CHAPTER 1

What Is a Trade Secret?

The law of trade secrets is distinguished by the amount of effort that is spent defining its very subject: what is a trade secret? It has been called “one of the most elusive and difficult concepts in the law to define.” Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.3d 714, 723 (7th Cir. 2003) (quoting Lear Siegler, Inc. v. Ark-Ell Springs, Inc., 569 F.2d 286, 288 (5th Cir. 1978)). Similarly, it has been said that “the concept of a trade secret is at best a nebulous one and has been variously defined by case and text authority.” Van Prods. Co. v. General Welding & Fabricating Co., 213 A.2d 769, 775 (Pa. 1965).

There are a number of different definitions of “trade secret”—statutory and common law, state and federal. Case law explores the nuances and distinctions between them and in their application, but certain fundamental principles stand out. All of the definitions and tests are intensely fact-specific. The inquiry centers around secrecy—a trade secret must not be generally known to others and this secrecy must be safeguarded by its owner’s reasonable efforts. A trade secret must also be valuable, and this also arises from secrecy: a trade secret provides a competitive advantage when competitors and prospective competitors do not know it.

I. Sources of Applicable Law

Trade secrets are generally governed by state law. See, e.g., Leggett & Platt, Inc. v. Hickory Springs Mfg. Co., 285 F.3d 1353, 1360 (Fed. Cir. 2002); Thermodyne Food Serv. Prods., Inc. v. McDonald’s Corp., 940 F.
Supp. 1300, 1304 (N.D. Ill 1994). While 46 states have adopted the Uniform Trade Secrets Act (UTSA), the state law of trade secrets is far from uniform. For starters, four states making up close to 20 percent of the U.S. Gross Domestic Product have not enacted it: Massachusetts, New York, North Carolina, and Texas. Many states that have enacted the UTSA have done so with important modifications, and there is significant variance between jurisdictions as to the application of common elements. A primary concern whenever counsel addresses trade secrets will be what law applies.

A. The Uniform Trade Secrets Act
The UTSA was approved by the National Conference of Commissioners on Uniform State Laws in 1979, with amendments approved in 1985. It has been adopted in some form by 46 states and the District of Columbia. It defines a trade secret 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 reasonable under the circumstances to maintain its secrecy.

UTSA § 1(4).

The UTSA also defines trade secret misappropriation at section 1(2) (as discussed in chapter 2 of this book); provides for remedies in sections 2 through 4 (as discussed in chapter 6); and addresses procedural issues arising in trade secret litigation in the remaining sections (as discussed in chapter 5). Section 8 provides that the UTSA “shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of [the UTSA] among states enacting it,” but even in the 46 states that have adopted the UTSA, we are far from having a nationally “uniform” law of trade secrets. Many state legislatures have tinkered with the “uniform” Act. The variances have led a leading commentator to refer to the UTSA as the “non-Uniform Trade Secrets Act.” A practitioner needs to be aware of the many differences among the enacting states’ versions of the UTSA.
Furthermore, even when an UTSA provision is the same in two jurisdictions, this is no guarantee that the courts of the two states have provided a uniform interpretation! For example, although California and Illinois both modified the UTSA’s definition of “trade secret” by eliminating the requirement that a trade secret not be “readily ascertainable by proper means by others,” a California appeals court has ruled that “under California law, information can be a trade secret even though it is readily ascertainable, so long as it has not yet been ascertained by others in the industry,” Abba Rubber Co. v. Seaquist, 286 Cal. Rptr. 518, 529 (Cal. Ct. App. 1991), while an Illinois court reached the opposite conclusion. In Hamer Holding Group, Inc. v. Elmore, 560 N.E.2d 907, 918 (Ill Ct. App. 1990), an Illinois appellate court reasoned that “the key to ‘secrecy’ is the ease with which information can be developed through other proper means: if the information can be readily duplicated without involving considerable time, effort or expense, then it is not secret.”

**PRACTICE TIP**

If you rely upon case law from another jurisdiction construing the UTSA, make sure that the court is construing the same statutory language that your state has enacted. Keep in mind, as well, that the courts of different jurisdictions reach different results on questions of interpretation, even when the statutory language is the same.

**B. State Common Law**

Three of the states that have not adopted the UTSA (Massachusetts, New York, and Texas) continue to rely upon common law principles, largely derived from and reflected in section 757 of the *Restatement (First) of Torts* (1939).10 See, e.g., American Derringer Corp. v. Bond, 924 S.W.2d 773, 776 n.1, 777 (Tex. 1996); Sylmark Holdings Ltd. v. Silicone Zone Int’l Ltd., 783 N.Y.S.2d 758, 771 (N.Y. Sup. Ct. 2004); Jet Spray Cooler, Inc. v. Crampton, 282 N.E.2d 921, 925 (Mass. 1972).10 Indeed, the influence of the *Restatement* formulation is such that it is also frequently applied by courts in UTSA jurisdictions. See, e.g., MTG Guarnieri Mfg., Inc. v. Clouatre, 239 P.3d 202, 209 (Okla. 2010).
The definition of “trade secret” is found in comment b to section 757 of the Restatement (First) of Torts. It states generally that “a trade secret may consist of any formula, pattern, device or compilation of information which is used in one’s business, and which gives an opportunity to obtain an advantage over competitors who do not know or use it,” before providing a six-factor test for determining whether particular information qualifies as a trade secret:

1. The extent to which the information is known outside of the business;
2. The extent to which it is known by employees and others involved in the business;
3. The extent of measures taken by the business to guard the secrecy of the information;
4. The value of the information to the business and its competitors;
5. The amount of effort or money expended by the business in developing the information; and
6. The ease or difficulty with which the information could be properly acquired or duplicated by others.

