FEATURE

The Next Revolution in Intellectual Property Law: Automated Trade Secret Asset Management

By R. Mark Halligan

Share this:

There is an intellectual property revolution on the horizon and it is called *automated* trade secret asset management (TSAM). Using computerized TSAM tools to capture and identify, classify, protect, and value trade secret assets will unleash and fuel the exponential growth of intellectual property assets in the twenty-first century. The days of sitting in a conference room with a yellow pad and Dunkin' Donuts to conduct "trade secret" ideation sessions are now over.

To understand the phenomenal impact that automated TSAM tools will have on the identification, classification, protection, and valuation of trade secret assets, this article addresses the current trade secret conundrum, the functional requirements for an automated TSAM system, and the economic advantages of automated trade secret asset management.

The Current Trade Secret Conundrum

Recent studies show that over 80 percent of senior executives recognize that trade secrets are critical and essential to their businesses.[1] Fifty percent of these senior executives say that trade secrets are more important than their patents and trademarks.[2] Even more (69 percent) say they foresee trade secret protection becoming more critical than safeguarding other types of intellectual property because of the rapid and furious pace of innovation.[3]

Over 60 percent of these senior executives say that protecting trade secret assets is a board-level issue.[4] Nearly one-third of the respondents ranked the protection of trade secret assets a top-five concern.[5]

So why is there a disconnect between the recognition of the importance of trade secret assets and the failure of companies to manage trade secret assets? The answer lies in understanding the various stages of trade secret asset management.

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.[6]

The problem lies in the *starting point* for trade secret asset management. Everyone starts at the *third* stage—protection—with policies, practices, and procedures and a labyrinth of physical, contractual, and technical requirements for "protecting" trade secret assets. This is a revelation: a trade secret asset management system that starts at the protection stage is doomed to fail. The starting point must be at the *first* stage—identification—what is *it* that is alleged to be a trade secret? You cannot take reasonable measures to protect *it* if you do not know what *it* is.[7]

The *second* stage is the classification stage—trade secrets must be classified, scored, and ranked. The modern definition of a trade secret encompasses any information that can be used in operating a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others. Because even a small company may have thousands of trade secret assets to identify and manage, both identification and classification must precede the protection stage.[8]

Once trade secret assets are identified and classified, everything should come together. Reasonable security measures can now be tailored to the optimum level of security required for the identified and classified trade secret assets.[9] This is the third or protection stage.

But trade secret asset management stalls again. Companies spend months on the internal trade secret project but eventually realize that the herculean task of *manually* identifying and classifying trade secret assets even in a small organization can take years. It is the equivalent of attempting to "boil the ocean."

This is the current trade secret conundrum. Companies keep adding more security measures to the organization, but economic espionage and trade secret theft continue unabated. Companies recognize the importance of trade secret assets but do not have the technological tools, the time, or the money to manually identify and classify trade secret assets. There is no audit trail, no ownership, no documentation.[10]

But all is not lost. There is now a solution to the trade secret conundrum that harnesses the power of the computer and allows trade secret asset management to begin at the identification stage with easy-to-use inputs that drastically reduce the time and costs of trade secret asset management.[11]

Imagine using the power of the computer to create a "card catalog" of metadata about the company's trade secret assets that validates the existence of the trade secret assets; permits the inventory, analysis, tracking, and valuation of trade secret assets; and can be used by inside or outside counsel as a litigation support tool that will dramatically reduce the legal costs and risks commonly associated with trade secret litigation.

The solution is an automated TSAM platform that can be run on a standalone workstation, a multiuser server, a cloud-based server, or even an iPad or smartphone.

There are five functional requirements for automated trade secret asset management: taxonomy, scoring, metadata, history, and proof. Each functional requirement is discussed below.[12]

Taxonomy

Taxonomy is the process of naming and classifying things.

A trade secret asset must be identified and categorized. One categorization system that works with automated TSAM systems is the SFP categorization system: for . The *Subject* corresponds to the department or other location within the company that creates or uses the trade secret. The *Format* encompasses the type of trade secret: formula, drawing, process, pattern, device, methods, techniques, designs, plans, programs, codes, compilations, etc. The *Product* encompasses an existing product, a prototype, or a failed product.

For example, "Has anyone seen the Engineering Specifications for the Model 5750?" *Engineering* is the Subject, *Specifications* is the Format, and the *Model 5750* is the Product.

It sounds simple. However, it turns out to be much more sophisticated. All possible SFPs within an organization form a three-dimensional trade secret space into which *all* the organization's trade secrets fit (regardless of the number of trade secrets).

