
Protecting Trade Secrets: Steps Every Trade Secret Owner Should Know

John M. Halan

Businesses must recognize that they typically take insufficient precautions to protect their trade secrets. In this article, the author suggests some additional steps that can be adopted.

Although trade secrets are often some of the most valuable assets owned by a business, most businesses do not take many of the precautions recommended to protect such assets. This article summarizes the main precautions that may or should be taken. Because others are possible, and the exact precautions needed depend on the business and trade secrets at issue, an intellectual property lawyer should always be consulted in formulating a trade secret protection strategy.

In general, a trade secret is a secret which gives the owner a commercial advantage over competitors. A trade secret may be, for example, "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."¹ The legendary Coca-Cola formula was a well-known example.

Trade secrets are based on state law. Accordingly, the definition of a trade secret may differ between selected states. Prior to the Uniform Trade Secrets Act (UTSA), a general trade secret definition often used was 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 him an opportunity to obtain an advantage over competitors who do not know or use it."² However, most states have adopted UTSA pursuant to which a trade secret is defined as follows:

Information, including a formula, a pattern, a compilation, program, device, method, technique, or process, that is both of the following:

(1) 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.

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

John M. Halan is a shareholder with the intellectual property firm Brooks Kushman, PC in Southfield, Mich. He can be reached at jbalan@brookskushman.com.

As set forth above, information qualifies as a trade secret only if reasonable efforts are taken to keep it secret. Even under the prior common law standard still employed by some states, a factor "considered in determining whether given information is one's trade secret [is] the extent of measures taken by him to guard the secrecy of the information."³

If reasonable efforts are not employed to keep information secret, the information cannot be enforced as a trade secret.⁴ The more efforts taken, the less likely it is that a trade secret will be found unenforceable.⁵

Such efforts can be broken down into three main categories:

1. Restricting access to the trade secrets;
2. Using agreements to restrict others from using or disclosing the trade secrets; and
3. Providing notice of the trade secrets.

These categories are explored in more detail below.

ACCESS RESTRICTIONS

A requisite element of a trade secret is that it indeed be secret.⁶ Accordingly, the best way to protect a trade secret is to keep it secret. Steps that can be taken to restrict access to the trade secrets of a business include the following.

First, trade secrets should be kept in restricted areas. For example, confidential processes, devices, or information can be performed or kept in sectioned-off or locked areas or receptacles to which only appropriate personnel have access.⁷ When trade secrets are maintained in a computer database, firewalls, cryptography, and passwords can be employed to restrict access. As to passwords, screen saver passwords can be used to prevent unescorted visitors from gaining access to the network and accessing trade secrets. As to escorts, courts have recognized that requiring visitors to be logged in and escorted while visiting is another factor favoring a finding of trade secret status.⁸

Second, disallow visitors from visiting areas where trade secrets are practiced or kept.⁹ The failure to do so could lead to the loss of trade secret rights.¹⁰ Relatedly, secure lobby areas, receptionist screenings, sign-in logs, and visitor badges also evidence secrecy efforts.¹¹

Third, restrict personnel having access to trade secret information to only those who have a need to know.¹² Employee access can be limited through the use of keys, combinations, passwords, or other means. For example, in *Infinity Prods., Inc. v. Quandt*,¹³ customer and pricing information available only to persons having a computer password were held

to be trade secrets. As another example, in *People v. Pribich*,¹⁴ “[e]ven the [sales] people . . . who had confidentiality agreements with the company were not permitted to view [development] work product.”

Fourth, use unnamed or coded components or ingredients. For example, in *Mangren Research & Dev. Corp. v. Nat'l Chem. Co.*,¹⁵ “[o]nce chemical ingredients were delivered . . . the labels identifying those ingredients were removed and replaced with coded labels understood only by employees.” Similarly, at one time Coca Cola ingredients were not only unlabelled and referred to as simply ingredients 1 through 9, the suppliers of those ingredients were required to use only the ingredient numbers on their invoices.

Fifth, if disclosure of a trade secret is necessary, divide the disclosure to avoid an assertion of easy replication. For example, the method used by KFC Corporation to protect its “secret recipe” fried chicken seasoning was to have one supplier supply one part of the recipe and another supply the other, with neither having knowledge of the components supplied by the other.¹⁶ As another example, in *United States v. Lange*,¹⁷ work was divided among subcontractors such that no one subcontractor received full schematics of the trade secret product. This ensures that no one subcontractor could easily replicate the product and was held to be a reasonable secrecy measure.

Sixth, limit the number of confidential information documents and destroy all unnecessary copies.¹⁸

AGREEMENTS

In general, two types of agreements may be used to protect trade secrets, employee agreements and agreements with others given access to trade secret information. The failure to have such agreements can lead to the loss of a trade secret.¹⁹ Such agreements are used ubiquitously.

