information. Finally, a company should place the greatest restrictions on highly sensitive confidential information. This information includes

highly confidential third-party information, such as information about medical conditions or credit cards. Failure to adequately protect this information may subject a company to legal liability.

Tailor the protocols and procedures to the specific needs of a company. Though the procedures undoubtedly will require a company to make changes to its operations, those changes should not be so overwhelming that they become impossible to implement. If a company makes vast changes, take a more practical approach, implementing the protections and protocols over time.

Conclusion

A company’s efforts to maintain its trade secrets and other intangible assets are ongoing and never ending. The task may seem overwhelming, but you must help your clients start now. Do not delay.

Your client can do nothing and hope that when its most valuable assets walk out the door with its employees at the end of the work day, they will always return intact the next day. Or, your client can recognize the vulnerability of its intangible assets and take appropriate steps to protect the company. 

Identifying

TRADE

SECRETS

in Litigation

BY SCOTT F. GIBSON

Your heart begins to race as you re-read the motion that opposing counsel just emailed you. Come to think of it, your head has been throbbing the past three days.

It all started when your best corporate client called you in a panic Tuesday morning at the crack of dawn.

"Counselor," she says with a tremble in her voice, "I just fired Bertram, our *former* COO. Late last night, I found some incriminating documents showing that he was starting a competing business. He knows *everything* about the company—our methods of doing business and all of our confidential information. If we don't stop him, he'll put us out of business."

Your mind immediately races through possible ways to stop the scoundrel. You remember that Arizona law protects a company's trade secrets and that the court has power to enjoin misappropriation of trade

secrets.

"Your company is the local leader in your industry," you remind her. "That's undoubtedly because you have better systems and methods of doing business. The law won't let Bertram misappropriate your trade secrets and confidential information."

"That's right!" she exclaims. "I developed all those systems and trade secrets myself. We're the best company in town because my systems are the best."

Thirty minutes later, you're at your desk doing computer research on misappropriation of trade secrets. When your assistant arrives 90 minutes later, you are cranking out pleadings to protect your client's business.

You eloquently describe how Bertram

willfully and maliciously misappropriated your client's valuable trade secrets and confidential information through improper means. Those trade secrets have actual or potential economic value, you argue, because they are not generally known to and are not readily ascertainable by proper means by other persons who can obtain economic value from their disclosure or use.

Your assistant brings you an energy drink so that you can work through lunch. By 3:30 p.m., you've emailed your client draft pleadings.

Early Wednesday morning, you appear *ex parte* in front of your assigned judge and make an impassioned appeal for a temporary restraining order. The judge signs your or-



der and sets a return hearing for next Monday morning. Your process server delivers your “ticking time bomb” to Bertram later that day. You begin preparing for the Order to Show Cause hearing on Monday.

Just before you go home late Thursday night, your in-box pings with an email from a lawyer across town. Attached is a motion she just filed asking the court to order you to specifically identify the trade secrets you allege that Bertram misappropriated from the company.

What gives here? you wonder. She can't make me disclose the misappropriated trade secrets before I have a chance to do discovery.

As you read the motion, your head begins to pound ruthlessly. *Ack! Maybe she can!*

Using Trade Secrets to Protect Intangible Assets

With intangible assets occupying a greater role in the digital economy, companies are increasingly relying on trade secret claims to protect those assets. And if non-compete agreements and other restrictive covenants¹ are abolished (as many state legislatures and the Biden administration seek to do), we will see an increase in trade secret litigation as businesses seek alternative means for protecting their valuable intangibles.

Courts deciding trade secret claims must “navigat[e] the line between the protection of unique innovative technologies and vigorous competition.”² While the owner of the alleged trade secret holds a property right in the technology, the defendant has a fundamental right to engage in fair competition.³

The law of trade secrets is primarily governed by state law,⁴ most notably under the Uniform Trade Secrets Act.⁵ The UTSA broadly defines a trade secret as “information, including a formula, pattern, compilation, program, device, method, technique, or process” that both:

- (a) 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

- (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy⁶

The definition is intentionally expansive, largely because a trade secret is a difficult and elusive concept to describe.⁷ The definition must be broad enough to include existing technologies as well as technologies

With intangible assets occupying a greater role in the digital economy, companies are increasingly relying on trade secret claims to protect those assets.

and ideas that have not yet been developed.

But this can make trade secret litigation cumbersome and convoluted. Other forms of intellectual property—patents, trademarks and copyrights—are issued by governmental entities certifying that the IP meets the appropriate legal requirements. At the review’s conclusion, the owner receives a document certifying that its patent, trademark or copyright is recognized.

In contrast, no governmental entity confers trade secret status on any information. “The only way to validate a trade secret is through litigation. Absent a court finding that trade secret property rights in information exist, the trade secret status of the information remains alleged but unproven.”⁸

“Morphing” of Trade Secret Claims

The lack of governmental oversight raises challenges not present in other types of IP litigation. A trade secret plaintiff simply proclaims that the information is a trade secret, and the parties must then fight over the validity of the owner’s (self-serving and often myopic) designation.

Those litigation challenges are compounded because plaintiff often lacks a clear idea of the nature and scope

of its alleged trade secrets.⁹ The owner frequently overestimates the uniqueness of its information and seeks to assert trade secret status on information that’s within the general skills and knowledge of its industry.¹⁰

Because the case often is speeding toward an expedited hearing for injunctive relief, the plaintiff typically seeks immediate and expensive discovery of defendant’s electronic information and other documents to determine what information the defendant has.

As plaintiff seeks invasive discovery of defendant’s information, plaintiff often refuses to specifically identify its own information that defendant allegedly misappropriated. This phenomenon creates two significant and related problems.

First, the defendant cannot properly prepare to defend from the allegations of misappropriation. He cannot adequately prepare to challenge the validity of the trade secret designation or prove he did not misappropriate the neb-

ulously identified trade secret.

Perhaps more disturbing, plaintiff’s failure to specifically identify its alleged trade secrets enables and emboldens plaintiff to “morph” the scope of its claims to correspond with whatever is learned through its invasive discovery. Although some plaintiffs may innocently fail to identify their alleged trade secrets, the failure to identify is often done as “a strategy, not an accident.”¹¹

It’s easy to understand why a party might impose that strategy. “The tactical advantages a plaintiff gains from non-identification are too tempting for a plaintiff to voluntarily provide such identification.”¹²

A party cannot be expected to defend against a moving target. Indeed, due process requires plaintiff to identify a plain statement of the claims so defendant can appropriately defend the case. Moreover, without identification of the alleged trade secrets, the court cannot determine whether proposed discovery encompasses the claims

SCOTT F. GIBSON is a partner with the Mesa law firm Denton Peterson Dunn, PLLC. Since 2008, he has taught a course on trade secrets and restrictive covenants at the Sandra Day O'Connor College of Law at Arizona State University. The opinions expressed in this article are my own; they do not necessarily represent the opinions of the attorneys, staff or clients of Denton Peterson Dunn, PLLC.



asserted, nor can it evaluate whether the morphing “trade secrets” are, in fact, trade secrets.