Restatement (First) of Torts § 757 cmt. b.

The 1995 Restatement (Third) of the Law of Unfair Competition provides, in section 39, a pithier definition of “trade secret”: “any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.” This more recent formulation explicitly instructs that the six factors listed in the Restatement (First) of Torts provide useful guidance but do not comprise a strict, six-part test: “[i]t is not possible to state precise criteria for determining the existence of a trade secret.” Restatement (Third) of Unfair Competition § 39 cmt. d (1995).

Beyond the definition of “trade secret,” common law principles also remain relevant in UTSA jurisdictions. While the UTSA “displaces conflicting tort, restitutionary, and other law providing civil remedies for misappropriation of a trade secret,” UTSA § 7(a), it is far from the only set of rights and remedies that needs
What is a Trade Secret?

to be considered when a trade secret is misappropriated. See UTSA § 7(b) & cmt. UTSA preemption of common law claims does not typically extend to duties to protect competitively sensitive information that are voluntarily assumed through express or implied contracts. Id.; see also, e.g., Frantz v. Johnson, 999 P.2d 351, 358 n.4 (Nev. 2000) (UTSA did not displace claim that former employee breached the implied covenant of good faith and fair dealing). Nor will it usually displace duties imposed by law that do not depend upon the existence of competitively sensitive information, such as a breach of fiduciary duty not solely dependent on the misappropriation of a trade secret. UTSA § 7(a); see also, e.g., AutoMed Techs., Inc. v. Eller, 160 F. Supp. 2d 915, 922 (N.D. Ill. 2001) (UTSA did not displace claim for usurpation of corporate opportunity); Paint Brush Corp. v. Neu, 599 N.W.2d 384, 393 (S.D. 1999) (UTSA did not displace claim for breach of duty of loyalty when employee prepared to compete before resigning employment).

C. Federal Law

There is no general federal law of trade secrets. Various federal statues, however, address trade secrets, and counsel faced with a trade secret issue should be familiar with them. For instance, the Economic Espionage Act of 1996 makes the commercial theft of a trade secret, or the receipt or possession of a trade secret with knowledge that it has been stolen, a federal crime, punishable by up to 10 years’ imprisonment or a $500,000 fine or both. 18 U.S.C. § 1832. (For business corporations or other organizations, the fine can be up to $5 million. Id.)

The Act defines “trade secrets” broadly:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to,
not being readily ascertainable through proper means by, the public.


The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, criminalizes a range of activities involving computers belonging to the federal government or national financial institutions or used in interstate commerce. (The advent of the Internet has made it difficult to find a computer not used in interstate commerce!) While trade secrets are not addressed per se, the CFAA has become an important weapon in the arsenal of a plaintiff alleging trade secret misappropriation under appropriate facts, for instance, the unauthorized access (or access that exceeds authorization) to a protected computer, causing damage. See 18 U.S.C. § 1030(a)(5)(A). The utility of the private right of action provided by CFAA is complicated in the context of trade secret misappropriation, however, by narrow statutory definitions of “damage” and “loss”\(^1\)\(^4\) that do not extend to damages beyond those arising from physical destruction of data.

D. State Criminal Statutes

A number of states have enacted criminal statutes for trade secrets theft. The three states that continue to apply a common law of trade secrets each have a criminal trade secrets statute on the books. See Mass. Gen. L. ch. 266, § 60A (2005) (theft of trade secrets); N.Y. Penal Code § 165.07 (unlawful use of secret scientific material); Tex. Penal Code § 31.05(b) (“A person commits an offense if, without the owner’s effective consent, he knowingly: (1) steals a trade secret; (2) makes a copy of an article representing a trade secret; or (3) communicates or transmits a trade secret.”)\(^15\)

Criminal statutes also exist in a number of UTSA jurisdictions. See, e.g., Fla Stat. § 812.081 (stealing or embezzling a trade secret a felony; adopting a criminal statutory definition of “trade secret”); Minn. Stat. § 609.52 (applying UTSA definition of trade secret); 18 Pa. Cons. Stat. § 3930 (prohibiting theft of trade secrets from computers or computer networks; adopting a criminal statutory definition of “trade secret”); Wis. Stat. § 943.205 (incorporating by reference UTSA definition of trade secret); Wyo. Stat. Ann. § 6-3-501-502 (including among “computer crimes” the disclosure of data which is a trade secret or is confidential).
II. What Factors Determine Trade Secret Status?

Whether under the UTSA or the six-factor test of the first Restatement, the definition of a trade secret shares three basic elements: it is not known to others; its secrecy makes it valuable; and it is the subject of reasonable efforts undertaken to maintain its secrecy. UTSA § 1(2); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b. See, e.g., IDX Sys. Corp. v. Epic Sys. Corp., 285 F.3d 581, 583 (7th Cir. 2002); Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277, 286 (Cal. Ct. App. 2002); Zemco Mfg., Inc. v. Navistar Int’l Trans. Corp., 759 N.E.2d 239, 245 (Ind. App. Ct. 2001); Hoffman-La Roche, Inc. v. Yoder, 950 F. Supp. at 1357-58.

A. A Trade Secret Is Not Known by Others

A trade secret must, in fact, be a secret, and this is frequently described as its principal attribute. See, e.g., Thermodyne Food Serv. Prods., Inc. v. McDonald’s Corp., 940 F. Supp. at 1304 (“whether the information sought to be protected qualifies as a trade secret focuses fundamentally on the secrecy of such information”) (emphasis in original); Dionne v. Southeast Foam Covering & Packaging Inc., 397 S.E.2d 110, 113 (Va. 1990) (“crucial characteristic of a trade secret is secrecy”). It is not necessary—and is rarely feasible—that the secrecy be absolute. Rather, a trade secret must be secret enough “to afford an actual or potential economic advantage over others,” that is, secret enough to make it difficult or costly for outsiders to acquire the information without resort to wrongful means. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39; Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983) (relevant question is whether “under the present state of the art, a prospective competitor could not produce a comparable motor without a similar expenditure of time and money”); see also Cook, Inc. v. Boston Scientific Corp., 206 F.R.D. 244, 248 (S.D. Ind. 2001).

