Reasonable measures to protect trade secrets

By R. Mark Halligan, Esq., FisherBroyles LLP

OCTOBER 10, 2022

Protecting confidential business information dates back to Roman law which afforded relief against a person who induced another's servant to divulge secrets relating to the master's commercial affairs.

The law of trade secrets evolved in England in the early 19th century and in the United States by the middle of the 19th century.

One of the earliest issues in trade secret law was the degree of secrecy required to qualify as a trade secret. There were two common law doctrines: absolute secrecy and relative secrecy.

The courts held that absolute secrecy was not required because absolute secrecy would prohibit the trade secret owner from exploiting the economic value of the trade secret with employees, agents, licensees, and others. In addition, absolute secrecy would encourage unproductive hoarding of useful information.

The majority view became relative secrecy. Courts do not require extreme and unduly expensive procedures to be taken to protect trade secrets. As Judge Richard Posner observed many years ago in the *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.* appeal: "If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention."

The Uniform Trade Secrets Act (UTSA) requires a trade secret to be the subject of efforts that are *reasonable* under the circumstances to maintain its secrecy.

The Defend Trade Secrets Act (DTSA) requires that the owner has taken *reasonable* measures to keep such information secret.

The term reasonable can have many meanings in different contexts based upon different factors. What are reasonable efforts to protect trade secrets under one set of facts may be deemed to be deficient efforts to protect trade secrets under a different set of facts.

In the context of trade secrets, there can be many different situational factors.

For example, there is a difference between a company that derives all or a substantial amount of its revenues from a single trade secret (e.g. The Coca Cola formula) versus a company with many and less valuable trade secrets. In these circumstances, it is reasonable to expect a greater level of security efforts to be expended to protect the secrecy of the "crown jewel" trade secret assets.

The nature of the industry is also a situational factor. In a highly competitive industry, there is often a greater risk of trade secret misappropriation. Sophisticated efforts to deter economic espionage may be required to protect against the unauthorized acquisition of trade secret assets. Poaching employees (with exposure to trade secrets) to change jobs and join head-to-head competitors is also a much higher risk in highly competitive industries.

The size of the company is another situational factor. A smaller company will not require the full panoply of physical and cybersecurity measures required by larger corporations. Reasonable measures for a smaller company may just involve simple physical security measures such as locking entrances and storing sensitive documents in a locked file cabinet in the engineer's office.

The term reasonable can have many meanings in different contexts based upon different factors. What are reasonable efforts under one set of facts may be deemed deficient under a different set of facts.

Financial strength is also a situational factor. Wealthy companies can deploy all the "bells and whistles" to protect trade secret assets. Start-ups and smaller companies cannot, and they must perform a rigorous cost/benefit analysis to protect trade secrets within the financial constraints of the enterprise.

There is a triad of measures to protect trade secret assets: organizational measures, technical measures, and contractual measures.

Organizational measures include physical security measures and policies, practices, and procedures to notify and protect trade secret assets.

Technical measures include various access controls and security measures to restrict trade secrets on a "need to know" basis and

to "break up the pieces of the puzzle" so the theft of a trade secret cannot be replicated.

Contractual measures include non-disclosure and confidentiality agreements, training, monitoring, entry and exit interviews and other measures deployed to protect against the unauthorized acquisition, disclosure or use of trade secret assets by current and former employees.

Specific security measures must be tethered to specific trade secrets. Trial courts are no longer tolerating the recitation of a "grab bag' of security measures untethered to specific trade secrets.

There are four stages of trade secret asset management: identification, classification, protection, and valuation. The four stages cannot be juggled around. Identification precedes classification, identification and classification precede protection; identification, classification and protection precede valuation. "Protection" of a trade secret is the third phase. Starting with "protection" before identification and classification of trade secret assets is doomed to fail.

Specific security measures must be tethered to specific trade secrets. Trial courts are no longer tolerating the recitation of a "grab bag' of security measures untethered to specific trade secrets.

The tests for "reasonable efforts" (UTSA) and "reasonable measures" (DTSA) are intertwined with the statutory definition of "improper means" which includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.

The misappropriation of trade secrets rests upon a breach of confidence or other wrongful conduct in acquiring, using, or disclosing the trade secret information. If the actual efforts expended to protect specific trade secrets are successful, then the measures will be deemed to be "reasonable" to prevent misappropriation. But if the actual efforts are unsuccessful to protect specific trade secrets, then these measures will be deemed to be not reasonable.

The reasonable/not reasonable test is often too simplistic to determine whether a piece of information qualifies as a trade secret. For example, if a document is marked "confidential" then it is automatically a "trade secret." If the document is not marked "confidential" then it is automatically not a" trade secret."

The status of information claimed as a trade secret must be ascertained through a comparative evaluation of all the relevant factors, including the value, secrecy, and definiteness of the information as well as the nature of the defendant's misconduct.

The American Law Institute Restatement Third of Unfair Competition defines a trade secret as follows: "A trade secret is 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."

Note there is **no** mention of "reasonable measures" or "reasonable efforts" to protect trade secrets in the ALI definition of a trade secret.

Courts instead turn to the six common law factors derived from Section 757 of the Restatement (First) of Torts to adjudicate whether a piece of information qualifies as a statutory trade secret.

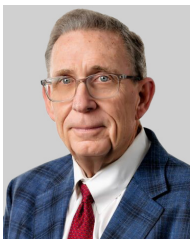
The six factors are:

> Factor 1: The extent to which information is known outside the company (the more extensively the information is known outside the company, the less likely that it is a protectable trade secret).
>
> Factor 2: The extent to which the information is known by employees and others involved in the company (the greater the number of employees who know the information, the less likely that it is a protectable trade secret).
>
> Factor 3: The extent of measures taken by the company to guard the secrecy of the information (the greater the security measures, the more likely that it is a protectable trade secret).
>
> Factor 4: The value of the information to the company and competitors (the greater the value of the information to the company and its competitors, the more likely that it is a protectable trade secret).
>
> Factor 5: The amount of time, effort and money expended by the company in developing the information (the more time, effort and money expended in developing the information, the more likely that it is a protectable trade secret).
>
> Factor 6: The ease of difficulty with which the information could be properly acquired or duplicated by others (the easier it is to duplicate the information, the less likely that it is a protectable trade secret).

All six factors must be considered. The evaluation of the owner's precautions to protect the secrecy of trade secret information is just one of the factors to be considered in determining the relative secrecy of a trade secret. Whether the trade secret owner's precautions will be deemed to be reasonable and sufficient depends upon a review of all six factors. Locking information in a vault will not transform information into a trade secret if the information is generally known in the trade. Likewise, a secret formula that is not known by anyone but two persons in the company will not lose its trade secret status because the document is not marked "confidential."

R. Mark Halligan is a regular contributing columnist on trade secrets law for Reuters Legal News and Westlaw Today.

About the author



R. Mark Halligan is a partner at **FisherBroyles LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He teaches Advanced Trade Secrets Law in the LLM program at University of Illinois Chicago School of Law and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on October 10, 2022.