Owner’s Duty to Specifically Identify Its Trade Secrets

At least in part because the owner is able to designate the trade secret status of its own information, the owner bears the burden of proving the information is entitled to protection. In litigation, the owner must prove that its information is in fact a trade secret, and that defendant misappropriated the trade secret.¹³

The scope of plaintiff’s burden is largely undisputed. “The burden is upon the plaintiff to specify [the bases for its charges], not upon the defendant to guess at what they are.”¹⁴ The plaintiff must establish “each of [the] statutory elements [of a trade secret] as to each claimed trade secret.”¹⁵ This burden requires that “a plaintiff who seeks relief for misappropriation of trade secrets [to] identify the trade secrets and carry the burden of

showing that they exist.”¹⁶

The facts of the case determine the level of specificity required in plaintiff’s designa-

ed with the *general skill and knowledge* that is properly retained by former employees.”¹⁷ The closer the “trade secret” gets to the information generally used in the industry, the less likely it is to actually be a trade secret.

So when must plaintiff identify its trade secrets? And what level of specificity must the plaintiff use in identifying them?

Disclosure Timing

The scope of litigation does not exist in a vacuum. Discovery is limited matters relevant to the case; the scope of relevance is determined based on the allegations of the pleading. In a case alleging misappropriation of trade secrets, the relevant inquiry is

whether plaintiff’s information constitutes a trade secret and, if so, whether defendant acquired or used that information through “improper means.”

The trade secret status of plaintiff’s information is the foundation upon which the case will be won or lost. All discovery will

If an alleged trade secret is revolutionary and highly innovative, the court may allow plaintiff to identify the secrets using a lesser degree of specificity.

tion. If an alleged trade secret is revolutionary and highly innovative, the court may allow plaintiff to identify the secrets using a lesser degree of specificity.

On the other hand, “a court may require *greater specificity* when the plaintiff’s claim involves information that is closely integrat-



focus at least in part on proving or disproving plaintiff's claim of trade secret status. For that reason, the court typically requires plaintiff to identify the "metes and bounds" of its alleged trade secret information at case inception so the parties can appropriately focus discovery efforts.

By statute, California requires a trade secret plaintiff to disclose the parameters of the alleged trade secrets "with reasonable particularity" before the start of discovery.¹⁸ It does not require plaintiff to prove that its information is a trade secret before the start of discovery, only to identify the alleged trade secret's parameters.

The statute had its origins in the California appellate decision *Diodes Inc. v. Franzen*,¹⁹ which involved a semiconductor company's allegations of misappropriation against former officers. The trial court sustained demurrers to three versions of plaintiff's complaint based on plaintiff's failure to plead facts showing it owned a protectable trade secret. After the third demurrer, the court dismissed the trade secret claim.

On appeal, the court held that plaintiff could not rely on conclusory allegations of

a "secret process," but rather must identify facts that, if proven, would establish that a trade secret existed. That must occur before the start of discovery.²⁰ Courts nationwide have adopted the policy stated in *Diodes* and in the California statute.²¹

Requiring plaintiff to identify before discovery minimizes the likelihood of ever-morphing "misappropriation" claims.²² It provides a framework for the parties to tailor discovery requests and the court to resolve discovery disputes based on the scope of that identification.

Required Specificity

The required level of specificity is governed by the plaintiff's burden of proving the existence of its trade secrets:

A plaintiff seeking relief for misappropriation of trade secrets must *identify the trade secrets* and *carry the burden of showing they exist*. The plaintiff should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general

knowledge in the trade or of special knowledge of those persons skilled in the trade.²³

It is insufficient for plaintiff merely to claim that something "contain[s] valuable trade secrets" without specifically identifying those secrets²⁴ or "simply rely upon 'catch-all' phrases or identify categories of trade secrets they intend to pursue at trial."²⁵ Instead, plaintiff must "clearly refer to tangible trade secret material" instead of referring to a "system which *potentially* qualifies for trade secret protection."²⁶

To comply with its duty, plaintiff must submit a "specific, clear, detailed and precise list of the trade secrets at issue"²⁷ that includes "only those items which Plaintiff considers to be actual trade secrets and which Plaintiff has reasonable grounds to believe were misappropriated by Defendant."²⁸

Adequacy of Identification

Let's examine how the disclosure of trade secrets have played out in various reported cases.

A plaintiff cannot satisfy its burden by



pointing to vaguely described categories of information. It must identify specific information that raises a prima facie showing of trade secret status. In *Purchasing Power, LLC v. Bluestem Brands, Inc.*,²⁹ for example, the court considered the identification of trade secrets in a dispute between competitors in the business of “payroll deduction” sales.

The plaintiff initially identified 12 “broad categories of information” and argued that the defendant “was provided with detailed information” in these categories.³⁰ After the parties had a “protracted dispute” over the specificity of plaintiff’s identification, plaintiff’s counsel sent a letter identifying 15 specific documents that plaintiff asserted contained its alleged trade secrets. The letter did not specify what information in the documents it maintained constituted its trade secrets.³¹

Defendant filed a motion for summary judgment asserting plaintiff had not met its burden of showing that it had protectable trade secrets. And despite having full opportunity to specifically identify its trade secrets, plaintiff never did so. In its response, plain-

To comply with its duty, plaintiff must submit a specific, detailed list of the trade secrets at issue.

tiff cited five paragraphs in its Statement of Additional Material Facts that purportedly identified “the individual trade secrets” it claimed had been misappropriated.

But, as the court held, those identifications described only general categories of information.³² Though plaintiff used words that were intended to sound specific and proprietary, the descriptions were simply vague statements of platitudes about the “uniqueness” of its information with no

facts showing *why* it allegedly created a trade secret.³³

In comparison, the Arizona Court of Appeals had no difficulty concluding defendant misappropriated trade secrets in *Enterprise Leasing Co. of Phoenix v. Ehmke*.³⁴ Defendant worked as a senior-level manager at a car rental company. After the company terminated him, it learned he’d “absconded with 45 confidential documents comprising [the company’s] strategic plans, programs, methods and approaches.”³⁵

The descriptions of the documents emphasize the trade secret status of the information they contained detailed information, including year-to-date fiscal activities by branch office, revenue per car for each branch office, number of vehicles per branch office, a Customer Service Worksheet, and more.³⁶

The court noted that the worksheet “encompasses general business principles involved in the operation of a successful car-rental branch office.”³⁷ But the description of the worksheet clarifies that it contained much more than general knowledge in the industry:

