Bloomberg Law Reports®

February 2, 2012

Intellectual Property

Trade Secrets

Protections from Disclosure

The "Secrets" to Maintaining a Sometimes Unrecognized Business Asset: Trade Secrets

BROOKS | KUSHMAN
INTELLECTUAL PROPERTY LAW

Contributed by John M. Halan, Brooks Kushman P.C.

The basic rule for maintaining a trade secret is a follows: Take all reasonable steps to keep it secret. If not, the trade secret status of the secret may be lost.

While such steps are relatively inexpensive, businesses commonly fail to take them. However, the same businesses will often expend large amounts of money in seeking patents, even if the resulting patents are less valuable than their trade secrets. This typically occurs because businesses do not understand (1) what a trade secret is, and accordingly are not aware they own valuable trade secrets, (2) the enormous value of their trade secrets, or (3) the appropriate steps which should be taken to protect their trade secrets. While briefly touching on the first two points, the focus of this article is the reasonable steps which should be taken to protect trade secrets.

While the definition varies between states, a trade secret is generally any secret information which gives a business a commercial advantage over competitors. Under the Uniform Trade Secrets Act ("UTSA") adopted by most states, trade secret information may include "a formula, pattern, compilation, program, device, method, technique, or process."[1] For example, as defined in Comment b of the Restatement of Torts, a trade secret may be "a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers."[2] In fact, a trade secret can be a compilation of information which is otherwise publicly available, but which took time, effort and expense to compile.[3] One well-known example of a trade secret is the Coca-Cola formula.

Beyond the obvious competitive advantages trade secrets can offer if utilized in secrecy, trade secrets can be enormously valuable if they are misappropriated–whether by a departing employee disclosing trade secret information to a competitor or through corporate espionage. Such enormous value can include (1) a large damage award against the misappropriating party, and (2) an injunction or exclusion order against the misappropriating party. As an example of the former, in September of 2011 jurors awarded $919.9 million in damages to DuPont Co., after finding that Kolon Industries Inc. misappropriated trade secret information relating to the manufacture of Kevlar.[4] As an example of the latter, the Federal Circuit recently upheld the authority of the United States International Trade Commission to exclude from importation goods made in China using a misappropriated trade secret manufacturing process.[5]

As to the focus of this article, many businesses are not aware of the appropriate steps which must be taken to protect a trade secret. Under the UTSA, the information must "[be] the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[6] If reasonable steps are not taken, a trade secret can

be lost. For example, in one lawsuit customer list information kept in a drawer was held not to be a trade secret because the drawer had been kept unlocked.[7] Accordingly, when an employee stole customer information from the list to start a competing company, the business had no recourse. Similarly, in another case boxed confidential materials kept within a locked company vehicle were deemed to have lost their trade secret status because employees had "potential" access to the vehicle and the box was unmarked.[8]

The following are some basic steps a business should take to protect its trade secrets.

Accessing trade secret information should be restricted to only those employees and other persons who have a need to know the information. One obvious way to do this is to keep trade secrets in a "locked" location, if possible. Such "locking" cannot be overdone. For example, in one case, a court held that a former employee had misappropriated trade secret manufacturing and pricing information because the employee had to bypass locked offices, locked file cabinets, and computer passwords in order to obtain the information.[9]

Similarly, any documentary records of a trade secret should be kept to a minimum, and unnecessary copies should be destroyed.[10] As to trade secrets kept in the form of an electronic database, firewalls, cryptography, unique user names and passwords should be used to protect such information.[11]

Preventing or restricting access to trade secret information should be extended to visitors, such as by requiring visitors to log in at the front desk and to be accompanied by an escort while in the building. Visitors, even family members, should never have access to any areas where trade secrets are kept or where protected processes occur.[12] If access is necessary, trade secrets should be concealed if practicable.[13]

If possible, it is also advisable to take steps to maintain the confidentiality of any separate elements of a single trade secret. For example, labels on the ingredients to a trade secret formula or recipe can be coded to prevent employees or visitors from learning the ingredients.[14] At one time, for example, Coca-Cola ingredients were simply referred to as ingredients 1 through 9, and suppliers were required to use only the ingredient numbers on invoices.

