Automated trade secret asset management: five elements

By R. Mark Halligan, Esq., FisherBroyles LLP

FEBRUARY 13, 2023

On Jan. 5, 2023, the U.S. Federal Trade Commission ("FTC") announced proposed rulemaking that would ban the use by employers of post-employment, non-compete agreements as a method of unfair competition calling it the "Non-Compete Clause Rule."

A non-compete clause is a contractual term between an employer and a "worker" that typically blocks the former employee or worker from seeking or accepting employment with a competitor, or starting a competing business.

For decades, non-compete clauses have been used to protect legitimate employer interests including near-permanent customer relationships and trade secrets. In many companies, using non-compete agreements is the primary way that the company protects its trade secrets.

However, based on the results of academic studies and various research efforts, the FTC has now concluded that non-compete clauses negatively affect competition in labor markets, result in reduced wages for workers across the labor force, and suppress labor mobility.

Trade secret owners must develop internal systems for the identification, classification, protection and valuation of trade secret assets. Prohibiting a former employee from working for a competitor will not be a viable option any longer.

The Non-Compete Clause Rule will ban, as an unfair method of competition, non-compete agreements.

It will violate Section 5 of the FTC Act for an employer to enter into or attempt to enter into a non-compete clause with an employee or worker. In addition, employers must rescind any such non-compete obligations with current or former employees or workers.

What does this mean for the protection of trade secrets?

It means that corporations and other business entities will not have a quick-fix solution to protect trade secret assets. Companies will now have to protect trade secrets under the Uniform Trade Secrets Act and/or the Defend Trade Secrets Act.

And this means that trade secret owners must develop internal systems for the identification, classification, protection and valuation of trade secret assets. Prohibiting a former employee from working for a competitor will not be a viable option any longer.

There are five necessary elements required to develop an automated trade secret asset management system: Taxonomy, Scoring, Metadata, History and Proof.

Trade secrets are some of the most valuable intellectual property assets in the world. Many companies owe substantial growth in their market value to their trade secret assets. Executives at those same companies now realize that safeguarding trade secrets is often more important than pursuing patent protection.

While most companies recognize the importance of protecting their trade secret assets, most of those companies still struggle and often fail to adequately manage and protect trade secret assets.

This is one of the major reasons post-employment restrictions on a former employee is so attractive. It is a quick-fix to protect trade secrets.

The solution going forward will be the implementation of an automated trade secret asset management system which will provide the trade secret holder with the tools necessary to identify, classify, protect and value trade secret assets. This author predicts that it will be the next revolution in intellectual property law.

There are five necessary elements required to develop an automated trade secret asset management system: Taxonomy, Scoring, Metadata, History and Proof.

Each one of these five necessary elements is discussed below.

(1) **Taxonomy**. The trade secrets must be by some easily understood taxonomy. Trade secrets existing as a large "blob" of undifferentiated knowledge is unacceptable. The classification system must be easy to understand so employees need not be trained to use it.

(2) **Scoring**. The trade secrets must be scored by some method that classifies the trade secrets and is easy to use. All trade secrets are not created the same. Some are better than others. An automated trade secret asset management system should classify and de-classify information assets that no longer provide economic value.

(3) **Metadata**. The automated trade secret asset management system should only capture metadata *about* the trade secrets, *not* the trade secrets themselves. Were the system to store the trade secret information, it would become a security risk. Further, putting the trade secret information into the system exposes more people to the trade secret information which weakens the protection of the trade secret assets. A method of asset management should not reduce the value or security of the assets themselves.

(4) **History**. The automated trade secret asset management system must retain all the metadata about trade secrets and be able to catalogue historical metadata. The period of interest in a trade secret lawsuit may be two or three years in the past. One cannot litigate a trade secret misappropriation lawsuit based on today's metadata; one must litigate based on the metadata at the time of the alleged trade secret misappropriation. Further, the historical treatment of the trade secret — proving reasonable security measures have been taken — will be an issue. The system must retain all versions of trade secret metadata and be able to reproduce the metadata as it existed at any prior time.

(5) **Proof**. The automated trade secret asset management system must contain methods for proving the existence and ownership of trade secrets — at any point in time — using modern hash code and blockchain technology that provides the necessary proof to prevail in a trade secret misappropriation lawsuit.

There is an uproar of concern about outlawing post-employment restrictions. However, there is a silver lining. Companies can now concentrate on the development and implementation of an automated trade secret asset management system, incorporating the five elements discussed above, for the identification, classification, protection, and valuation of trade secret assets.

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 February 13, 2023.