Thus, secrecy is more than a function of the steps taken to protect the trade secret from discovery (a separate inquiry under both the UTSA’s and the Restatement’s definitions); it is also a function of “the ease with which information can be readily duplicated without involving considerable time, effort or expense.” Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209, 215 (Ill. App. Ct. 1995); see also American Derringer Corp. v. Bond, 924 S.W.2d at 776; Sylmark Holdings Ltd v. Silicone Zone Int’l Ltd., 783 N.Y.S.2d at 770-71.

The UTSA’s definition of “trade secret” includes the requirement that the information “derive[ ] 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.” UTSA § 1(4)(i) (emphasis added). Thus, even if the information is not “generally known,” but can be learned without undue effort—for instance, through reverse engineering16—it is not a trade secret.17

Both the comment to the UTSA and the courts agree that information may be classified as a trade secret, regardless of its presence in the public domain or the ability of a competitor to acquire the information, based on the difficulty in discovering the trade secret, for example, through reverse-engineering.

Crane Helicopter Servs., Inc. v. United States, 56 Fed. Cl. 313, 324 (2003) (citing UTSA § 1(4) cmt.); see also C&F Packing Co., Inc. v. IBP, Inc., 224 F.3d 1296, 1302 (Fed. Cir. 2000); Hoechst Diafoil Co. v. Nan Ya Plastics Corp., 174 F.3d 411, 419 (4th Cir. 1999); Walker Mfg., Inc. v. Hoffmann, Inc., 261 F. Supp. 2d 1054, 1082 (N.D. Iowa 2003) (under Iowa’s trade secrets act, “once a device has been publicly disclosed, for example, by public sales, the ease with which the device can be ‘reverse engineered’ is certainly relevant to the question of whether or not the device remains a ‘trade secret’”).

This requirement that trade secret information be sufficiently secret to impart value to its owner and competitors “precludes trade secret protection for information generally known within an industry even if not to the public at large.” Mangren Research & Dev. Corp. v. National Chem. Co., 87 F.3d 937, 942 (7th Cir. 1996). “If the principal persons who can obtain economic benefit from information are aware of it, there is no trade secret.” USTA § 1 cmt. See Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d at 285 (a trade secret is separate from “matters of general knowledge in the trade or . . . special knowledge of those persons who are skilled in the trade”); Stampedede Tool Warehouse, Inc. v. May, 651 N.E.2d at 216 (“an employee’s general knowledge is not a trade secret”); see also Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) (“The subject of a trade secret . . . must not be of public knowledge or of a general knowledge in the trade or business.”).

Novelty in the patent-law law sense is not required. Kewanee Oil Co. v. Bicron Corp., 416 U.S. at 476; Basic American, Inc. v. Shatila, 992 P.2d 175, 185 (Idaho 1999). “A trade secret may be no more than a slight mechanical advance over common knowledge and practice in the art.” SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1255
What is a Trade Secret?


The fact that some or all of the components of the trade secret are well known does not preclude protection for a combination, compilation, or integration of the individual elements, so long as the compilation is a secret. “[E]ven if all of the information is publicly available, a unique combination of that information, which adds value to the information, also may qualify as a trade secret.” Penalty Kick Management Ltd. v. Coca Cola Co., 318 F.3d 1284, 1291 (11th Cir. 2003). In Penalty Kick, the plaintiff’s “Magic Windows” beverage labels “accomplished an effective, successful and valuable integration of the public domain elements” and thus were afforded trade secret protection. Id. (quoting Essex Group, Inc. v. Southwire Co., 501 S.E.2d 503 (Ga. 1998)); see also Basic American, Inc. v. Shatila, 992 P.2d at 186, 189 (method of introducing additives to dehydrated potatoes was a “unique combination of generally known elements”).

A Massachusetts case provides a down-to-earth example. While the “basic ingredients, flour, sugar, shortening, chocolate chips, eggs, and salt, would be common to any chocolate chip cookie,” trade secret protection was afforded to “[t]he combination in which those ingredients are used, the diameter and thickness of the cookie, and the degree to which it is baked.” Peggy Lawton Kitchens, Inc. v. Hogan, 466 N.E.2d 138, 139-40 (Mass. App. Ct. 1984). But see Weins v. Sporleder, 569 N.W.2d 16, 21 (S.D. 1997) (because ingredients in cattle feed supplement were public knowledge, being the first to combine them did not warrant protection).

It is not unheard of for more than one party to possess the same trade secret, if each developed it independently. The “owner of the trade secret [need not] be the only one in the market. Several developers of the same information . . . may have trade secret rights in that information.” Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d at 900; accord Mangren Research & Devel. Corp. v. National Chem. Co., 87 F.3d at 944 n.4; Bestechologies, Inc. v. Trident Env’tl. Sys., Inc., 681 So. 2d 1175, 1176-77 (Fla. Dist. Ct. App. 1996). But, as noted above, this logic cannot be extended too far: if too many competitors have the same trade secret, then it is probably not a “secret.” E.g., Stratienko v. Cordis Corp., 429 F.3d 592, 602 (6th Cir.
2005) (idea must “not be one that is already used by others”); Bestechnologies, Inc. v. Trident Env. Sys., Inc., 681 So. 2d at 1177 (when every competitor has discovered the same process, it has become “generally known” or “readily ascertainable” and is no longer a trade secret).

