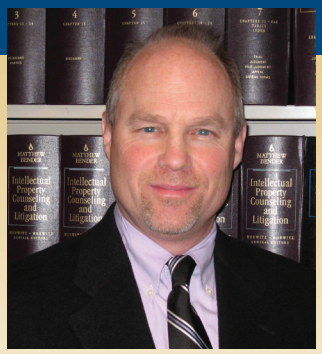
John W. Boger, Esq.
Heslin Rothenberg Farley & Mesiti P.C.



Pssst...It's a Secret...Don't Tell Anyone!!!

Remember back to your youth when keeping secrets was an everyday occurrence? Sometimes it was between classmates or siblings, and the results of not keeping it were temporary. As one grew older, keeping secrets took on a more serious tone as the consequences of disclosure usually had a more significant impact—just ask a certain golfer. In business, keeping secrets can be critical to the success of a company and the products it produces or sells. These types of secrets are commonly known as "Trade Secrets" and are the topic of this article.

The Legal Definition of a Trade Secret

How a trade secret is defined typically varies from state to state. The Uniform Trade Secrets Act (UTSA), adopted in 46 states in some form, defines a trade secret to be "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 secrecy." That is a pretty dense definition, but essentially says the information is more valuable when kept a secret.

You need to take some steps to keep the information secret in order for the information to qualify as a "trade secret." The other forms of intellectual property (i.e., patents, trademarks and copyrights) are defined and protected by Federal law. Trade secrets are an anomaly and are protected by state law, although the Federal Economic Espionage Act of 1996 (EEA) offers some protection. The EEA is a criminal statute that makes it a felony to sell, disseminate or otherwise deal in trade secrets, or attempt to do so, without the owner's consent. The definition of a trade secret under the EEA is potentially much broader than the UTSA definition provided above. The EEA trade secret definition includes in part "all forms and types of financial, business, scientific, technical, economic or engineering information, including . . . codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . ." (See 18 U.S.C. §1839 (13))

The four states that have ***not*** adopted the UTSA are Massachusetts, New Jersey, New York and Texas. Massachusetts, New Jersey and Texas have a separate state statute protecting trade secrets, while New York protects trade secrets under common law. The important point to remember is that treatment of trade secrets will vary from state to state.

Elements of a Trade Secret

To qualify as a trade secret, four elements must be present. Exhibit 1 summarizes the elements, which we'll then examine in detail.

Exhibit 1: The Four Elements of a Trade Secret

1. Must consist of information that is categorized as technical or business-related.
2. Must derive potential or actual economic value from the fact that it is secret.
3. Cannot generally be known either in the public domain or by others in your marketplace.
4. Must be treated as a secret and be the subject of reasonable measures to maintain secrecy.

First, the trade secret must consist of **information**. Typically, information will fall within two categories, technical or business information. Materials that will likely fall within the technical information category include plans, designs and patterns for equipment, devices, implants, etc; processes and formulas that are used to manufacture a food article, chemical, or drug; techniques for manufacturing products; lab and engineering notebooks; negative information, such as plans or designs of objects that did not work; and computer software (e.g., source code).

Business information would appear to be more broadly based. Information that likely would fall within this category include non-public financial information, including pricing and cost data; in-house market analysis and product forecasts; manufacturing/production information; customer lists; confidential alliances/business relationships; merger or acquisition targets; product purchase or acquisition possibilities; marketing, advertising, sales and distribution plans for future and existing products and services; and personnel information including special compensation/benefit programs.

The second element that must be present for information to be deemed a trade secret is that it must derive potential or actual **economic value** from the fact that it is secret. In other words, value must come from the fact that no one else knows about it and thus, it cannot be used by others. This flow of value is separate from the intrinsic value that the information may have. The value of this secret information may also be realized by the fact that a competitor (actual or potential) would have to expend time, energy and money to find and develop the secret information.

The third element is that the information **cannot be generally known** either in the public domain, or more importantly, by others in the marketplace in which you operate. This means the information cannot be generally known to the public, competitors or anyone else who could realize economic value from its disclosure or use. However, courts have found that the unique combination of generally known concepts and information can be deemed to be a trade secret.

The fourth and final element that must be present for information to be deemed a trade secret is that the information must be treated as a **secret** and be the **subject of reasonable measures** to maintain its secrecy. An owner's mere desire or intent to keep information a secret does not meet the standard. For the information to acquire and maintain trade secret status, reasonable efforts must be consistently put forth to keep it confidential. This fourth element is usually the one that varies the most between states. Importantly, courts are the ones that will make the determination of what was or was not "reasonable" with most courts holding that extreme or extravagant measures need not be taken in order to protect a trade secret.

What are "Reasonable Measures?"

So, what are the steps that must be taken to garner trade secret protection? To reiterate the point above, extravagant or expensive measures do not have to be put in place to satisfy the "reasonable measures" standard. Common sense and good business practice is the more prudent approach. Exhibit 2 details the steps to take as an owner of a trade secret that will go a long way to satisfying your "reasonable" efforts obligation.

