Protecting Trade Secrets: 
Maximizing the Chances of Proprietary Information 
Being Deemed a Trade Secret 

Douglas E. Dexter and Jessica Beckett-McWalter

Shin-Guo Tsai gave notice of his resignation as a design engineer at Volterra, a Fremont semiconductor company, allegedly telling his employer that he was retiring to Taiwan to get married. In fact, Tsai had downloaded information on Volterra’s products and sent it to a Taiwanese startup company that had recruited him for a new job. After Volterra and the FBI confronted Tsai, the FBI arrested him. He is now out on bail awaiting trial.1

Misappropriation of a company’s confidential information most commonly results from employee or contractor access to the information.2 Although some employers attempt contractually to prevent employees from competing after termination, courts in many jurisdictions are reluctant to enforce such agreements for fear of precluding the former employee from pursuing his or her profession. Rather than focusing on the “reasonableness” of the noncompete agreement, courts in many jurisdictions are increasingly examining whether the employer is protecting a bona fide trade secret in attempting to limit former employees’ competitive behavior.

Thus, employers concerned with unfair competition from ex-employees would best focus their efforts on establishing a record supporting trade secret characterization of key confidential information. The good news is that trade secret characterization can be dramatically strengthened by the employer’s own actions. This article is designed to help focus those steps. Part I of the article discusses how to identify potential trade secrets and establish a record supporting that characterization. Part II, to be published next month, will discuss how an employer can act to discourage trade secret misappropriation both as its employees go to competitors and as it hires employees away from its competitors.

Identifying Potential Trade Secrets

Most states have adopted the Uniform Trade Secrets Act (UTSA) or a version of it.3 The definition of a trade secret under the UTSA consists of three elements: (1) information (2) that derives independent value, actual or potential, from not being generally known to the public and not readily ascertainable by proper means, and (3) that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.4 Thus, the first step is to identify that information that may be deemed valuable by virtue of its secrecy. Employers should then focus their demonstrable efforts on sustaining that secrecy.
Of course, protectable information may take many forms. Technical information about a manufacturing process is the paradigmatic type of trade secret, but it only begins the list. Field information bulletins or diagnostic software containing technical information used by a company in repairing and servicing its products may be a trade secret. A program may be a secret when the source code is secret, even if the object code is not. Trade secrets may also relate to the company’s sales process in the form of confidential customer lists, marketing plans, and pricing information.

**Defining What Is “Unknown to Others” and “Not Readily Ascertainable”**

Trade secret law is designed to protect and encourage modern high-technology innovations by granting inventors the legal right to protect this resultant competitive advantage. Put another way, they grant protection of confidential information resulting from hard work. Thus, “unknown to others” and “not readily ascertainable” are generally understood to mean that the owner’s time and effort has created information not publicly available. If the information did not require effort or time to acquire or develop, it would be easy for another person to replicate it and does not warrant trade secret protection. One court stated as a general rule that the more difficult it is to gather the information and the more time and resources expended by the employer to gather such information, the greater the likelihood that a court will consider the information a trade secret.

Information that is public, self-evident, or readily ascertainable will not be deemed a trade secret no matter how closely it is held within the company. Thus, trade secret protection is mutually exclusive from patent protection. In filing the patent, the holder of the secret exchanges its trade secret interest in the technology for the patent’s limited monopoly. The information then becomes public (although still proprietary) as part of the process and moves into the public domain when the patent expires.

Information that is “unknown to others” and “not readily ascertainable” can be a trade secret. For example, courts have found such things as the secret recipes for pizza crust and sauce and the drawings and specifications relating to airplane cockpit windows protected as trade secrets. In addition, courts have deemed a chemical formula and its mixing instructions, the source code of a software program, and a customer database and the accompanying field information bulletins that contained technical data to aid in the repair and servicing of computers protected as trade secrets. These pieces of information were granted trade secret protection because the owner kept the information secret from competitors and the public alike. The courts consider the specific circumstances surrounding the information in determining whether it is “unknown to others” and “not readily ascertainable” and thus secret and warranting trade secret protection.

Even though the public could see the object code of the software, for example, the source code was granted trade secret protection because the software was copy protected in such a way that an expert programmer, let alone the general public, could not gain access to the source code; thus it was “not readily ascertainable.”