If a trade secret owner discloses its trade secret to a third party that is under no obligation to maintain the confidentiality of the information or publicly discloses the secret, the information is no longer a trade secret. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1001 (1984). Similarly, there can be “no trade secret protection, as a matter of law, if the secrecy is necessarily lost when the design or product is placed on the market.” LinkCo, Inc. v. Fujitsu Ltd., 230 F. Supp. 2d 492, 498 (S.D.N.Y. 2002). Thus, a hotel room concept was not a trade secret because it was publicly disclosed once the hotel room was built, marketed, and occupied, Hudson Hotels Corp. v. Choice Hotels Int’l, 995 F.2d 1173, 1177 (2d Cir. 1993), and a window crank was not a trade secret because it was “a device that upon marketing and sale is open to public inspection of all of its features,” Blank v. Pollack, 916 F. Supp. 165, 175 (N.D.N.Y. 1996).

B. A Trade Secret Is Valuable

A trade secret possesses “independent economic value, actual or potential,” UTSA § 1(4), and that value is commonly understood to be a substantial business or competitive advantage, e.g., Morlife, Inc. v. Perry, 66 Cal. Rptr. 2d 731, 736 (1997). See Restatement (Third) of Unfair Competition § 39 (a trade secret is “sufficiently valuable . . . to afford an actual or potential economic advantage over others”); Restatement (First) of Torts § 757 cmt. b (a trade secret may consist of information “which gives . . . an opportunity to obtain an advantage over competitors who do not know or use it”). The source of the value is typically the fact that it is unknown to others who might make use of it. See UTSA § 1(4) (a trade secret derives its value “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. . .”).

Under the UTSA, the trade secret owner does not need to be using the trade secret actively in its business, and it does not matter if the trade secret owner has not yet had an opportunity or acquired the means to exploit its trade secret. UTSA § 1 cmt. “[T]he proper criterion is not ‘actual use’ but whether the trade
secret is ‘of value to the company.’” *Learning Curve Toys, Inc. v. Ply-Wood Toys, Inc.*, 342 F.3d at 727 (although plaintiff had never used the invention, defendant’s sales “sky-rocketed” after misappropriation). Under the *Restatement* definition of “trade secret,” a trade secret must be “continuously used in one’s business,” *Restatement (First) of Torts* § 757 cmt. b, although the case law in non-UTSA jurisdictions applies this requirement unevenly. *Compare Astro Tech., Inc. v. Alliant Techsystems, Inc.*, 2005 WL 6061803 (S.D. Tex. Sept. 28, 2005) (“Plaintiff has not presented evidence that it used the alleged trade secret in its business”), *with Elcor Chem. Corp. v. Agri-Sul, Inc.*, 494 S.W.2d 204, 213 (Tex. Civ. App. 1973) (mere fact that plaintiff “was not utilizing the information at the present time does not prevent same from being a trade secret”).

Similarly, the UTSA’s definition of trade secret does not require that there currently be competitors in the field occupied by the trade secret, only that there be actual or potential value to be derived from the secret. *See, e.g., Religious Tech. Ctr. v. Netcom On-Line Comm. Servs, Inc.*, 923 F. Supp. 1231, 1253 (N.D. Cal. 1995). “[O]bsolete information,” on the other hand, “cannot form the basis for a trade secret claim because the information has no economic value.” *Fox Sports Net North, LLC v. Minnesota Twins P’ship*, 319 F.3d 329, 336 (8th Cir. 2003) (telecast agreements of which former employee was aware had been superseded).

The “amount of effort and money spent in developing the information” is considered in determining whether a trade secret is valuable, although it is relevant largely as evidence of “[t]he relative ease or difficulty by which the secret information could be legally acquired or duplicated by others.” *Phillip Morris Inc. v. Reilly*, 113 F. Supp. 2d 129, 137 (D. Mass. 2000). The focus on effort and expense as a proxy for the amount of effort a competitor would need to expend means that trade secret protection can extend to information that has commercial value from a “negative” viewpoint, that is, information about what does not work or should not be pursued. *See UTSA § 1 cmt.* (“lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor”) (emphasis in original); *On-Line Tech., Inc. v. Perkin-Elmer Corp.*, 253 F. Supp. 2d 313, 322 (D. Conn. 2003); *Novell, Inc. v. Timpanagos Research Group, Inc.*, 46 U.S.P.Q.2d 1197, 1217 (D. Utah 1998); *Courtesy Temporary Serv., Inc. v. Camacho*, 272 Cal. Rptr. 352, 357 (Cal. Ct. App. 1990) (valuable information about what will not work, which can only be replicated with a similar expenditure of “work effort”).
Because the real source of value is the amount of “work effort” a competitor would need to expend, a trade secret can also be “valuable” even if its owner did not spend a great deal of money or effort to develop it. A “valuable” trade secret may equally result from a creative flash or intuitive leap, if it could be expected that it would be difficult for the competitor to replicate it. Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d at 728 (“cost was less than one dollar and time spent was less than one-half hour”).

C. A Trade Secret Is Protected by Reasonable Means

Finally, under both the UTSA and the Restatement (First) of Torts, a trade secret must be “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” UTSA, § 1(4); cf. Restatement (First) of Torts § 757 cmt. b (trade secret status depends in part upon “the extent of measures taken . . . to guard the secrecy of the information”).

The UTSA’s language is instructive: efforts to keep the information a secret need not be extreme or unduly expensive; “the standard is reasonableness, not perfection.” TouchPoint Solutions, Inc. v. Eastman Kodak Co., 345 F. Supp. 2d 23, 29 (D. Mass. 2004). The effort need not exceed the need (to educate employees, to warn off competitors, to create a record for litigation, to prevent theft) but must be substantial enough to satisfy it.