It is also advisable to divide the elements of a single trade secret between various employees, contractors, or suppliers if possible. For example, Kentucky Fried Chicken uses different suppliers to supply each ingredient of its "secret recipe" seasoning, thus preventing any one supplier from knowing the entire recipe.[15] As another example, in building or assembling a trade secret device or structure, the work can be divided between contractors such that no one contractor has knowledge of the entire trade secret.[16] As yet another example, trade secrets divisible by geographic area, such as customer lists, need only be given to employees who work in those geographic areas.[17]

Furthermore, all employees, contractors, customers, suppliers, or others who must have access to trade secret information should be required to sign an appropriate agreement beforehand restricting any use or disclosure of such trade secrets.[18] Such agreements are especially enforceable if the trade secrets are identified in the agreement.[19] The absence of such an agreement can be a factor in a later court determination that reasonable precautions were not taken,[20] and additional consideration is sometimes required for such an obligation to be enforceable.[21] While employees usually have an implied duty not to use or disclose the trade secrets of their employer, the aforementioned agreements are useful to clarify, and provide notice of, the trade secret status of certain information. As discussed below, such notice is often useful in later establishing misappropriation of the trade secret information at issue. Such agreements—often referred to as confidentiality or nondisclosure agreements—typically restrict an employee from using or disclosing an employer's trade secrets. It is also recommended that employees be reminded of such obligations (1) through training or instructions,[22] (2) materials such as employee handbooks,[23] preferably signed to acknowledge that the material was read and understood, and (3) on a periodic basis, such as during employee performance reviews.

Trade secrets may additionally be protected through non-compete agreements, which restrict a former employee from engaging in competitive activities for a reasonable period of time within a reasonable territory. The appropriateness of such non-compete restrictions will vary from state to state.

In addition to restricting access, steps should be taken to provide notice to others that the information in question is indeed a trade secret. This is advisable because trade secret misappropriation typically is deemed to have occurred when (1) a person acquires the information knowing or having reason to know it was acquired by improper means, or (2) there is a disclosure or use of a trade secret, without the owner's consent, by a person who knew or had reason to know that his or her knowledge of the trade secret was derived from or through a person who had used improper means to acquire it or who had acquired it under circumstances giving rise to a duty to maintain its secrecy. In other words, the thief of a trade secret must generally know or have reason to know that it was a trade secret to be liable for misappropriation. Accordingly, companies should take all reasonable steps to designate trade secrets as trade secrets and to remind their employees and others of their trade secret obligations.

For example, all documents and materials including trade secret information should be marked as such, with appropriate confidentiality legends.[24] Similarly, entry signs or legends should be used to warn that trade secret information is contained within rooms, files, drawers, computer files, or other areas where trade secret information is kept and that access to such information is restricted.

Another precaution that should be employed, but often is not, is the exit interview trade secret reminder. Such reminders can be a factor in a later dispute whether reasonable secrecy steps were taken.[25] More specifically, a departing employee should be (1) reminded of his or her confidentiality obligations regarding trade secrets of the company, even if the employee never signed a confidentiality agreement, and (2) asked to return all confidential

materials belonging to the business. The departing employee could also be asked to sign a document acknowledging his or her trade secret obligations.

The exit interview should be documented and a follow-up letter should be sent to the departing employee to again confirm all trade secret obligations. It is recommended that all such verbal and written reminders include a general description of the trade secret information which the departing employee has knowledge of or has been exposed to–without disclosing the actual trade secrets. This will prevent the employee from later claiming ignorance of the status of certain information as being a trade secret or any corresponding trade secret obligations.[26]

The departing employee should also be asked to disclose their next employer. An obligation to do so should be addressed in the initial hiring agreement and could include a continuing obligation to do so for a certain number of years following the employee's departure. This information is necessary in order to warn the next employer or employers, preferably in writing, that the departing employee has trade secret obligations regarding certain types of information which can be identified in general terms. This prevents the next employer from claiming that it was not aware that particular information was a trade secret and that the employee was restricted from disclosing or using it at the new job. In fact the departing employee can sometimes be enjoined from assuming the new position if there is a substantial likelihood that trade secret information will be disclosed or used.[27]

In summary, a business should take all reasonable precautions available to protect its trade secrets. Given the variety of business practices and trade secret information which can be at issue, and the varying laws between states, an attorney should always be consulted in developing and instituting a trade secret protection program.

John M. Halan is a shareholder with the intellectual property law firm of Brooks Kushman P.C., where he specializes in litigation, including patent, trade secret, and related commercial litigation. He has tried many cases and has successfully argued before the United States Court of Appeals for the Federal Circuit. He has also acted as a patent dispute mediator. In addition to litigation, John has negotiated numerous intellectual property and related commercial agreements and has prepared many infringement and validity patent opinions. At Brooks Kushman, he is the head of the firm's trade secrets group.