The Worksheet includes market attributes: office appearance and traffic flow ... ; personnel attributes; leadership attributes in delegation, planning, organization and management; care condition and preparation; cycle of service at the telephone, pick-up process, branch arrival, rental contract, car, callback and vehicle return stages; and problem resolution. Each of these sections also detailed further criteria and provided lines for general written comments.³⁸

Similarly, the Ninth Circuit held that a plaintiff had identified its alleged trade secrets with enough specificity to create a genuine issue of material fact about the adequacy of the identification.³⁹ Plaintiff asserted a trade secret interest in “the logic and architecture of its securities tracking database;” the defendant asserted that its systems were “an independent improvement to the securities tracking marketplace.”⁴⁰

After defendant moved for summary judgment on plaintiff’s inability to prove it had a trade secret, plaintiff submitted two declarations that expanded upon its initial definition and described specific features. It provided information regarding “the specific tables, table columns, account identifiers, codes, and



methodologies” that the plaintiff claimed as trade secrets.⁴¹


The Ninth Circuit held the declaration raised a genuine issue of material fact as to whether plaintiff had adequately identified its alleged trade secrets with sufficient particularity. It noted the plaintiff had “identified aspects of its database logic and architecture with enough specificity to create a triable issue of fact.”⁴² Plaintiff had not simply used “catchall” phrases or “merely identified categories of information.

Note that the court did *not* hold that the information identified constituted a trade secret. Rather, it held that the information was specific enough to enable a trier of fact to determine whether the information was a trade secret.

Conclusion

Would-be authors have been counseled from time immemorial to “show, not tell” the important parts of their stories—and

that’s true with trade secrets, as well. Rather than use vague terminology that simply *proclaims* information is a secret, a plaintiff successfully identifies its trade secrets by *showing* opposing counsel and the court *why* the information should be protected.

Plaintiff’s duty to specifically identify and describe the parameters of its alleged trade secrets has never been greater. That identification must come at the start of the case, before the parties have spent a small fortune on unfocused discovery. 

endnotes

- For a discussion of how Arizona courts treat restrictive covenants, see Scott F. Gibson, *Three Tips for Drafting Enforceable Restrictive Covenants*, ARIZ. ATT’Y, Jan. 2022, at 36.
- InteliClear LLC v. ETC Global Holdings Inc.*, 978 F.3d 653, 655 (9th Cir. 2020).
- The freedom to compete is fundamental to free enterprise, and that freedom necessarily contemplates the probability of harm to the commercial relations of other participants in the market. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1 *comment a* (AM. LAW. INST. 1995).
- In 2016, Congress passed the Defend Trade Secrets Act and added a private right of action for misappropriation of trade secrets to the existing criminal penalties under the Economic Espionage Act. 18 U.S.C. § 1831-1839. The definition of a trade secret under the DTSA is consistent with the definition under the UTSA, but it “has been expanded to make its application to modern computer technology clearer.” R. Mark Halligan & Richard F. Weyand, *Trade Secret Asset Management 2018*, 145 (2018).
- Arizona adopted the UTSA in 1990, codified at A.R.S. § 44-401 et seq.
- A.R.S. § 44-401(4).
- A trade secret “is one of the most elusive and difficult concepts in the law to define.” *Lear Siegler Inc. v. Ark Ell Springs Inc.*, 569 F.2d 286, 288 (5th Cir. 1978).
- Halligan & Weyand, *supra* note 4 at 17.
- Owners should conduct regular audits of its trade secrets. See Scott F. Gibson, *Important Considerations in Conducting a Trade Secret Audit*, FOR THE DEFENSE, February 2011 at 36.
- For example, a semiconductor manufacturer filed claims for misappropriation of trade secrets against eight former executives who resigned to accept positions with a competitor. *Motorola Inc. v. Fairchild Camera & Instrument Corp.*, 366 F. Supp. 1173 (D. Ariz. 1973). It initially identified 140 alleged trade secrets. Before trial, the company voluntarily dropped its claim to 134 of the alleged trade secrets, and later added four new ones just before and at trial. The court ultimately rejected plaintiff’s claims for misappropriation and chastised the company for its indecision over the trade secrets, finding that plaintiff “did not even know what it was intending to claim.”
- Charles Tait Grave & Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, NORTHWESTERN J. OF TECH. & INTELLECTUAL PROP., Vol 5, No. 1, 68 (Fall 2006).
- Id.*
- RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 *comment d* (1995) (emphasis added). See also *Leucadia Inc. v. Applied Extrusion Techs. Inc.*, 755 F. Supp. 635, 636 (D. Del. 1991) and *Ikon Office Solutions Inc. v. Konica Minolta Business Solutions*, 2009 U.S. Dist. LEXIS 116372, at *11-12 (W.D.N.C. Nov. 25, 2009).
- Xerox Corp. v. International Business Machines Corp.*, 64 F.R.D. 367, 371 (S.D.N.Y. 1974).
- Peat Inc. v. Vanguard Research Inc.*, 378 F.3d 1154, 1158 (11th Cir. 2004).
- Rent Info. Tech. Inc. v. Home Depot USA Inc.*, 268 Fed. Appx. 555, 557 (9th Cir. 2008).
- RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 *comment d* (1995) (emphasis added).
- Cal. Code Civ. P. § 2019.210.
- 260 Cal. App. 2d 244 (1968).
- Id.* at 253.
- See *Engelhard Corp. v. Savin Corp.*, 505 A.2d 30, 33 (Del. Ch. 1986) and *Dura Global Techs., Inc. v. Magna Donnelly Corp.*, 2007 U.S. Dist. LEXIS 89650, at *15-16 (E.D. Mich. Dec. 6, 2007).
- For a thorough analysis of the considerations involved in identifying trade secrets in litigation, see Graves & Range, *supra* note 11, at 68.
- IMAC Corp. v. Cinema Tech. Inc.*, 152 F.3d 1161, 1164-65 (9th Cir. 1998) (emphasis added).
- MAI Sys. Corp. v. Peak Computer Inc.*, 991 F.2d 511, 522 (9th Cir. 1993).
- InteliClear*, *supra* note 2, at 658.
- Id.*, quoting *Imax Corp. v. Cinema Techs. Inc.*, 152 F.3d 1161, 1164 (9th Cir. 1998) (emphasis in original).
- CardioVent Inc. v. Medtronic Inc.*, 483 F. Supp. 2d 830, 844 (D. Minn. 2007); see also *Porous Media Corp. v. Midland Brake Inc.*, 187 F.R.D. 598, 599-600 (D. Minn. 1999) (requiring plaintiff to provide a “list of its trade secrets upon which its allegations are based”).
- Decision Insights Inc. v. Sentia Group Inc.*, 311 Fed. Appx. 586, 589-590, 2009 WL 367585, at *2 (4th Cir. 2009).
- 22 F. Supp. 3d 1305 (N.D. Ga. 2014).
- Id.* at 1331.
- Id.*
- Id.* at 1313.
- Plaintiff described its alleged trade secrets using flabby, generic descriptions, providing nothing that sets the alleged trade secret apart from the general skills and knowledge of the industry. For example, plaintiff does not indicate *why* its “underwriting process” is unique, *how* its additional due diligence requests are focused differently than those its competitors use, or *what* aspects of its business related to “marketing, merchandising, operations, finance, credit and tax” are outside the general knowledge of the business.
- 197 Ariz. 144, 3 P.3d 1064 (Ariz. Ct. App. 1999).
- 3 P.3d at 1067 ¶ 3.
- Id.* at 1067 ¶ 3 n. 2.
- Id.* at 1068 ¶ 10.
- Id.* at 1068 ¶ 10 n. 3.
- InteliClear*, 978 F.3d at 653.
- Id.* at 655.
- Id.* at 658-59. Because the portions of the declarations describing the elements of the “InteliClear System” as trade secrets were filed under seal, the Ninth Circuit referred to those sections in general terms. *Id.*, 978 F.3d at 658 n. 2.
- Id.* at 659.