Trade secret protection does not inure to what a court finds to be within common knowledge. The Ninth Circuit, for example, held that recipes for American culinary staples, such as barbecued chicken and macaroni and cheese, were not protectable as trade secrets. The owners of Old Country Buffets, Inc., accused its competitor of misappropriating Old Country Buffets’ recipes when it opened a competing restaurant that served the same food.
reasoned that the recipes were little more than typical American fare” and so obvious that they were “readily ascertainable” by the general public and not entitled to trade secret protection.19

Similarly, trade secrets do not include information that is primarily based on common sense or that becomes common practice in an industry. In one case, for example, the employer claimed that its employment counseling instruction techniques were trade secrets. The instruction techniques included the program being conducted on consecutive days beginning with Wednesday, conducting instructor review and critique of thank you notes, holding a surprise cocktail party prior to the normal ending time on the last day of class, and conducting dress rehearsals for job interviews.20 The court concluded that each of these items was already a matter of common public knowledge or completely disclosed to students taking the course.21 Therefore, the court declined to permit the employer to “appropriate as his own ‘secrets’ common pedagogical and job search techniques which would be used in any job placement course.”22

Even reading information to potential customers may defeat the trade secret status. A court held, for example, that telemarketing scripts could not be trade secrets, because they had been disclosed in the course of use.23 Similarly, another court concluded that the posting on the Internet of religious writings from the Church of Scientology by someone other than the church owner makes them “generally known” to potential competitors of the church owner, thus rendering them not secret.24 “Once trade secrets have been exposed to the public,” the court said, “they cannot later be recalled.”25 This is so even if the use of the product itself causes the disclosure.26

Courts are reluctant to protect customer lists if they embody information that is readily ascertainable through public sources, such as business directories. If the employer has expended time and effort identifying customers with particular needs or characteristics, however, courts will prohibit former employees from using this information to capture a share of the market.27 Protection of trade secrets may cover information that “is sophisticated .. . and irrefutably of commercial value and not readily ascertainable to other competitors,”28 such as billing rates, key contacts, specialized requirements, and markup rates.

In one case, for example, a customer list that a roofing company developed over time that included contact information as well as pricing information, knowledge about particular roofs, and roofing needs of customers was deemed to have independent economic value.29 The roofing company expended time and effort identifying customers with particular needs, so it would be unfair to allow a former employee-turned-competitor to benefit from these sales efforts by selectively and more effectively focusing on only certain identified customers.30 Similarly, in a Florida case involving a company that customized clothing with fraternity emblems, the court awarded protection to a list of 6,800 fraternities and sororities that included a detailed purchasing history for each sorority and fraternity that had ordered from the company.31

Confidentiality of the Information Must Have Independent Economic Value

The analysis of whether the information is readily ascertainable and whether the secrecy of the information has independent economic value overlaps, and courts frequently discuss these elements together. The purpose of trade secret law is to protect the owner’s competitive advantage derived from the secrecy. If the information is “readily ascertainable” by the public, the owner cannot derive independent economic value from the secrecy of the information. It therefore follows that in addition to being secret, the confidentiality of the information must add
value to the information itself. That value added (actual or potential) is the property of the owner of the secret.

The confidentiality of the information must make the information more valuable to the proprietor as well as to his or her competition. For example, when a faithless corporate officer used a confidential list of employee salaries to help him recruit his coworkers to defect to the competition, the court held that he had violated his fiduciary duty to the corporation by using its confidential information against it. The court also held, however, that the list was not a trade secret, because the information did not have any independent economic value. The court reasoned that keeping salary information confidential does not necessarily give the owner a competitive advantage in a given industry, because it does not relate to the product being sold. In another case, old technical drawings for a workbench already in production were held not to be trade secrets because they had long since lost any economic value to the manufacturer due to the fact that the company was no longer solvent.

In contrast, confidential information about one company’s pricing strategy that would allow a competitor to gain an unfair pricing advantage in the relevant market has independent value to the owner, while marketing research regarding the general industry formulas for setting prices does not. For example, a company’s secret information about its “pricing, profit margins, costs of production, pricing concessions, promotional discounts, advertising allowances, volume rebates, marketing concessions, payment terms and rebate incentives . . . have independent economic value because [it] would be valuable to a competitor to set prices which meet or undercut” their own. Keeping this information secret is valuable to the owner because it allows the owner to compete in the industry effectively. On the other hand, general market industrywide pricing formulas do not have independent value; they are not secret and do not provide a market advantage to the owner of the information because everyone in the industry has access to it.

Reasonable Efforts to Maintain Secrecy

Once an employer has identified information potentially worthy of trade secret protection, steps taken to protect the information’s secrecy have the dual value of minimizing disclosure and maximizing trade secret legal characterization. The degree of such demonstrable efforts will indicate to a court whether the owner truly valued the information’s secrecy or is merely attempting to thwart the legitimate success of a competitor or former employee. Therefore, a program designed to maintain secrecy is not only good policy, it is essential for statutory trade secret protection.