PRACTICE TIP

When deciding how much protection is enough, be aware that the circumstances will include a wide spectrum of case-specific factual components. At a minimum, however, these will include

- the value of the information
- the incremental cost of security measures
- the necessity of disclosure
- the foreseeability of efforts to use wrongful means to obtain the secret
- the manner of necessary disclosure and number and type of people to whom it must be disclosed
- industry standards with respect to security
What is a Trade Secret?

It is important to get the balance right because insufficient efforts to maintain the confidentiality of what would otherwise be a trade secret will destroy its legal protection. E.g., Wyatt v. PO2, Inc., 651 So. 2d 359, 363 (La. Ct. App. 1995) (declining to protect a customer list because of a lack of effort to safeguard its secrecy).

The broad array of potential steps a prudent trade secret owner may wish to take is discussed in chapter 3. As dependent as the “reasonableness” of efforts to preserve secrecy is on context, some themes can be discerned in the case law.

➤ A “reasonable effort” means considering the threats to confidentiality and putting in place measures that respond to those threats.

A firm’s list of security measures will be ad hoc in the sense that it will have been adopted in response to the specific threats to security present at that time and place. This can mean the adoption of a large number of precautions targeting different threats to the trade secret. For instance, in Northern Electric Co. v. Torma, 819 N.E.2d 417, 427 (Ind. App. Ct. 2004), a “nonexhaustive” list of steps to maintain confidentiality included

1. requiring employees to sign confidentiality agreements or otherwise advising them of the confidential nature of the process;
2. posting warning or cautionary signs, or placing warnings on documents;
3. requiring visitors to sign in and execute confidentiality agreements;
4. shielding trade secret processes from the view of visitors;
5. segregating trade secret information;
6. using unnamed or code-named ingredients; and
7. keeping secret documents under lock and key.

Similarly, in Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d at 216, security measures included

1. locking certain company offices;
2. checking garbage daily;
3. using of special computer access codes;
4. disseminating customer information was limited to persons on a need-to-know basis;
5. keeping hard copies of customer lists under lock and key;
6. prohibiting sales personnel from removing call books or customer cards from office;
7. installing security cameras; and
8. requiring employees to sign confidentiality agreements.

➤ A combination of “notice” and “physical” measures are typically needed.

“Physical” measures to maintain secrecy (such as limiting access to the secret and prohibiting the dissemination of the secret more widely than necessary) and “notice” measures (such as ensuring that the secret is marked as confidential and requiring employees using the secret to sign confidentiality agreements) are usually both necessary, in one form or another. See, e.g., Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d at 285 (“[R]easonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on a ‘need to know basis,’ and controlling plant access.”); Hoffman-La Roche Inc. v. Yoder, 950 F. Supp. at 1362 (requiring both “some kind of facial indicia that the document is in fact confidential” and physical security measures).

➤ The operational needs of the business itself will influence what steps must “reasonably” be taken.

Security measures must be tailored to the operations of the business and the nature of the secret. For instance, in 205 Corp v. Brandow, 517 N.W.2d 548 (Iowa 1994), the Iowa Supreme Court recognized a restaurant’s need to enforce one set of secrecy measures for its pizza sauce recipe and another set for its pizza crust recipe. The restaurant kept all of the recipes in a safe deposit box and refrained from generally circulating them; however, because of the number of people required to make crust, the crust recipe necessarily faced broader disclosure within the business.

➤ The foreseeability of efforts to misappropriate influences the level of “reasonable” effort needed to protect trade secret status.

“[C]ourts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage.” UTSA § 1 cmt. In adopting reasonable security measures, it is only necessary to protect against reasonably foreseeable security risks. In E.I. du Pont de Nemours & Co. v.
What is a Trade Secret?

Christopher, 431 F.2d at 1015-16, a competitor flew over plaintiff’s plant, taking aerial photographs of new construction. This was not a security breach that the plaintiff was charged with foreseeing and protecting against.

➤ Developments in technology also influence what will be considered a “reasonable effort.”

The digital revolution has completely changed how trade secrets are protected—both because the trade secrets themselves are now often digitized and because developing electronic capabilities have increased the ways in which misappropriation can occur. For instance, since it is now common for cell phones to have cameras and video and audio recording capabilities, allowing a third party to have access to trade secrets without surrendering his cell phone would likely not be reasonable.

III. Examples of Trade Secrets

“The determination of whether information constitutes a trade secret is a highly fact-specific inquiry.” Thermodyne Corp. v. 3M Co., 593 F. Supp. 2d 972, 986 (N.D. Ohio 2008). The “same information that qualifies as a trade secret under one set of facts may not be afforded protection under a different set of facts.” Northern Elec. Co. v. Torma, 819 N.E.2d at 425 (quoting Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 916 (Ind. 1993)). A good argument why a given piece of information should or should not be afforded trade secret protection requires a deep understanding of the facts of the case and close familiarity with the ways in which the statutory and common law tests discussed in this chapter apply to those facts. This section examines some commonly litigated instances in which trade secret protection is sought for types of business information.

PRACTICE TIP

When a dispute arises, it is a common first reaction to look for a case where the same particular category of documents or information was held to be—or not to be—a trade secret. (Did you skip straight to this section when you picked up this book?) Be careful: with the fact-based analysis of the factors discussed herein, it is difficult to make sweeping generalizations about what is or is not a trade secret.
A. Customer Lists

Customer lists comprise perhaps the most frequently litigated category of purported trade secrets. Not surprisingly, the tests discussed above are applied: whether a customer list is protected as a trade secret depends on whether, as a compilation of information, (1) it is valuable, (2) the information is unknown to others, and (3) the owner has taken reasonable steps to keep the information secret. E.g., *Ed Nowogroski Ins., Inc. v. Rucker*, 971 P.2d 936, 944 (Wash. 1999); *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 873-74 (N.D. Ill. 2001). *See also Restatement (Third) of Unfair Competition § 42 cmt. f* (“general rules that govern trade secrets are applicable to the protection of information relating to the identity and requirements of customers”).