What is a Trade Secret?

Trade secrets are the oldest form of intellectual property, with origins tracing back to ancient Roman times.¹ Despite this extensive history, a trade secret “is one of the most elusive and difficult concepts in the law to define.”²

The difficulty in defining trade secrets arises in part because a trade secret is intangible, made up of ideas or information that often are not specifically defined. For that reason, “the question of whether certain information constitutes a trade secret ordinarily is best ‘resolved by a fact finder after full presentation of evidence from each side.’”³

Although trade secret protection has been around since ancient times, the area of the law is relatively new and the parameters of trade secret law are evolving. In 1939, the *Restatement of Torts* outlined the first comprehensive definition of trade secrets under American law:

A trade secret may consist of any formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device or a list of customers.⁴

The *Restatement* distinguished a trade secret from other confidential business information, noting that “it is not simply information as to a single or ephemeral events in the conduct of the business” but rather “is a process or device for continuous use in the operation of the business.”⁵ It further acknowledged the difficulty in identifying trade secrets, noting, “An exact definition of a trade secret is not possible.”⁶ Nonetheless, it identified six factors to be considered in determining whether 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 the measures taken by him to guard the secrecy of the information
4. the value of the information to him and to his competitors
5. the amount of effort or money expended by him in developing the information
6. the ease or difficulty with which the information could be properly acquired or duplicated by others⁷

Despite further evolutions in trade secret law, the six factors still provide a useful indication of the trade secret status of information.

Trade secrets are defined and protected under both state and federal law,⁸ and the *Restatement* definition remained the gold standard of trade secret law until 1979, when the National Conference of Commissioners on Uniform State Law approved the Uniform Trade Secrets Act (UTSA).⁹ Commissioners noted that although trade secret law was critically important to interstate commerce, “this law has not developed satisfactorily.”¹⁰ It had developed robustly in commercial centers but had lagged in less-populated jurisdictions whose economies were more agriculturally based.¹¹

The UTSA sought to eliminate this uneven development of the law. Over the past 40-plus years, it has become the standard for defining trade secret law in the United States, with 48 states¹² and the District of Columbia having adopted its scheme. Arizona adopted the UTSA in 1990.

The UTSA broadly defines what constitutes 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 accessible 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 rea-

sonable under the circumstances to maintain its secrecy.¹³

The UTSA prohibits “misappropriation” of trade secrets through “improper means.” While it is impossible to provide a “complete catalogue” of improper means, the UTSA sets forth a partial listing of prohibited conduct, including “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”¹⁴

In addition, “improper means” may include conduct that otherwise might be lawful but that is improper under the circumstances, such as “an airplane overflight used as aerial reconnaissance to determine the competitor’s plant layout during construction of the plant.”¹⁵

While the UTSA prohibits discovery of a trade secret through improper means, it specifically authorizes discovery and use of trade secrets learned through “proper means,” including discovery by:

- independent invention
- reverse engineering
- a license from the owner of a trade secret
- observing the item in public use or on public display
- reading published literature¹⁶

Despite the professed uniformity of the UTSA, states often have their specific interpretations of trade secret law. “While most states have enacted the UTSA in some form, the trade secret protection granted in each state is far from uniform relative to the other states. This often leads to the result that the ability to recover for theft of a trade secret becomes a choice of law or contract interpretation question.”¹⁷

Trade secrets differ from other forms of intellectual property (i.e., patents, trademarks and copyrights) in significant ways:

1. A trade secret has an unlimited shelf life. As long as the information is not commonly known in the industry and the owner takes “reasonable” efforts to maintain the secrecy of the informa-

tion, its trade secret status may last in perpetuity.

2. A trade secret need not be “novel” in the same manner required by patent law. “Although trade secret cases sometimes announce a ‘novelty’ requirement, the requirement is synonymous with the concepts of secrecy and value

... and the correlative exclusion of self-evident variants of the known art.”¹⁸

3. Trade secret status does not convey exclusivity on the holder. As long as they each developed the information through “proper” means, more than one person can claim trade secret status

on the same information, provided that the information has not risen to the level of “public knowledge or of general knowledge in an industry.”¹⁹ Nonetheless, “a trade secret may consist of a combination of elements even though each individual component may be a matter of common knowledge.”²⁰ **AZ**

endnotes

1. “In ancient Rome, trade secret laws established legal consequences for a person who induced another’s employee (or slave) to divulge secrets relating to the master’s commercial affairs.” Karl F. Jorda, *Trade Secrets and Trade Secret Licensing in Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices* (eds. Anatole Krattiger et al.), MHR, 1045 (2007) available at www.IPHandbook.org.
2. *Lear Siegler Inc. v. Ark Ell Springs Inc.*, 569 F.2d 286, 288 (5th Cir. 1978).
3. *Carbo Ceramics Inc. v. Keefe*, 2006 WL 197340 **3, n. 1, quoting *Lear Siegler*, 569 F.2d at 289.
4. RESTATEMENT OF TORTS § 757 cmt. b (1939).
5. *Id.*
6. *Id.*
7. *Id.*
8. See, e.g., Arizona Uniform Trade Secrets Act, Ariz. Rev. Stat. Ann. §§ 44-401 to -407 (West 2019); Defend Trade Secrets Act, 18 U.S.C. §§1831-1839 (2018). In 2016, Congress amended the Economic Espionage Act to add a private civil cause of action. The definition of trade secret is substantially the same under the DTSA and the UTSA.
9. Ironically, the RESTATEMENT (SECOND) OF TORTS did not address the topic of trade secrets.
10. Uniform Trade Secrets Act, *Commissioners Prefatory Note*.
11. *Id.*
12. Massachusetts and New York are the two holdouts.
13. UTSA § 1(4). Arizona uses a substantially similar definition of “trade secret,” which is codified at A.R.S. § 44-401(4).
14. UTSA § 1(1). That same definition of “improper means” is codified under Arizona law at A.R.S. § 44-401(1).
15. UTSA § 1, *Commissioners Comment*. “Aerial reconnaissance” refers to the famous case of *E.I. DuPont de Nemours & Co. Inc. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970), which the court described as “a case of industrial espionage in which an airplane is the cloak and a camera is the dagger.”
16. UTSA § 1, *Commissioners Comment*.
17. J. Derek Mason et al., *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, 15 COMPUTER LAW 14, 15 (March 1999).
18. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, cmt. f (1993).
19. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).
20. *Enterprise Leasing Co. of Phoenix v. Ehmke*, 3 P.3d 1064, 1069 ¶ 17 (Ariz. Ct. App. 1999).