Courts’ Expectation of a Combination of Security Measures

Common security methods include:

1. Requiring employees to sign confidentiality agreements and otherwise advising them of the confidential nature of the information;
2. Posting warning or cautionary signs or placing warnings on documents;
3. Requiring visitors to sign confidentiality agreements or shielding a process from their view;
4. Segregating information;
5. Using unnamed or codenamed ingredients; and
6. Keeping secret documents under lock or password with access provided on an as-needed basis.\textsuperscript{36}

Generally, courts expect to see a combination of measures that keep nonemployees from gaining access to the information and measures that put employees on notice of their responsibilities regarding confidential materials. In one case, for example, security measures recognized as sufficient to protect engineering technology, drawings of notes, quality controls, and testing procedures included extensive internal controls (\textit{e.g.}, visitor logs, signout sheets for proprietary documents, and a document destruction policy), the use of locked storage cabinets in the engineering department, the use of restrictive legends on the documents, and a policy that engineering notes and detailed plans and drawings used in the manufacturing process were never made available to third parties.\textsuperscript{37}

An Illinois court found that the measures implemented by PepsiCo to protect its trade secrets were not only reasonable but more than what was required under trade secret law.\textsuperscript{38} PepsiCo provided confidential information to employees only on a need-to-know basis, regularly marked documents “private and confidential,” required all personnel with access to confidential information to execute a nondisclosure agreement, and emphasized to attendees of meetings at which confidential information was discussed that the information was confidential.\textsuperscript{39}

Similarly, the Fourth Circuit Court of Appeals found that the security measures used for software were reasonable, because the owner of the software regulated both employee and outsider access to the software. In addition to internal security measures, owner only licensed two complete versions of the software, got promises from the recipients that they would not copy or transfer or use the program for any purpose other than its intended purpose, and implemented a password system to prevent unauthorized access to the software.\textsuperscript{40}

Yet, courts will recognize the practical necessity of widely circulating some information within a workplace. In a case in which the owner of a pizza place sought protection of the recipe for the pizza crust and pizza sauce, for example, the court recognized that the “realities of crust preparation differed from those involved in the sauce preparation to an extent requiring different confidentiality procedures.\textsuperscript{41} Unlike the sauce recipe, which was kept in a safe-deposit box at all times, the crust recipe was known by the kitchen employees who prepared the dough because it had to be made daily.\textsuperscript{42} The court held that under the circumstances specific to the use of the crust recipe, the owner of the recipe made a reasonable effort to keep the crust recipe confidential.\textsuperscript{43}

Evidence of the safeguards used within the information itself may demonstrate the proprietor’s reasonable efforts to keep information confidential. A court concluded, for example, that although the object code of a certain version of software was publicly available, the source code was not accessible to the public because the owner of the software had copyprotected the software so that the public could not copy it.\textsuperscript{44} The internal safeguard within the software was adequate to show that the owner of the software made a reasonable effort to protect the confidentiality of the source code.\textsuperscript{45}

Written confidentiality policies and agreements between employer and employee that specifically reference the information for which trade secret protection is sought are critical evidence of efforts to keep information confidential. In the roofing customer list case, for example, the court noted that the employment contract included a confidentiality provision that expressly referred to its customers’ names and numbers, and the employee handbook also
contained an express statement that employees “shall not use or disclose Morlife secrets or confidential information subsequent to their employment including lists of present and future customers.”46 One court, in concluding that an employer satisfied the reasonable-efforts prong of the trade secret definition, relied exclusively on the fact that employees were required to sign a confidentiality agreement regarding a customer database.47

**Security Policies Should Be Tailored, Consistently Applied, and Publicized**

It is critical that the security procedures be tailored to identify the specific information worthy of trade secret protection. Too often, security documentations call out every possible form of information—some not even related to the employer’s business and some that already has been widely published. Such broad language will do little to convince a court that the employer considered a particular piece of information to be proprietary.