Where the customer list can be easily replicated, it is not sufficiently secret and hence not sufficiently valuable to be a trade secret. *Molife, Inc. v. Perry*, 66 Cal. Rptr. 2d at 736 (“[T]he more difficult information is to obtain, and the more time and resources expended by an employer in gathering it, the more likely a court will find such information constitutes a trade secret.”). “A customer list of readily ascertainable names and addresses will not be protected as a trade secret.” *Guy Carpenter & Co., Inc., v. Provenzale*, 334 F.3d 459, 467 (5th Cir. 2003). The bar is typically set quite a bit higher. For instance, in *Vigoro Industries, Inc. v. Crisp*, 82 F.3d 785 (8th Cir. 1996), a list including the identity of 200 farm store customers, together with their planting history, types of products purchased, credit history, and whether they allowed farm store salesman to “scout” farms for insects and perform soil analyses, was not entitled to trade secret protection. All of this information could easily be discovered, the court ruled, because customers farmed in small geographic areas and interested farmers would readily provide information calculated to help them purchase appropriate farm supplies inexpensively. *Id.* at 790-91.

On the other hand, an electricity supplier sought to protect a customer list that included specific individual contact information for each customer, each customer’s order history information, the rates paid by each customer, customer-specific product type information, customer contract renewal dates, and customer energy usage data. Even though each type of information was publicly available, the court ruled that the suppliers would likely be able to establish a trade secret: the information had been accumulated over a long period of time and only by entering into a contract
What is a Trade Secret?

with each customer and its value to a competitor was clear on its face. Liberty Power Corp. v. Katz, 2011 WL 256216, at *3 (E.D.N.Y. Jan. 26, 2011). Similarly, customer information in an insurer’s database was a trade secret when the customer names were filtered for their suitability to buy insurance. The owner of the database derived independent economic value from this information not being generally known to or readily ascertainable by competitors. American Family Mut. Ins. Co. v. Roth, 485 F.3d 930, 933 (7th Cir. 2007).

B. Social Media Followers

As marketing moves from traditional venues onto social media platforms, lists of social media followers can become as important as traditional customer lists. At least one court has considered whether a compilation of account followers on the social media site Twitter constitutes a trade secret. In PhoneDog v. Kravitz, 2011 WL 5415612, at *1 (N.D. Cal. Nov. 8, 2011), an interactive mobile news and reviews web resource sued a former employee for, among other things, misappropriation of trade secrets where the former employee continued to use the Twitter account provided to him as part of his employment. The company claimed that the identities of the approximately 17,000 Twitter account followers were trade secrets under the California Uniform Trade Secret Act. The former employee sought dismissal of this claim under Federal Rule of Civil Procedure 12(b)(6), arguing that the account followers were not trade secrets because “they are and have been publicly available for all to see at all times.” Id. at *6. The court declined to dismiss the claim since determination of whether the account followers are trade secret required consideration of evidence outside the complaint and, therefore, was more appropriately decided upon a fully developed evidentiary record at the summary judgment stage. Id. at *7.

C. Identity of Industry Contacts

The identity of “industry contact people does not rise to the level of a trade secret because this type of unprotected information is readily ascertainable within a trade.” Fox Sports Net North, LLC v. Minnesota Twins P’ship, 319 F.3d at 336; accord Bradbury Co., Inc. v. Teissier-duCros, 413 F. Supp. 2d 1209, 1225 (D. Kan. 2006) (plaintiff failed to establish identity of its “high level” contacts were not known or readily ascertainable); Softchoice Corp. v. MacKenzie, 636 F. Supp. 2d 927, 937 (D. Neb. 2009) (knowledge of industry contact
people is readily ascertainable within a trade); Fleming Sales Co., Inc. v. Bailey, 611 F. Supp. 507, 514 (N.D. Ill. 1985) (information about personnel of the customers with whom salesman did business was “part and parcel of a salesman’s experience” and not a trade secret). But see B.U.S.A. Corp. v. Ecogloves, Inc., 2006 WL 3302841, *4 (S.D.N.Y Jan. 31, 2006) (while plaintiff’s corporate customers were not a trade secret, the names of specific contacts at those companies were because they were not readily available to others in the industry, plaintiff took numerous measures to protect the information, and defendant could only reproduce the information with great difficulty).

D. Customer Contract Renewal Dates
A competitor’s customer’s contract renewal dates can be very valuable because they indicate when a customer may be most susceptible to marketing efforts. Although these might be obtained from the customers themselves, where “it would be a monumental task to duplicate plaintiff’s customer expiration dates,” they may be afforded trade secret status. TIE Sys., Inc. v. Telcom Midwest, Inc., 560 N.E.2d 1080, 1085 (Ill. App. Ct. 1990). To be contrasted are situations in which an employee either recalls the information or receives the information directly from the customers. Millet v. Crump, 687 So.2d 132, 136 (La. Ct. App. 1996) (information about renewal dates an insurance agent could recall or was told owing to a long-term business and social relationship were not trade secret).

E. Information about Suppliers
Information about suppliers—prices charged and lead time—is generally not afforded trade secret protection because it is already in the hands of the vendors, who have every right to market their goods and services, and is available to competing consumers of those suppliers’ wares. Restricting the free dissemination of information about suppliers would put an “undue burden on the innocent vendors, as well as place an artificial constraint on the free market.” SI Handling Sys., Inc. v. Heisley, 753 F.2d at 1257 (knowledge of suppliers’ lead times is in the hands of those very suppliers “who have every incentive, and every right, to disclose it to their customers”); see also Australian Gold, Inc. v. Hatfield, 436 F.3d 1228, 1245 (10th Cir. 2006) (list of suppliers that “sets out only a collection of suppliers whom any participant in the industry would presumably be able to access” not a trade secret); Minnesota Mining & Mfg.
What is a Trade Secret?

