Identifying trade secrets in litigation, but when?

By R. Mark Halligan, Esq., FisherBroyles, LLP

DECEMBER 21, 2021

A trade secret is simply a piece of information that provides the creator with actual or potential economic value derived from the secrecy of the information. It requires the "it" analysis: What is "it" that is alleged to be a trade secret? The "it" analysis is the beginning point and ending point of trade secrets law.

The historical development of trade secrets law starts with the American Law Institute Restatement of Torts Section 757 (1939). The scholars and trial lawyers that worked on this project reviewed the case law in the 19th Century and early 20th Century to determine when a piece of information should be given the special status of a "trade secret."

The result was the six-factor test:

(1) The extent to which the information is known outside the company.

(2) The extent to which the information is known by employees and others involved in the company.

(3) The extent of measures taken by the company to guard the secrecy of the information.

(4) The value of the information to the company and competitors.

(5) The amount of time, effort and money expended by the company in developing the information.

(6) The ease or difficulty with which the information could be properly acquired or duplicated by others.

Today, the six-factor test has become the litmus test for determining whether an alleged information asset (a "piece of information") qualifies as a statutory trade secret. In many jurisdictions, it is reversible error to adjudicate whether a piece of information qualifies as a trade secret without a factual evaluation of the six factors.

One of the hot-topic issues in trade-secret law today is when a piece of information must be identified as an alleged trade secret "with particularity." Does the piece of information have to be identified during the pre-filing investigation; before pre-trial discovery; at the summary judgment stage; before the trial begins; or in post-trial proceedings.

Initially, the law requires the confidential protection of the alleged trade secret. The trade secret holder cannot be compelled to identify the alleged trade secrets until there is a confidential protective order in place. It is mandatory for a trial court to preserve the secrecy of an alleged trade secret. It is an abuse of discretion to compel disclosure of an alleged trade secret without granting a protective order, holding in camera hearings, sealing the record, or ordering any person in the litigation not to disclose the alleged trade secret without prior court approval.

The "timing" issue — when to identify the alleged trade secrets — continues to be a perplexing issue in trade secret litigation but it should not be. Trade secret identification should take place during the pre-filing investigation *before* the lawsuit is filed.

The trade secret holder cannot plead a cause of action for misappropriation of a trade secret unless a trade secret exists that has been allegedly misappropriated (actual or threatened).

Delaying the identification of the alleged trade secrets until after the lawsuit is filed — and attorneys and experts search for documents, interview potential witnesses, scour electronic evidence — weakens the protection of legitimate trade secrets, results in millions of dollars in wasted discovery, and eradicates the obligation of the trade secret owner to develop internal trade secret asset management systems for the identification, classification, protection and valuation of trade secret assets.

The safety valve of liberal discovery under the rules of civil procedure is the reason most U.S. companies have no internal trade secret asset management system. There is no need to invest the resources. If a key employee leaves the company, the employer can file a trade secret misappropriation lawsuit and then use the liberal rules of civil procedure to ferret out a favorable identification of alleged trade secrets during discovery. The "trade secret audit" occurs *after* the trade secret misappropriation lawsuit is filed.

The cause of action is "trade secret misappropriation." There is no cause of action for just "trade secrets." There is no cause of action for just "misappropriation." There can be no cause of action for misappropriation without a trade secret. There must be threatened or actual "misappropriation" of a "trade secret."

The trade secret holder cannot plead a cause of action for misappropriation of a trade secret unless a trade secret exists that has been allegedly misappropriated (actual or threatened). The alleged misappropriation must be causally linked to the trade secret. Without at least one trade secret, linked to at least one act of misappropriation, there cannot be a cause of action for trade secret misappropriation.

The rush to the courthouse to protect an alleged trade secret in an emergency TRO hearing rarely happens today. In the early days (before the computer revolution), the company trade secrets were locked in a file drawer in the engineer's office and the door to the engineer's office was locked too. Locating the trade secrets was an easy task.