[1] Uniform Trade Secret Act with 1985 Amendments ("UTSA"), Section 1(4).

[2] Restatement of Torts Section 757, comment b.

[3] *AvidAir Helicoptor Supply, Inc. v. Rolls Royce Corp.*, 101 U.S.P.Q2d 1069 (8th Cir. 2011) (court interpreted "trade secrets" to encompass compiled instructions for overhauling Roll-Royce engines).

[4] *E.I. Du Pont de Nemours & Co. v. Kolon Industries Inc.*, No. 3:09-cv-00058, 2011 BL 253296 (E.D. Va. 2011).

[5] *TianRui Group Co., Ltd. V. International Trade Commission*, 661 F.3d 1322 (Fed. Cir. 2011).

[6] UTSA, Section 1(4)(ii).

[7] *Dicks v. Jensen*, 768 A.2d 1279 (Vt. Sup. Ct. 2001).

[8] *Jones v. Hamilton*, 53 So.3d 134, 140 (Ala. Civ. App. 2010).

[9] *See, e.g., Infinity Prods., Inc. v. Quandt*, 775 N.E.2d 1144, 1146-1147 (Ind. Ct. App. 2002) (information limited to persons having computer password held to be trade secrets.).

[10] *United States v. Lange*, 312 F.3d 263 (7th Circuit 2002) (keeping records to a minimum, and shredding extra copies, cited as trade secret factors).

[11] *See, e.g., International Hair & Beauty Systems, LLC v. Simply Organic, Inc.*, No. 8:11-cv-01883, 2011 BL 283700 (M.D. Fla. 2011) (unique user name and password requirements cited as trade secret factors).

[12] *Hildreth Mfg., L.L.C. v. Semco, Inc.*, 785 N.E.2d 774, 786-787 (Ohio Sup. Ct. 2003.) (efforts to maintain secrecy ruled insufficient where employee family members and visitors were allowed in building where trade secret methods were practiced).

[13] *See, e.g., Progressive Products, Inc. v. Swartz*, 292 Kan. 947, 258 P.3d 969 (Kan. Sup. Ct. 2011) (key ingredients of trade secret concealed when visitors were present).

[14] *Mangren Research & Dev. Corp. v. Nat'l Chem. Co.*, 87 F.3d 937, 940 (7th Cir. 1996).

[15] *See KFC Corp. v. Marion-Kay Co.*, 620 F. Supp. 1160, 1166-1167 (S.D. Ind. 1985).

[16] *See, e.g., U.S. v. Lange*, 312 F.3d 263, 266 (7th Cir. 2002).

[17] *See, e.g., Amedisys Holding, LLC v. Interm Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1311 (N.D. Ga. 2011).

[18] *See, e.g., Mattel, Inc. v. MGA Entertainment, Inc.*, No. 04-09049, 2011 BL 202572 (C.D. Cal. 2011) (access to private showrooms conditioned on confidentiality agreement).

[19] *Bradshaw v. Alpha Packaging, Inc.*, 2010 Ark. App. 659, (Ark. Ct. App. 2010).

[20] *See, e.g., Hildreth*, 785 N.E.2d at 786-787.

[21] *See, e.g. Jostens v. National Computer Systems*, 318 N.W.2d 691, 703-704 (Minn. Sup. Ct. 1982).

[22] *Triton Const. Co., Inc. v. Eastern Shore Elec. Services, Inc.*, No. 3290-VCP, 2009 BL 114055 (Del. Ch. 2009) (lack of employee training or instruction was factor in denying trade secret).

[23] *See, e.g., Crafty Kids Club v. Gressis*, No. B226687, 2011 BL 227006 (Cal. Super. Ct. 2011) (whether employee handbook identified database as confidential deemed evidence of reasonable precautions).

[24] *See, e.g., Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897, 899–900 & n. 4 (8th Cir. 2005) (use of proprietary legend on documents cited as a trade secret factor).

[25] *See, e.g. In re Innovative Construction Systems, Inc.*, 793 F.2d 875, 884 (7th Cir. 1996).

[26] *See, e.g., Hexcomb Corp. v. GTW Enterprises, Inc.*, 875 F. Supp. 457, 467 (M.D. Ill. 1993) (Ex-employee knew machine was a trade secret because he had been so notified during exit interview).

[27] *See, e.g., Pepsico Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995); *FMC Corp. v. Varco Int'l, Inc.*, 677 F.2d 500, 501 (5th Cir. 1982).