Co. v. Pribyl, 259 F.3d 587, 605 (7th Cir. 2001) (suppliers of commercially available resin product not a trade secret); Tyson Metal Prods, Inc. v. McCann, 546 A.2d 119, 122 (Pa. Super. 1988) (supplier price list not a trade secret).

On the other hand, when the circumstances demonstrate that the information could not be independently developed by a competitor, or could be developed only with a great deal of effort, supplier information may be afforded trade secret protection. See Elm City Cheese Co., Inc. v. Federico, 752 A.2d 1037, 1046 (Conn. 1999) (as part of plaintiff’s “unique” overall business plan, list of milk suppliers was protected); Sigma Chem. Co. v. Harris, 794 F.2d 371, 372-75 (8th Cir. 1986) (specialty chemical company’s information about which vendors supplied which chemicals at requisite quality and price was not public knowledge and chemical company took extensive measures, including armed guards, color-coded badges, and work rules concerning removal of files, to prevent dissemination); Yeti by Molly, Ltd. v. Deckers Outdoor Corp., 259 F.3d 1101 1108 (9th Cir. 2001) (identity of boot designer’s suppliers and particulars about materials supplied could be trade secret).

F. Pricing Information

Information relating to cost and pricing may be entitled to trade secret protection if its “value . . . lies in the fact that it is not generally known to others who could benefit by using it, or could not be acquired through general skills and knowledge.” Delta Medical Sys. v. Mid-America Medical Sys., Inc., 772 N.E.2d 768, 791 (Ill. App. Ct. 2002). That is, to be entitled to trade secret protection, pricing information cannot simply be the application of commonly used industry formulas or readily available industry information. There must be some component that is unique to the trade secret owner. For instance, in Delta Medical, pricing offered by a medical equipment vendor was a function of the type of equipment, its age, and its service history, all of which was readily available from the manufacturer. Id. at 791. See also Progressive Prods., Inc. v. Swartz, 258 P.3d 969, 978 (Kan. 2011) (customer pricing not protected because price list was “available to customers, and customers were free to communicate with each other how much they were paying for certain work”); Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d at 287-88 (if pricing information is just commonly used industry formula, it is not a trade secret); AEE-EMF, Inc. v. Passmore, 906 S.W.2d 714, 723 (Mo. App. Ct. 1995) (price list that former employee could have
replicated based on industry knowledge was not a trade secret). But see Avery Dennison Corp. v. Kitonas, 118 F. Supp. 2d 848, 854 (S.D. Ohio 2000) (cost and price files were trade secret when password protected and employee access limited).

In other cases in which price and cost information is not available from third parties or otherwise based on industry-wide information, cost and price information has been afforded trade secret protection. See, e.g., SL Handling Sys., Inc. v. Heisley, 753 F.2d at 1260 (“costing” and “pricing” information “is not information that is readily obtainable by anyone in the industry” and thus qualifies for trade secret protection); Cardinal Freight Carriers v. J.B. Hunt Transp. Servs., Inc., 987 S.W.2d 642, 645-46 (Ark. 1999) (margins of profitability used in pricing model were a trade secret). In Burbank Grease Services LLC v. Sokolowski, 693 N.W.2d 89 (Wis. App. Ct. 2005), the court drew a distinction between “pricing information” and the actual price charged the customer. The former could be protected, it held, if based upon a complicated or unique formula, of which the customers as well as competitors were ignorant. The price actually charged to a customer, on the other hand, could not be protected as a trade secret because a third party might, in the absence of a confidentiality agreement, obtain it from the customer. Id. at 96.

G. Market Research

Market research may in some circumstances qualify as a compilation of information protectable as a trade secret. E.g., Air Prods. & Chems. v. Johnson, 442 A.2d 1114, 1121-22 (Pa. Super. 1982). For instance, “[m]arketing research can be trade secret if it ‘explores the needs of numerous, diverse buyers,’ but is not protectible if it ‘relates to a single prominent buyer that is presumably aware of its own needs and which would naturally like to choose among competing sellers.’” Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d at 288 (quoting SL Handling Sys., Inc. v. Heisley, 753 F.2d at 1259).

Market research questions that were specifically designed for public consumption on a toll-free telephone message were not entitled to trade secret protection. Strategic Decisions Group, Inc. v. Bristol Myers Squibb Co., 293 F.3d 1062, 1065 (8th Cir. 2002). Sales manuals reflecting the results of market research conducted by plaintiff were entitled to trade secret protection where extensive steps had been taken to prevent dissemination of sales manuals.
What is a Trade Secret?


H. Market Strategy or Business Plan

Marketing strategies can be trade secrets, while general business knowledge cannot. A marketing strategy must be unknown to competitors and not readily ascertainable to be entitled to trade secret protection. *IKON Office Solutions, Inc. v. America Office Prods., Inc.*, 178 F. Supp. 2d 1154, 1169-70 (D. Or. 2001). For instance, in *Bradbury Co., Inc. v. Teissier-duCros*, 413 F. Supp. 2d at 1223, the court noted that plaintiff’s ‘‘Australian strategy’ . . . consisted of nothing more than a plan to sell products in Australia’ and would not be protected, while in *Allied Erecting & Dismantling Co., Inc. v. Genesis Equipment & Manufacturing, Inc.*, 649 F. Supp. 2d 702, 719 (N.D. Ohio 2009), it was held that a jury question existed whether a business plan that included “detailed engineering data, cost data, and production/scheduling information” constituted a protectable trade secret. As the Connecticut Supreme Court explained when extending trade secret protection to a cheese producer’s business plan in *Elm City Cheese Co. v. Federico*:

Elm City’s business is unique. If the business were not unique—that is, if both the individual components of Elm City’s business plan, and the way in which those components are combined, were generally known—Elm City arguably would not be entitled to trade secret protection. . . .