Each alleged trade secret — each piece of information (alleged to be a trade secret) — requires evaluation under the Restatement six-factor test.

But today, millions/billions of pieces of information exist in a labyrinth of computers and computer networks. Trade secret identification is a much more difficult task. But this is no excuse for allowing trade secret owners to file trade secret misappropriation lawsuits without the required pre-filing investigation and the identification of at least one trade secret misappropriated or at the risk of misappropriation.

The drafters of the Uniform Trade Secrets Act understood this potential abuse of trade secrets law and added a section in the UTSA for an award of attorney fees if a claim of trade secret misappropriation is made or maintained in bad faith. The DTSA (Defend Trade Secrets Act) also enacted the bad faith provision. The trade secret holder cannot file or prosecute a claim for "trade secret misappropriation" based on mere suspicion or mere apprehension of injury.

Take an example from the *FLIR v. Parrish* case in California. The plaintiff rested on the discovery of a "hard drive" as the evidence of trade secret misappropriation. The hard drive no longer existed. Yet FLIR was unaware of the hard drive until after the trade secret misappropriation lawsuit was filed and there was no evidence that the contents of the hard drive were improperly accessed or used. *FLIR Systems, Inc. v. Parrish*, 2d Civil No. B209964, 2009 WL 1653103 (Cal. App. 2d Dist. June 15, 2009).

FLIR kept litigating the claim for trade secret misappropriation under an "inevitable disclosure" theory and after an eight-day bench trial, the trial court found that the trade secret misappropriation claim was made in bad faith awarding $1,641,216.78 in attorney fees and costs to the former FLIR employees.

Over-designation of alleged trade secrets is another example of failing to conduct a reasonable pre-filing investigation of a trade secret misappropriation claim. In the *IDEX v Epic* litigation involving medical practice software, IDEX produced a 43-page description of the alleged trade secrets encompassing the methods and processes and the interrelationship of various features in the IDEX software package. *IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581 (7th Cir. 2002).

The 7th U.S. Circuit Court of Appeals observed that the complete documentation for the IDEX software leaves "mysterious" what pieces of information are trade secrets. The trade secret holder must do more than just identify a broad technology and then invite the court (and the defendants) to hunt through the details in search of items of information that meet the statutory definition of a trade secret.

The discovery quagmire surrounding the "timing" of trade secret identification overlooks the pre-filing investigation stage of a trade secret misappropriation claim. Each alleged trade secret — each piece of information (alleged to be a trade secret) — requires evaluation under the Restatement six-factor test. Once specific trade secrets are identified using the six-factor test, the specific alleged trade secrets must be causally linked to acts of threatened or actual misappropriation.

The policy arguments at the "discovery" phase of a trade secret misappropriation lawsuit have been around for years: The plaintiff has no way of knowing what trade secrets have been misappropriated until it obtains discovery from the defendants; the defendants seek to avoid "fishing expedition" discovery until the trade secret claims have been identified with particularity.

Two states have resolved the policy arguments for the trade secret defendant. Both California and Massachusetts by statute require that the trade secret plaintiff identify the alleged trade secrets with sufficient particularity to allow the court to determine the appropriate parameters of discovery and to enable the trade secret defendant to prepare a defense. Many other states impose the same requirements under their rules of civil procedure or local rules.

Trade secret plaintiffs should not be permitted to utilize the "discovery" phase of a trade secret misappropriation lawsuit to create trade secrets ex post facto. This should be the legal responsibility of the trade secret owner *before* the trade secret misappropriation lawsuit is filed.

A trade secret is simply a piece of information that provides the creator with actual or potential economic value derived from the secrecy of the information. It requires the "it" analysis: What is "it" that is alleged to be a trade secret? The "it" analysis is the beginning point and ending point of trade secrets law.

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 has taught Advanced Trade Secrets Law in the LLM program at UIC John Marshall Law School for the past 26 years 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 December 21, 2021.