Exhibit 2: Steps to Satisfy "Reasonable Meaures" Standard

a. Identify each piece of information you want to protect as a trade secret and establish a system that is continuously used to monitor existing secrets and identify new ones

b. Label all documents and materials that contain trade secret information as "confidential" and treat them accordingly. Limit the number of copies made of the documents and require the return of these materials at the completion of the review or when demanded.

c. Avoid being overly inclusive or broad when choosing which information to protect. Remember the value element

d. Institute a "need-to-know" policy and limit employee access to the documents and materials.

e. Instruct all new and existing employees about which information is considered a trade secret and the precautions that must be taken.

f. Require all employees who may use or be exposed to the trade secret or related information to sign confidentiality agreements and non-competes.

g. Implement internal security measures such as secure zones/rooms, employee I.D., badges, passwords, security and locked storage facilities or cabinets. Limit public tours of your facilities only to areas where trade secrets are not in use. Institute a strict visitor registration process, including having to wear identification badges and possibly signing confidentiality agreements. Prohibit all visitors and employees from using cameras or other electronic recording devices.

h. Institute strict IT security procedures including monitoring electronic notebooks and securing computer stations. Any trade secrets that are accessible electronically should be password protected and the passwords changed frequently with limited distribution.

i. Include a confidentiality provision in all agreements with vendor, distributor/licensees, joint venturers, temporary workers, customers and any other outside entities.

j. Monitor all advertising and marketing materials, including sales collateral and training publications to ensure that protected information is not mistakenly distributed.

k. Conduct periodic security audits to ensure no leak of trade secrets have occurred.

l. If the protected information relates to a product or assembly, use different vendors for the different component parts and do not disclose how the final product is assembled. Require all of the different manufacturing vendors to sign confidentiality agreements.

m. Hold annual training sessions with employees, reminding them of their ongoing confidentiality obligations and review all written policies of (n) below.

n. Establish written policies and manuals that outline how the company protects its intellectual property, including trade secrets, and include such policies in the employee handbook. Require each employee to read the policies and sign an attestation form signifying that they have read, understood and agree to comply with the policies.

o. Consistently correct and discipline any employees who may violate the polices of (n) above.

p. Conduct extensive exit interviews with departing employees to ensure the return of any trade secret or confidential information, as well as any security passwords, access codes and keys. Departing employees should be reminded of the expectations of compliance with any non-compete, non-disclosure or other continuing obligations (i.e., duty to assign inventions). Ensuring compliance can be garnered through linking such behavior with severance payments or benefits.

Trade Secrets in Indiana and Tennessee

As discussed above, trade secrets are treated differently in each state. Thus, as many orthopaedic manufacturers are located in both Indiana and Tennessee, we have looked at how these two jurisdictions treat trade secrets. A brief overview is provided below. Please note: the author is not licensed to practice law in Indiana or Tennessee, so local counsel should be consulted when evaluating trade secrets.

Indiana adopted the UTSA in part and has defined a "trade secret" to be "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."

Indiana courts have stated that the owner of the alleged trade secret must take reasonable steps, though not overly extravagant measures, to protect its secrecy. With that in mind, examples of reasonable measures in Indiana include: (i) requiring employees to sign confidentiality agreements or otherwise advising them of the confidential nature of the process; (ii) posting warning or cautionary signs or placing warnings on documents; (iii) requiring visitors to sign confidentiality agreements, sign in, and shielding the trade secret process from their view; (iv) segregating information; (v) using unnamed or code name ingredients; and (vi) keeping secret documents under lock and key.

Recently, additional "reasonable" steps have been identified by the courts of Indiana that lead information to qualify as a trade secret. These include: (i) limiting the underlying access to trade secret recipes by limiting the number of employees who have access to them, particularly to only the group of employees who have a "need to know" the trade secret; (ii) using security codes for employee access to secret files; (iii) having a security agreement in place that includes a provision which explicitly acknowledges the trade secret nature of the formula.

Tennessee has also enacted a form of the UTSA. Under the Tennessee version, some of the acts that have been found to maintain a trade secret include: (i) adopting a code of conduct for employees regarding trade secrets; (ii) requiring high level employees to sign confidentiality agreements; (iii) limiting visitor

access to facilities in terms of time and locations; and (iv) binding third-party companies and vendors to confidentiality agreements.

Tennessee courts have also suggested several supplemental steps companies can take to ensure trade secret protection. These include: (i) labeling guides, manuals or other documents that contain any trade secret information; (ii) retrieving from a departing employee any trade secret information or data that may be in the employee's possession upon departure or if they breach a confidentiality agreement; (iii) including in employee agreements a restrictive or non-compete provision; (iv) creating internal corporate policies regarding trade secret protection and disclosure to third parties; (v) instituting internal security measures including password protecting computers and computer systems, document marking protocols, in-house document securement, and requiring consultants to sign confidentiality agreements as a pre-requisite of retainment.