752 A.2d at 1048.

Notes


4. See Appendix A for the full text of the UTSA, with the 1985 amendments.

5. A comprehensive list of state statutes adopting the UTSA, in whole or in part, is found in Appendix B.

6. Pooley, supra note 3, § 2.03[1].

7. Several states adopted the 1979 UTSA, with amendments, while others have adopted the 1985 revision, with amendments. Still others, including notably California and Illinois, incorporate portions of both UTSA revisions in their state statutes. For a detailed discussion of the differences among the various state acts, see Samuels and Johnson, The Uniform Trade Secrets Act: The States’ Response, 24 Creighton L. Rev. 49 (1990), reprinted in 24 Intell. Prop. L. Rev. 509 (1992).

8. For a more thorough discussion of these differences, see Brian M. Malsberger, Trade Secrets: A State-By-State Survey (4th ed. 2011).

9. The text of Section 757 of the 1939 Restatement of Torts, with its influential comments, is reproduced in Appendix C.

10. In Massachusetts, a statutory tort for the theft of trade secrets, Mass. Gen. L. ch. 93, § 42, enables the imposition of up to double damages for a violation of the statute. The Massachusetts Appeals Court has, however, noted that “we do not in any way intimate that these statutes change the ambit of trade secret protection in a civil action.” Chomerics, Inc. v. Ehrreich, 421 N.E.2d 453, 458 n.14 (Mass. App. Ct. 1981).

11. Sections 39 through 45 of the Restatement (Third) of Unfair Competition are reproduced in Appendix D.

12. Like the UTSA, the Restatement (Third) of Unfair Competition also addresses misappropriation, §§ 40–43, and provides guidance on remedies, §§ 44–45.

13. The UTSA’s preemption of common law claims for trade secret misappropriation, an important and sometimes complicated concern for trade secret litigators, is discussed in chapter 5, section III.

14. “Damage” is defined as “impairment to the integrity or availability of data, a program, a system, or information,” 18 U.S.C. § 1030(e)(8), while “loss” is defined as
any reasonable cost to any victim, including the cost of respond-
ing to an offense, conducting a damage assessment, and restor-
ing the data, program, system, or information to its condition
prior to the offense, and any revenue lost, cost incurred, or other
consequential damages incurred because of interruption of
service.

18 U.S.C. § 1030(e)(11). Thus, the statutory definition focuses on dam-
age to the computer or data itself—and consequential damages that
may arise from the unauthorized access (such as security consultants
and identity theft protection)—but not on the damage to the trade secret
owner’s competitive position caused by the misappropriation of a trade
secret. See, e.g., Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d
704 (N.D. Ill. 2006) (damages caused by trade secret misappropriation
do not constitute “damage” under CFAA); ResDev v. Lot Builders Ass’n,
diminution in the completeness or useability of data or information on a
computer system”).

15. Some of these state criminal statutes employ a statutory defi-
nition of “trade secrets” that may be different—typically narrower and
more specific—than either the UTSA or the common law. For instance,
the Texas criminal statute defines a “trade secret” as “the whole or any
part of any scientific or technical information, design, process, proce-
dure, formula, or improvement that has value and that the owner has
taken measures to prevent from becoming available to persons other
than those selected by the owner to have access for limited purposes.”
Tex. Penal Code § 31.05(a)(4).

16. Reverse engineering, the process of “starting with the known
product and working backward to divine the process which aided in its
development or manufacture,” Kewanee Oil Co. v. Bicron Corp., 416 U.S.
470, 476 (1974), is, without more, a “proper means” of learning a trade
secret. See chapter 2, section 1.

17. California omitted the “readily ascertainable” language when it
adopted the UTSA, see Cal. Civ. Code § 3426.1(d)(i), so this is not part of
the definition of a trade secret in California. Abba Rubber Co. v. Seaquist,
286 Cal. Rptr. at 528. A defendant in California thus cannot argue that
information is not a trade secret because a product in which it has been
incorporated would be easy to reverse engineer unless the product has
actually been reverse engineered and the information divulged to the
industry. Id.; see also Imax Corp. v. Cinema Tech., Inc., 152 F.3d 1161, 1168
n.10 (9th Cir. 1998) (same). As discussed briefly in section I, the courts of
Illinois appear to disagree.

18. Thus, if the trade secret information is disclosed in a patent,
there is no trade secret. On-Line Techs., Inc. v. Perkin-Elmer Corp., 253 F.
Supp. 2d 313, 324 (D. Conn. 2003). See also Rototron Corp. v. Lake Shore Burial Vault Co., 712 F.2d 1214, 1215 (7th Cir. 1983) (the “process cannot be regarded as a trade secret, because the grant of a patent automatically constitutes full disclosure of the patented process”).

19. This reflects an important policy behind trade secret legislation. As the Alabama state legislature commented, “The trade secret statute is not intended to serve as a privacy statute; rather, it is designed to encourage exploitations of information that can provide valuable goods or services to the public.” Ala. Code § 8-27-2 cmt. a.

20. The Restatement (Third) of Unfair Competition does not include reasonable protection measures in its definition of trade secrets. Restatement (Third) of Unfair Competition § 39. Instead, whether the owner has employed reasonable protection measures is a factor in determining whether the trade secret was acquired by wrongful means. Id. § 43 cmt. c.