General Skills and Knowledge

Trade secret law protects an employer’s proprietary information from being misappropriated and used improperly. But most information used in a business is not proprietary or novel, even if it is important in operation of the business.

The lack of trade secret status is a rude awakening for many business owners. In the same way that a grandfather might believe that his grandchildren are the smartest, best looking and most talented children in history, a business owner typically believes that everything about his business is special and unique.¹ It is not.

The bulk of the information used in a business does not rise to the level of trade secret status but instead is part of the “know how”—the general skills and knowledge—used by all practitioners of the industry. That fact does not mean the information lacks value. It simply means that the business owner cannot prevent others from us-

ing that commonly known information.

“Information that forms the general skill, knowledge, training, and experience of an employee cannot be claimed as a trade secret by a former employer *even when the information is directly attributable to an investment of resources* by the employer in the employee.”²

General skills and knowledge vary from industry to industry. Defined broadly, they consist of the knowledge and skills possessed by a competent practitioner, i.e., the skills taught to any person embarking in a particular field.

It matters not whether it takes a competent practitioner many years (e.g., a brain surgeon or a rocket scientist) or a few weeks to acquire the general skills and knowledge: An employer “*cannot preclude [a former employee] from exercising the skill and general knowledge he has acquired or increased through experience or even instructions while*

in the employment.”³

Information cannot be protected as a trade secret unless it is outside the general skills and knowledge of the industry. “Trade secret rights are more likely to be recognized in specialized information unique to the employer’s business than in information more widely known in the industry or derived from skills generally possessed by persons employed in the industry.”⁴

An employee has a fundamental right to use the general skills and knowledge learned through his profession:

[T]he right of an individual to follow and pursue the particular occupation for which he is best trained is a most fundamental right. Our society is extremely mobile and our free economy is based on 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. These skills are valuable to such employee in the marketplace for his services. Restraints cannot be lightly placed upon his right to compete in the area of his greatest worth.⁵

Or, as the Arizona Court Appeals vividly explained, a former employee “is not required to undergo a prefrontal lobotomy” when she changes jobs.⁶ Thus, the court rejected an employer’s contention that “the nature of the employment as a dental technician involves ‘trade secrets’” even though the employer testified that “he teaches his laboratory technicians an art: ‘how to hold the spatula’ and how to ‘flow the wax,’ when to use an eyedropper with the wax instead of tweezers, etc.”⁷ The owner could not identify any processes that he used that were “unknown or unavailable to other laboratories.”⁸ In other words, he taught his dental technicians the general skills and knowledge they needed to competently perform their jobs.

Likewise, an employer could not claim trade secret status for sales techniques it

had taught its employee because those techniques were the “subject of books at a public library” and “clearly in the public domain.”⁹ Although those techniques were valuable to the success of the employer’s business, those “general (and generally recognized as sound) methods and principles of doing business could not be the subject

of a misappropriation.”¹⁰

Similarly, an employer could not restrict a departing employee from using “any information” she learned of, possessed as a result of, or accessed through her employment. Nor could the employer reclassify public information as confidential even if “the public has to do ‘substantial searching’ in public publications for it or must combine information from multiple publications to derive it.”¹¹ **AR**

endnotes

1. While it is true that *my* grandchildren fit this description, most other children are not exceptional in every aspect of their lives. But the fact that these other children are ordinary in most ways does not mean that their grandparents should not dote on them. Rather, their “ordinariness” emphasizes how magnificent and remarkable *every* child is (and the corresponding duty that society has to nurture and protect its amazing children). In a similar vein, the “ordinariness” of general skills and knowledge emphasizes how important the discipline is to the customers who rely on the “ordinariness” of that information to address their pressing needs.
2. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. d (1995) (emphasis added).
3. *Lessner Dental Laboratories Inc. v. Kidney*, 492 P.2d 39, 42 (Ariz. Ct. App. 1971) *quoting* *Roy v. Bolduc*, 34 A.2d 479 (Me. 1943) (emphasis in original).
4. *Id.*
5. *Amex Distributing Co. Inc. v. Mascari*, 724 P.2d 596, 603 (Ariz. Ct. App. 1986), *quoting* *ILG Indus. Inc. v. Scott*, 273 N.E.2d 393, 396 (Ill. 1971).
6. *Amex*, 724 P.2d at 603.
7. *Lessner*, 492 P.2d at 41.
8. *Id.*
9. *Amex*, 724 P.2d at 602.
10. *Id.*
11. *Orca Comms. Unlimited LLC v. Noder*, 314 P.3d 89, 95 ¶ 17 (Ariz. Ct. App. 2013).

Protecting Business Information

By Scott F. Gibson

The law protects trade secrets. Other types of confidential information can be protected through narrowly drafted contracts.

Trade Secret, Confidential, or Generally Known

The intercom beeps, followed closely by the cheery voice of your firm's receptionist. "Good morning, Counselor," she says. "Jasper Wilde is in the west conference room. He's anxious to talk to you."

After a few minutes of chitchat, Jasper takes a sip of coffee and turns to the reason for his visit.

"You've been hounding me for years to implement a plan to protect my business information. I'm finally ready to do something."

"I was nervous when the Federal Trade Commission decided to abolish noncompete agreements," he continues. "But I'm breathing easier now that the judge in Texas threw out the FTC rule. So now we've got nothing to worry about. I need you to update my noncompete agreements so that I can keep my employees from competing if they stop working for me."

"Not so fast," you say. "It's not quite that simple."

You explain that although employers may have dodged the proverbial bullet when Judge Ada Brown struck down the FTC rule banning noncompete agreements, the battle over noncompetes is just starting to heat up. First, her decision needs to survive appellate review.

But even if the courts ultimately uphold the ban, restrictive covenants are still in peril. The outrage toward restrictive covenants did not originate with President Biden's direction to the FTC. State legislatures have been rewriting the law of restrictive covenants for years making it increasingly more difficult to restrict former employees from competing.