Non-Compete Agreements in Indiana and Tennessee

One of the uniformly recognized "reasonable measures" for garnering trade secret protection for information is to require certain employees to sign non-compete as a condition of their employments. In the orthopaedic world, non-compete agreements are a hot issue. Thus, we have examined these provisions to see how they have been treated in the past in Indiana and Tennessee.

Again, please be aware that local counsel should be retained for review of your non-compete. Validity of non-competes vary from state to state with some, California for example, not enforcing non-compete provisions because of public policy reasons. An interesting twist is that depending on the terms, non-competes with a current or former employer outside of California may be enforceable in California.

Covenants not-to-compete are generally disfavored in Indiana, but may be valid if they are narrowly tailored to protect a legitimate interest of the employer and are not unduly burdensome to the employee and the public interest. A non-compete agreement may be used to limit former employees where the limits are reasonable with respect to time, area and scope. Covenants not-to-compete that are associated with the sale of the business may contain greater restraints, although they are generally not enforceable if assigned to a second company unless the employee agrees to such assignment. In addition, a covenant not-to-compete must be supported by adequate consideration. In Indiana, continued at-will employment would satisfy this requirement.

Indiana courts have been willing to uphold time restrictions of one to three years, however longer periods have also been enforced. The geographic area that is typically found to be acceptable is the county or city in which the employee worked.

In Indiana, if a court has found the non-compete to be unenforceable because of unduly burdensome time or geographical restrictions, a separate clause restricting the disclosure of trade secrets may still be enforced. Indiana

courts have also shown a willingness to strike overly broad language, but will not rewrite or add new language to the non-compete agreement.

In Tennessee, covenants not-to-compete are also generally disfavored, although they may be valid and enforceable if there is an underlying employment agreement. If found to be unenforceable, the covenant not-to-compete may be severed from the remainder of the agreement. Non-competes are subject to higher scrutiny if it prevents competition by professionals, for example, physicians, dentists or veterinarians, although Tennessee allows non-compete agreements to be used to bind independent contactors.

Tennessee courts when evaluating such covenants will look to: (i) the danger to the employer if there is no agreement; (ii) the economic hardship on the employee; (iii) the public interest and (iv) the amount of consideration supporting the agreement (e.g., size of the severance package). The amount of time and size of territory that is covered by the non-compete is also considered. Generally, the courts have stated that a restraint is unreasonable, if the restraint is greater than the employer needs, or if the employee's interests outweigh the employer's interests. Unlike Indiana, Tennessee courts are willing to rewrite employment agreements and will reduce overly broad restrictions to an area to protect the employers' interests.

Stealing a Trade Secret

What happens when you have taken all of the necessary reasonable steps to protect your information and qualify it as a trade secret and someone steals it? The UTSA provides in part that stealing or the "misappropriation" of a trade secret occurs when: a person who knows or has reason to know that the trade secret was acquired by improper means (e.g., theft, bribery, espionage, fraud, etc.); the trade secret was disclosed or used by a person without the owner's consent and used improper means to acquire the trade secret; or was obtained under an obligation not to disclose or use it. Essentially, anything other than reverse engineering a trade secret would constitute stealing or misappropriation, unless that trade secret information has fallen into the public domain or they have permission from the owner.

What is the trade secret owner's recourse under the law? The UTSA imposes civil liability on the thief. Any criminal liability falls under the noted EEA statute described above. In the event one knows that their trade secret has been stolen or misappropriated, the victim may file suit (within three years of finding out about the theft) requesting injunctive relief (i.e., having the court issuing a restraining order and possibly providing for future royalty payments if the secret is used). Other remedies for the victims of a trade secret theft may include an awardment of actual damages, or if the person stealing the trade secret acted willfully and maliciously, the court may award punitive damages up to twice the amount of the actual damages, as well as attorney's fees. Having your attorney's fees paid by the thief may be enough of a deterrent in and of itself.

Conclusion

Trade secrets can be a very valuable intellectual property asset and provide long term competitive advantages that are not available with patents or copyrights. Special steps must be taken to ensure that employees are aware of the existence of these secrets and that if such designated information is stolen, that courts will then recognize them as trade secrets, thus availing you to the remedies and protection provided for under your state's trade secret law.

The author would also like to recognize Garth H. Mashmann, Esq., who assisted with the research relating to this article.

John W. Boger is an associate with the Albany, New York law firm of Heslin Rothenberg Farley & Mesiti P.C. and is a member with the firm's Medical Products and Technology Practice Group. Before attending law school, Mr. Boger worked for eight years with a large orthopaedic device manufacturer in various positions, including as a Product Development Engineer. He can be reached at 518-452-5600 or at jwb@hrfmlaw.com.

Heslin Rothenberg Farley & Mesiti P.C.
5 Columbia Circle
Albany, NY 12203 USA
518-452-5600 (phone)
www.hrfmlaw.com