Employees generally have an implied duty not to use or disclose an employer's trade secrets.²⁰ However, employee agreements directed to the trade secrets of a business are useful to clarify ambiguities regarding trade secret status and provide notice of trade secret ownership. Such employee agreements (often referred to as confidentiality, or non-disclosure agreements) typically restrict an employee from using or disclosing the trade secrets of a business (often referred to as confidential or proprietary information). All employees who might be exposed to the trade secrets of a business should be required to sign such an agreement. The agreement can be in the form of a contract or an employee handbook acknowledged by signature as having been read and agreed to by the employee. Annual or other periodic reminders of an employee's obligations are recommended.

Such agreements typically include other terms requiring the inventor to disclose the full detail of any inventions or discoveries conceived by

the employee and assigning ownership of such to the employer. The possible use or disclosure of trade secrets may be further protected by way of non-competition terms that restrict an ex-employee from engaging in competitive activities for a reasonable period of time within a reasonable territory.

A little-used term that should be employed is one requiring an exiting employee to identify his or her next employer and future responsibilities. This enables the trade secret owner to notify the next employer of the use and disclosure restrictions on the employee—notice which is sometimes important as explained in the Notice portion of this article. This also enables one to evaluate the probability of trade secret disclosure to the new employer. In states which follow the inevitable disclosure doctrine, an employment can be enjoined if there is a substantial likelihood or threat of trade secret disclosure.²¹

Non-employees who must be given access to trade secrets should also be required, before being given such access, to sign an agreement restricting use or disclosure of such trade secrets. Such non-employees might include contractors, suppliers, vendors, professional consultants, customers, potential licensees, and potential buyers of the business. For such persons, and for all visitors allowed into areas where a trade secret might be viewed, it is recommended that a business employ at minimum a standard confidentiality or secrecy agreement restricting use or disclosure of trade secret information.

NOTICE

Under UTSA, misappropriation of a trade secret—which may lead to liability—consists of either one of the following:

1. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.

2. Disclosure or use of a trade secret of another without express or implied consent by a person who did 1 or more of the following:
 - Used improper means to acquire knowledge of the trade secret.

 - At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it, acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or derived from or

through a person who owed a duty to the person to maintain its secrecy or limit its use.

- Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

As noted above, liability for trade secret misappropriation often turns on the knowledge of the misappropriator that such information was indeed a trade secret. While such a notice may be provided in a number of ways, including by way of the agreements previously discussed, the following methods may also be used.

First, it is recommended that an employee leaving a business be given an exit interview during which the employee can be reminded of the obligation not to disclose trade secrets—whether or not a confidentiality agreement has previously been used. While not determinative, such interviews are a factor which can be considered in determining the reasonableness of secrecy measures.²² While under no obligation to do so, an exiting employee may also be requested to sign an exit document acknowledging the continuing obligation reminder. In any event, the interview should be documented and the reminder confirmed in a follow-up letter. Such oral and written warnings should also identify, to the extent possible, all trade secrets of which the employee has knowledge—especially those considered to be valuable. Such precautions will make it difficult, if not impossible, for the employee to later claim that he or she had no reason to know that such was a trade secret or acquired by improper means.²³ Additionally, the employee should be requested to return all property and information of the business, including in particular those including or comprising trade secret information.

Second, if the employee leaving a business has been required—as suggested in the Agreement portion of this article—to disclose the next employer, that employer can be contacted and warned that the employee is restricted from using or disclosing trade secrets. Without identifying the specific trade secrets, the next employer could be warned that the employee has acquired trade secrets in a specific area, *e.g.*, manufacturing, sales, etc. Such notice could also be provided in writing to avoid any later denials of such notice. Again, this prevents the next employer from later claiming that it did not know the particular information was a trade secret or that it was acquired by improper means.

Third, documents and other things which include trade secret information should be provided with legends or signs denoting such to be proprietary trade secret information.²⁴

Fourth, and relatedly, notices such as signs can be employed on any portals to trade secrets or areas in which trade secret information is kept. Such portals could include doorways, file cabinets, drawers, and computer files.

Again, this article is not meant to be an exhaustive list of the precautions which may or should be employed in protecting trade secrets. Instead, it will hopefully serve to assist businesses in recognizing that insufficient precautions are being taken or that additional precautions could be used. In any event, the reader is urged to consult with an intellectual property attorney in preparing an adequate trade secret protection program.