If that weren't enough, the National Labor Relations Board asserts that noncompetes and other restrictive covenants violate the National Labor Relations Act. And

Congress – on both sides of the aisle – regularly threatens to "do something" about noncompete agreements.

"Change is coming," you note. "You need to increase the likelihood that your restrictive covenants will survive by narrowing the scope of those restrictions. We can help you do that. But we also need to talk about what you can do to protect your business information without using a noncompete agreement."

"Tell me what you mean."

"Some business information belongs exclusively to the Company. We can implement protocols and procedures to safeguard that information. Other information cannot be protected because it belongs in the public arena. We need to talk about how the law classifies business information and how those classifications apply to your business."

"I'm listening, Counselor."

Trade Secrets

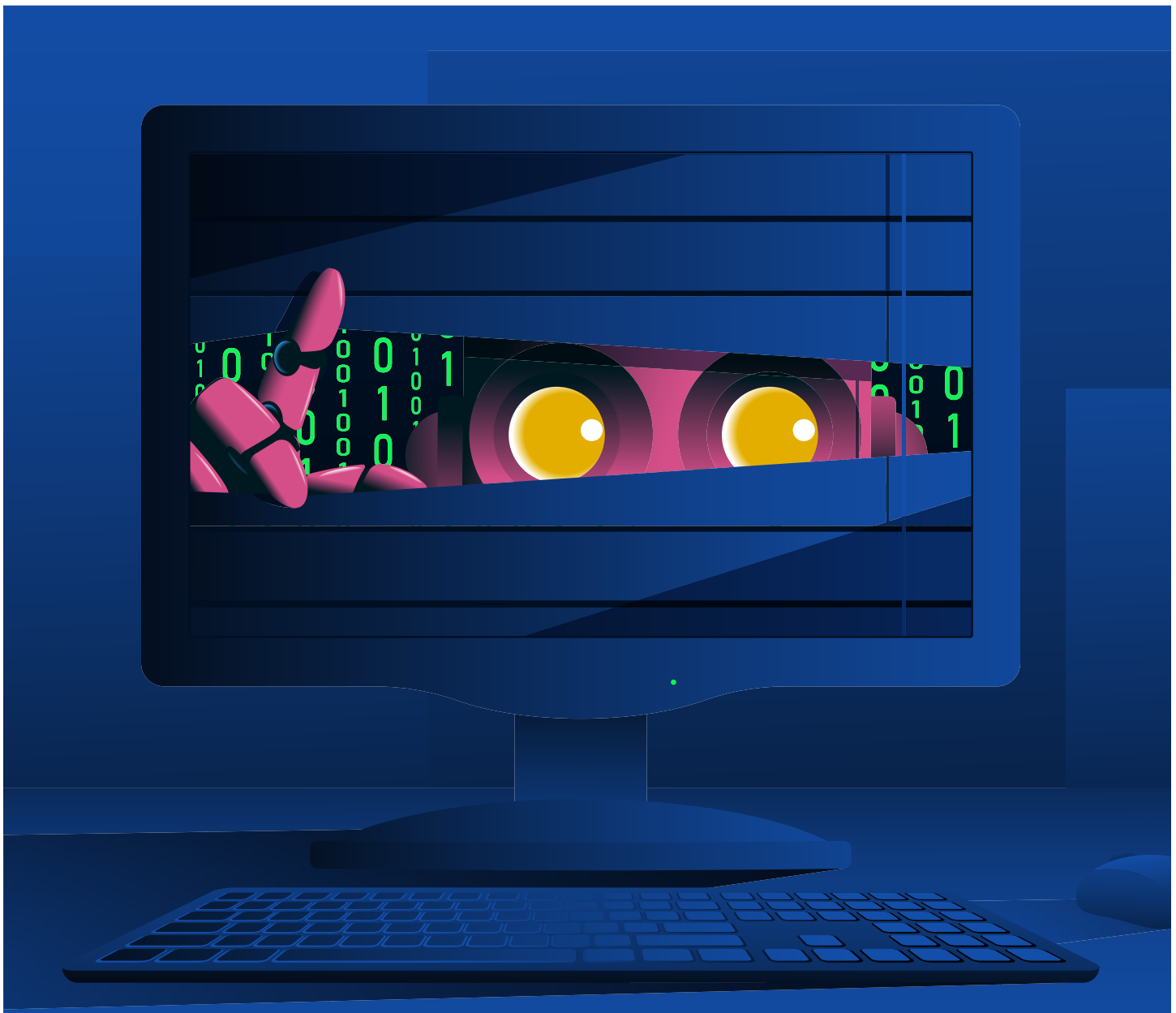
A company's ability to protect business information depends in large part on how the law classifies that information. The law protects trade secrets. Other types of confidential information can be protected through narrowly drafted contracts. But companies cannot lay claim to the lion's share of their business information, as that information is general known in the industry.

Most clients are familiar with the concept of trade secrets, the highest level of protection afforded business information. Both state and federal statutes prohibit misappropriation (think "unauthorized use") of trade secrets.

Every state except New York has adopted some version of the Uniform Trade Secrets Act, which defines a trade secret as



Scott F. Gibson is a partner with the Mesa, Arizona law firm of Denton Peterson Dunn. He is a member of DRI and its Employment and Labor Law Committee. Since 2008, Scott has been an adjunct professor of law at the Sandra Day O'Connor College of Law at Arizona State University teaching a course on Trade Secrets and Restrictive Covenants. He holds LL.M. degrees from Arizona State University (Biotechnology and Genomics) and from Baylor University (Litigation Management).



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.”

Uniform Trade Secrets Act § 1(4). (New York relies on the common law to protect

trade secrets, with similar, though not necessarily identical, results. *Ashland Mgmt. v. Janien*, 82 N.Y.2d 395, 407 (N.Y. 1993)).

In a claim alleging misappropriation, the owner of the alleged trade secret “bears the burden of proving the existence and ownership of a trade secret.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 *comment d*. Meeting that burden is no easy task, as a trade secret is “one of the most elusive and difficult concepts in the law to define.” *Lear Siegler, Inc. v. Ark Ell Springs, Inc.*, 569 F.2d 286, 288 (5th Cir. 1978).

That elusiveness arises in part because the law defines trade secrets broadly. The

definition needs to be broad enough to encompass existing technologies, while still leaving room to technologies and ideas yet to be discovered.

Because a trade secret may consist of any type of information, “[a]n exact definition of a trade secret is not possible.” Restatement of Torts § 757 *comment b* (1939). A trade secret is not limited solely to emerging technologies but may exist in any field.