Consistency and discrimination in the use of security procedures affect trade secret protection. If a company uses a “Confidential—Do Not Distribute” stamp, for example, the company must use it for all confidential materials or risk a court concluding that the unstamped materials are not trade secrets.48 On the other hand, overuse or inconsistent use of a confidentiality stamp may lead a court to conclude that the information at issue is not really a trade secret because it is treated no differently from any other information. For example, if a stamp is not consistently used and there is no set company policy stating when it should be used, a court is unlikely to conclude that stamping procedures were reasonably used to protect the security of the information in question, regardless of whether or not the specific document in question has a stamp.49

It is not enough simply to have these security policies written down somewhere; they must be known to the employees and routinely honored. One court, for example, held that a job manual did not contain trade secrets, because employees were allowed to keep the manual at home even though the policy stated that they were to be kept in the manager’s office.50 The court concluded that because employees were not advised that the manual contained confidential information or that there were security measures in place to prevent their disclosure, there was the suggestion that “the owner of the manual’s interest in security was minimal.”51 Another court concluded, however, that the evidence was sufficient to demonstrate a reasonable effort to keep the information confidential: Employees who had access to confidential information did so only on a need-to-know basis; such access was limited to the branch office, where the employees worked; and the employer informed the employees of the confidential and proprietary nature of the information.52

The security measures also must be applied to all potential trade secret information or the existence of such measures may harm a future claim for trade secret protection of information that was not subject to these measures. A manufacturer of oxygen regulators, for example, took substantial measures to protect some of its confidential information by keeping technical drawings in secure and locked areas, limiting access to information regarding technical drawings stored on computers, and maintaining a burglar alarm.53 The manufacturer, however, failed to take even basic steps to protect the technical drawings it provided to a supplier of component parts for the regulators, and on this ground, the court held that the manufacturer failed to take reasonable steps to ensure the security of the specific technical drawings at issue.54 The court suggested that if the manufacturer had obtained a confidentiality agreement from the supplier or
even an assurance from the supplier that the information would be kept secret, it might have been enough to constitute a reasonable effort to keep the information confidential.55

Customer Disclosure

A common issue is determining: What is a reasonable level of disclosure of confidential information to customers or potential customers. If, as part of a sales pitch, pertinent information about a product is disclosed to customers, will it destroy the owner’s ability to later argue that the information is confidential and should be deemed a trade secret under the law? Generally, the information in such sales pitches is not treated as trade secrets because it is disclosed to customers and potential customers alike.56

One court concluded that because there was no secrecy agreement on the record pertaining to a new product line offered to Home Depot, Home Depot presumably could show the information to other competitors and the proprietor of the information thus had not made a reasonable effort to keep the information secret.57 There are many situations in which companies must disclose sensitive, confidential information to customers or potential customers in order to consummate a deal. This secrecy dilution can be minimized by requiring customers and potential customers to sign nondisclosure agreements when confidential information is disclosed to them in the course of a sales pitch.

Conclusion

Trade secret identification and security are the surest ways to minimize competitor use of proprietary information. The resources invested in those efforts may pay off when a key employee goes to work for a competitor. Part II of this article will address how an employer can discourage its employees from taking its trade secrets and minimize accusations that it has taken the trade secrets of its competitors.

3 See www.nccusl.org/update/uniformact_factsheets/uniformacts-fs-utsa.asp for further information on which states have adopted the UTSA. The UTSA codified trade secret common law and was recommended for enactment in all states in 1979 and approved by the American Bar Association in 1980.
4 See Q-Co Indus., Inc. v Hoffman, 625 F.Supp. 608, 617 (S.D.N.Y 1985).
16 Q-Co Indus. at 617.
17 Buffets Inc. v Klinke, 73 Fad 965, 968 (9th Cir. 1996).
18 Buffets at 967.
19 Buffets at 968.
20 Self Directed Placement Corp. v Control Data Corp., 908 F2d 462, 465 (9th Cir. 1991).
21 Id.
22 Id.
24 Religious Technology Center, 923 F Supp. at 1256.
25 Religious Technology Center at 1254.
27 Morlife at 1521-1522.
29 Morlife at 1521-1522.
30 Id.
35 See Whyte at 1455-1456.
37 Vacco Indus. at 42 and n.3.
39 PepsiCo at *16.
41 205 Corp. at 550-551.
42 Id.
43 Id.
44 See Q-Co Indus. at 617-618.
45 Q-Co Indus. at 618.
46 Morlife at 1523.
47 MAI Sys. at 521.
48 See In re Providian Credit Card Cases at 308. (When "confidential—do not distribute" stamps were used for some material but not for others, this was evidence that the others were not treated as trade secrets.)
50 Buffets at 970.
51 Id.
52 Courtesy Temp.Service at 1288.
54 Flotec at 1004-1005.
55 Id.
56 In re Providian Credit Card Cases at 305.
57 Whyte at 1454-1455.