NOTES

1. Restatement of Torts, § 757, comment b.
2. *Id.*
3. *Restatement of Torts*, § 757, comment b.
4. See, e.g., *Auto Channel, Inc. v. Speedvision Network, LLC*, 144 F.Supp.2d 784, 794-796 (W.D. Ky. 2001) (Information supplied to potential investors without confidentiality or proprietary markings and without a non-disclosure agreement was not subject to reasonable efforts of secrecy and did not qualify as a trade secret.).
5. See, e.g., *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179-180 (7th Cir. 1991) ("[T]he more the owner of the trade secret spends on preventing the trade secret from leaking out, the more he demonstrates that the secret has real value deserving of legal protection. . .").
6. See, e.g., *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1199 (5th Cir. 1986) ("[M]atters of general knowledge in an industry cannot be a trade secret.").
7. See, e.g., *Morton v. Rogers*, 20 Ariz.App. 581, 514 P.2d 752, 755 (1973) (Blending directions and formulae kept locked-up with only limited employee access upheld as trade secrets.); *Dicks v. Jensen*, 172 Vt. 43, 768 A.2d 1279, 1284-1285 (2001) (Customer list which was not locked and was available to any employee held not a trade secret); *United States v. Lange*, 312 F.3d 263, 266 (7th Cir. 2002) (Keeping all drawings and manufacturing data in room protected by special lock, alarm system, and motion detector confirmed use of reasonable secrecy measures.).
8. See, e.g., *Otis Elevator Co. v. Intelligent Sys., Inc.*, 17 U.S.P.Q.2d 1773, 1775 (Conn. Super. 1990).
9. See, e.g., *Surgidev Corp. v. Eye Technology, Inc.*, 828 F.2d 452, 455 (8th Cir. 1987) (Trade secret upheld where owner "restricted visitor access to its sales and administrative headquarters.").
10. See, e.g., *Hildreth Mfg., L.L.C. v. Semco, Inc.*, 151 Ohio App.3d 693, 709, 785 N.E.2d 774, 786-787 (2003) (Efforts to maintain secrecy were held not reasonable where employee family members and visitors were allowed in the building where trade secret methods were practiced.).
11. See, e.g., *Valco Cincinnati, Inc. v. N&D Machining Serv., Inc.*, 24 Ohio St.3d 41, 47, 492 N.E.2d 814, 819 (1986) (receptionist screened every visitor and operated buzzer lock system on the door to a confidential processing area.).

12. *See, e.g.,* Murco Agency, Inc. v. Ryan, 800 S.W.2d 600, 604 (Tex. App. 1990) (Customer lists were held to be a trade secrets where "those lists were divided among employees on a 'need to know' basis.").
13. 775 N.E.2d 1144, 1146-1147 (Ind. Ct. App. 2002).
14. 21 Cal.App. 4th 1844, 27 Cal. Rptr. 2d 113 (1994).
15. 87 F.3d 937, 940 (7th Cir. 1996).
16. KFC Corp. v. Marion-Kay Co., 620 F. Supp. 1160, 1166-1167 (S.D. Ind. 1985).
17. 312 F.3d at 266.
18. *See* Lange, 312 F.3d at 266 (minimizing number of copies of sensitive information and shredding surplus copies confirmed use of reasonable secrecy measures.).
19. *See e.g.,* Hildreth, 151 Ohio App. 3d at 709, 785 N.E.2d at 786-787 (Absence of nondisclosure agreements was a factor in finding a failure to take reasonable precautions.).
20. *See, e.g.,* Picker Int'l, Inc. v. Blanton, 756 F. Supp., 979 (N.D. Texas 1990).
21. *See, e.g.,* FMC Corp. v. Varco Int'l, Inc., 677 F.2d 500, 501 (5th Cir. 1982) (Where employee was hired by a competitor and was to be placed in charge of developing a competitive product, the court enjoined the disclosure of plaintiff's trade secrets and the placement of the employee "in a position that would create the inherent risk of disclosure and use" of plaintiff's trade secrets.); Weed Eater, Inc. v. Dowling, 562 S.W.2d 898, 902 (Tex. Civ. App. 1978) (Employee extensively involved in manufacturing could not "prevent his knowledge of his former employer's confidential methods from showing up in his work" and was enjoined from working for new employer in any capacity related to the manufacture of competitive products.).
22. *See, e.g.,* Innovative Construction Systems, Inc., 793 F.2d 875, 884 (7th Cir. 1986).
23. *See, e.g.,* Hexcomb Corp. v. GTW Enterprises, Inc., 875 F. Supp 457, 467 (N.D. Ill. 1993) (Defendant knew of the trade secret status of a machine because he had been put on notice of such during exit interviews.).
24. *See, e.g.,* Hildreth, 151 Ohio App. 3d at 709, 785 N.E.2d at 786 (Lack of trade secret status was bolstered by fact that no legends were used on documents containing trade secret information.); Picker Int'l Corp. v. Imaging Equip. Servs., Inc., 1995 U.S. Dist. LEXIS 11622, p. 46 (D. Mass. 1995) (Diagnostic software upheld as trade secret where proprietary legends were used on copies and, on later versions, were viewed on computer screens in conjunction with a lockout mechanism.).