The modern concept of trade secrets was first discussed in the Restatement of Contracts in 1939. Although the definition of a trade secret has evolved over the years, courts still look to six factors identified by



the Restatement in determining whether 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 the measures taken by him to guard the secrecy of the information;
4. the value of the information to him and to his competitors;
5. the amount of effort or money expended by him in developing the information;
6. the ease or difficulty with which the information could be properly acquired or duplicated by others.

RESTATEMENT OF TORTS § 757 *comment b* (1939).

Jasper looks confused.

"That analysis sounds complicated. Please tell me there's a simple way to determine whether something is or isn't a trade secret," he says.

"I wish I could. But the analysis is based on a number of moving parts. If we're going to protect your information as a trade secret, we need to be prepared to show why it is a trade secret well before anyone has a chance to misappropriate your information."

While government authorities establish the existence of other types of intellectual property, no governmental agency "validates" the existence of trade secrets. The owner simply proclaims that the information is a trade secret, and the proclamation goes unchallenged unless and until litigation arises over the trade secret status.

This lack of governmental oversight creates a practical problem. "The only way to validate a trade secret is through litigation. Absent a court finding that trade secret property rights in information exist, the trade secret status of the information remains alleged but unproven." R. Mark Halligan, Richard F. Weyand, *Trade Secret Asset Management 2018*, 17 (Weyand Associates, Inc. 2018). Indeed, as one court noted, "the question of whether certain information constitutes a trade secret ordinarily is best 'resolved by a fact finder after full presentation of evidence from each side.'" *Carbo Ceramics, Inc. v. Keefe*, 166 F. App'x 714, 718 n. 1 (5th Cir. 2006)(quoting *Lear Siegler*, 569 F.2d at 289).

Many trade secret owners never critically consider the trade secret status of their information until they find themselves in court frantically seeking to prevent the "misappropriation" of that information. Once in court, the owner must prove both that the information is in fact a trade secret and that the defendant misappropriated the trade secret.

A person claiming rights in a trade secret bears the burden of defining the information for which protection is sought with sufficient definiteness to permit a court to apply the criteria for protection . . . and to determine the fact of an appropriation.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 *comment d* (1995) (emphasis added).

The plaintiff must establish "each of [the] statutory elements [of a trade secret] as to each claimed trade secret." *Peat, Inc. v. Vanguard Research, Inc.*, 378 F.3d 1154, 1158 (11th Cir. 2004). This burden requires that "a plaintiff who seeks relief for misappropriation of trade secrets [to] identify the trade secrets and carry the burden of showing that they exist." *Rent Info. Tech., Inc. v. Home Depot USA, Inc.*, 268 F. App'x 555, 557 (9th Cir. 2008).

The owner must typically identify the trade secret with reasonable specificity at the inception of the case, before any discovery occurs. Highly innovative and revolutionary information may be adequately described with a low degree of specificity. On the other hand, "a court may require greater specificity when the plaintiff's claim involves information that is closely inte-

grated with the *general skill and knowledge* that is properly retained by former employees." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 *comment d* (1995) (emphasis added).

For a more detailed discussion of a plaintiff's burden of identifying its trade secrets in litigation, see Scott F. Gibson, *Identifying Trade Secrets in Litigation*, 60 Arizona Attorney 28 (March 2024).

Confidential Information

"Let me see if I understand," Jasper says. "I don't have to do register my information with the government for it to be a trade secret. But the information must be generally unknown to others in my industry and must be valuable because others don't know it. And I've got to take reasonable steps – whatever that means – to make sure the information remains a secret."

"That's right."

Jasper pauses and considers what you have discussed.

"A lot of people in my industry talk about protecting their 'proprietary information.' Is proprietary information the same as a trade secret?"

"All trade secrets are confidential and proprietary," you say, "but not all proprietary information is a trade secret."

Even if some business information does not rise to the level of a trade secret, a company may prevent its employees from using the information through a narrowly tailored nondisclosure agreement. A properly drafted non-disclosure agreement can "clarify and extend the scope of an employer's rights" beyond the scope of protections arising under trade secret law. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 *comment g*.

The non-disclosure obligation must be narrow and precise. A non-disclosure agreement is an unreasonable restraint of trade if it seeks to protect "information that is generally known or in which the [employer] has no protectable interest." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 *comment d*.

"[T]he rules governing trade secrets are still relevant in analyzing the reasonableness and enforceability of non-disclosure provisions because, in order to justify the contractual restraint, information subject to non-disclosure

Many trade secret owners never critically consider the trade secret status of their information until they find themselves in court...

provisions must share at least some characteristics with information protected by trade secret statutes.” *Orthofix, Inc. v. Hunter*, 630 F. App’x 566, 567 (6th Cir. 2016).

“In many ways, ‘confidential information’ under an NDA is both ‘trade secret like’ and ‘trade secret lite,’” you explain. “A company can’t wave a magic wand and transform common knowledge into ‘confidential information,’ no matter what the NDA says. If it wasn’t confidential before the employee signed the NDA, it didn’t suddenly become confidential because she signed an agreement.”

General Skills and Knowledge

“That makes sense,” Jasper says. “Confidential information is information that is like a trade secret, but falls short of the legal definition. If I have a valid contract with my employees, I can protect that information as well.”

“That’s right.”

“So if I have a ‘narrowly tailored’ NDA, I can keep my employees from competing against me,” Jasper says.

“Hold your horses, cowboy. While fair competition allows you to protect your trade secrets and other ‘trade-secret-like’ confidential information, you can’t prevent your employees from using the skills and knowledge that are generally known in your industry.”

Jasper looks puzzled. “What do you mean?”

Many companies vastly overestimate the confidentiality and importance of the information used in their businesses. In the same way that grandparents believe their grandchildren are the most exceptional children roaming the earth, business owners often believe that everything about their business is extraordinary, original, and unique. In reality, however, it is not.

Most information used in a business is neither a trade secret nor otherwise proprietary and protectable. Although that information is important in the operation of the business, it does not belong to the employer, but rather constitutes part of the general base of information used in the industry.

“Information that forms the general skill, knowledge, training, and experience of an employee cannot be claimed as a trade

secret by a former employer even when the information is directly attributable to an investment of resources by the employer in the employee.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 *comment d* (1995).

Specialized knowledge is the gateway to success in any industry. Farmers need to understand how and when to sow, fertilize, and irrigate their crops. Doctors need to master anatomy, physiology, and pharmacology. Plumbers must understand water pressure, building codes, and blueprints. Every industry has its own set of general skills and knowledge.

“General skill is an employee’s personal knowledge based upon his education, ability and experience.” *GTI Corp. v. Calhoun*, 309 F.Supp. 762 (S.D. Ohio 1969). Defined broadly, general skills and knowledge consist of the items that a competent practitioner in the industry holds: the skills taught to any person embarking in the field.

No occupation can function without its base of common knowledge. And because that knowledge base belongs to the industry in general, no employer can claim a proprietary interest in the general skills and knowledge common to the industry.

Rather, general industry knowledge belongs to anyone who takes the initiative to learn the information, whether through formal schooling, training, apprenticeship, or the school of hard knocks. And because the knowledge in every industry is constantly growing, the “general knowledge” in the industry likewise continues to grow.

No matter how long it took the employee to acquire the general skills and knowledge of the industry, an employer “cannot preclude [a former employee] from exercising the skill and general knowledge he has acquired or increased through experience or even instructions while in the employment.” *Lessner Dental Laboratories, inc. v. Kidney*, 492 P.2d 39, 42 (Ariz. App. Ct. App. 1971) (quoting *Roy v. Bolduc*, 34 A.2d 479 (Me. 1943)(emphasis in the original).

“The distinction between trade secrets and general skill, knowledge, training, and experience is intended to achieve a reasonable balance between the protection of confidential information and the mobil-

ity of employees.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 *comment d*.

The non-disclosure obligation must be narrow and precise.

Jasper sighs and downs the last swig of his coffee.

“That doesn’t seem fair,” he says. “I teach them everything I know about the industry and they can go out and compete against me? Where’s the justice in that?”

“It’s the price we pay for a free economy,” you say. “And remember how you got your start in the industry. You worked for MegaTech for 15 years before going out on your own. If you hadn’t learned the business there, you never could have started the Company. Fair competition improves the quality of our lives and makes the economy grow.”

The freedom to compete is fundamental to free enterprise:

The freedom to engage in business and to compete for the patronage of prospective customers is a fundamental premise of the free enterprise system. Competition in the marketing of goods and services creates incentives to offer quality products at reasonable prices and fosters the general welfare by promoting the efficient allocation of economic resources. The freedom to compete necessarily contemplates the probability of harm to the commercial relations of other participants in the market.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1 *comment a*.

While the law protects trade secrets from misappropriation, information cannot be a trade secret unless it is outside the general skills and knowledge of the industry. “Trade secret rights are more likely to be recognized in specialized information unique to the employer’s business than in information more widely known in the industry or derived from skills generally possessed by persons employed in the

industry.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 *comment d* (1995)

In many ways, general skills and knowledge are a type of “anti-trade secret.” Trade secrets are valuable because they are *unknown* to other practitioners in the industry; general skills and knowledge are valuable because they are *known* by all competent practitioners. Without that base of common knowledge, the industry would not exist.

We have airlines because pilots have the skills and knowledge needed to safely take off and land a jet. General aviation skills belong to all pilots. And the rest of us gladly pay to have pilots exercise those skills to take us from Point A to Point B regardless of who they work for and would want those skills going from employer to employer.

What Does This All Mean?

“Your explanation is fascinating, Counselor,” Jasper says, “but it’s also quite academic. I’m a practical man who runs a practical business. Why should I care about how the law classifies my information?”

“I can give you 72 million reasons why,” you reply.

The founders at Zunum Aero envisioned a future with hybrid and electric air craft providing a green alternative to travel. But funding a green future is an expensive endeavor, so Zunum sought funding from various investors, including aviation behemoth Boeing.

After \$9 million of loans, Boeing pulled the plug. Without any sources of revenue, Zunum shuttered its doors.

Zunum sued Boeing under multiple legal theories, including misappropriation of trade secrets. And the jury agreed, awarding Zunum \$72 million in damages.

The victory was short lived, however, as the trial judge granted Boeing’s motion for judgment as a matter of law and vacated the jury award for a simple reason: “Zunum failed to identify any of its alleged trade secrets with sufficient particularity or prove by substantial evidence that its alleged trade secrets derived value from not being generally known to or readily ascertainable by others.” *Zunum Aero., Inc. v. Boeing*, 2024 U.S. Dist. LEXIS 144978, *14 (W.D. Wash. 2024).

Zunum had in fact presented expert testimony stating that its information was a trade secret. But its case failed because those experts never explained *why* the information was a trade secret. Rather, the witnesses simply proclaimed that the information was a trade secret.

Zunum ignored the fundamental rule all aspiring authors know: *show, don’t tell*.

The court vacated the jury award because Zunum did not “provide the jury with any means of reasonably determining the metes and bounds” of its trade secrets. Zunum “failed to provide any non-conclusory testimony or other evidence that [the alleged trade secret] derived value from not being generally known to or readily ascertainable by proper means by other persons.” Zunum simply proclaimed that certain information was “novel, valuable, [and] kept secret,” but did not explain *why* it was novel or valuable or *what efforts* Zunum took to keep the information secret.

In writing parlance, Zunum did a lot of telling and very little showing. And the court properly noted that conclusory testimony cannot meet the owner’s burden of proving the existence of a trade secret.

Jasper shakes his head. “Seventy-two million dollars,” he says pausing for dramatic effect. “That’s a lot of dough.”

“And it all could have been prevented if Zunum had shown the jury why its information met the legal definition of a trade secret. But instead of doing that, it simply had its witnesses recite the elements of a trade secret without explanation. And because Zunum didn’t present evidence showing that its information was outside the general knowledge of the industry, the trial court held that the information was unprotectable general knowledge.”

“What can we do to avoid that problem?” Jasper asks.

“Lawyers and judges are smart people who don’t understand math or science. We need to prepare a smart, articulate witness who can both describe what your technology is and explain why it differs from the knowledge commonly available in the industry. We need to prepare a witness who is a good teacher – someone who can explain your technology so clearly that even a lawyer can understand.”

“That’s a perfect description of Minerva, our chief engineer,” Jasper exclaims. “She

can explain complex engineering concepts in ways that our investors can understand.”

You explain how the Company will need to hold regular trade secret audits to identify, describe, and segregate its trade secrets. The ongoing audits will enable the Company to draft non-disclosure agreements that narrowly identify the “confidential information” they seek to protect. Those audits will set the foundation for ongoing training on how to protect the Company’s most valuable intangible assets.

“As part of that first audit, we can help Minerva refine her descriptions so that she can show that your information is a trade secret,” you say. “I hope that we never need to go into court to protect your trade secrets. But if we do, we’ll have Minerva ready to testify. Her descriptions need to be vivid and specific so that even if the judge doesn’t understand how the technology works, she can understand why the information is a trade secret.”

“Show, don’t tell. I get it,” he says with a smile.

Suddenly, the theme from Mission Impossible blares from Jasper’s cell phone. He answers the call and listens intently to a frantic engineer describing the latest crisis at the office.

“I’ll be right there,” he says as he concludes the call.

Jasper grabs his backpack and makes his way toward the door of the conference room.

“It’s great to see you again, Counselor,” he says. “Thanks for your advice. I’ll have Margo call to schedule our next meeting so that we can stop talking and start implementing our plan.”