For example, a company with 10 departments, 30 information formats, and 20 products has 6,000 SFPs *available* as trade secret *categories*. Into this structured three-dimensional set of descriptive categories, the TSAM system can efficiently sort all of the *tens or hundreds of thousands of trade secret assets* in the company. This, in turn, enables further processing of the trade secret asset within each category, including elimination of redundancies, analysis of security issues, and the creation of a framework for the discovery of other trade secret assets in the company.

The SFP taxonomy is easy to use because employees are already familiar with the names of the departments in the company, the different information formats that capture the various types of trade secrets, and the various products and services provided by the company. No employee training is required to use these 6,000 categories since everyone already knows what constitutes an Advertising Plan for Snack Products or a Packaging Design for Laundry Detergent.[13]

Scoring

Trade secret assets must be scored and classified. All trade secrets are not created the same. Some are better than others. The basic "go/no-go" test for a potential trade secret asset requires proof that the information is not generally known in the trade; the information is not readily ascertainable by proper means; reasonable measures have been taken to protect the information; and the trade secret owner derives independent economic value from the secrecy of the information.

However, these requirements do not evaluate gradations. A more sensitive and granular evaluation of the potential trade secret asset can be accomplished by scoring the potential trade secret using the Restatement six-factor litmus test that the courts use to determine whether an alleged information asset qualifies as a trade secret.[14] The six factors are:

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; and
6. The ease or difficulty with which the information could be properly acquired or duplicated by others.[15]

Like the SFP categorization process, the identification process can be simplified by one-to-five scoring on each of the six factors. It is surprisingly accurate in ranking the trade secret assets, and it has the additional advantage of ranking the trade secret assets using the *same* legal tests used by the courts to determine whether an alleged information asset qualifies as a statutory trade secret asset. Like SFP categorizations, employees immediately understand one-to-five scoring from multiple life experiences such as hotel and movie ratings.[16]

The intersection of SFP classification—the taxonomy—and the six-factor identification—scoring—provides another revelation: trade secrets within a given SFP have similar six-factor rankings. This means that the bulk of the trade secret assets within a company can be ranked at a macro-level by ranking the SFPs instead of attempting to rank thousands of individual trade secret assets at a micro-level.[17]

The automated TSAM system should be a two-stage system: *potential* trade secret assets and *accepted* trade secret assets. The two-stage system allows inputs from any employee (from the shop floor to the C-level suite) as "potential" trade secrets, with a second stage review "accepting" or "rejecting" the potential trade secret asset. In addition, metadata relating to the trade secret asset can be reviewed and revised before final acceptance of the trade secret asset into the automated TSAM system.

Metadata

An automated TSAM system operates as a trade secret "card catalog" equivalent to a library card catalog. The automated TSAM system *never exposes the actual trade secret*. Instead, it provides a *pointer* to the trade secret asset. This ensures maximum security.

The library card catalog entry for a book in the library contains the name of the book, the name of the author, the year the book was published, the topic of the book, and where the book is located within the library.

An automated TSAM system operates the same way. A trade secret worksheet collects the SFP information, scores the potential trade secret asset, and collects other information about the potential trade secret asset as necessary based on the type of trade secret and the type of company. The "registry" or "inventory" approaches, which recommend warehousing the actual trade secrets in one central location, invite disaster and create a huge security risk in a target-rich environment.

An automated TSAM system should capture only the metadata relating to trade secret assets. A method of asset management should *not* reduce the value or security of the underlying assets themselves. Like a library card catalog, which contains no books, an automated TSAM system contains no trade secrets.[18]

History

The relevant period of time in trade secret litigation may date back many years. There is a discovery rule in trade secret law: the cause of action for trade secret misappropriation does not begin to run until the misappropriation is discovered or, by exercising reasonable diligence, should have been discovered. One cannot litigate a trade secret misappropriation case based on today's environment; the law requires that a trade secret misappropriation lawsuit be litigated at the time of the alleged misappropriation.[19] Therefore, trade secret asset management requires retention of the historical metadata relating to the trade secret asset forever.

Proof—Existence, Ownership, Notice, and Access

The plaintiff in a trade secret misappropriation lawsuit must prove existence, ownership, notice, and access (EONA proofs).

- *Existence:* The information qualifies as a trade secret, i.e., a trade secret exists.
- *Ownership:* The plaintiff has ownership rights in the information.
- *Notice:* The defendant had actual, constructive, or implied notice of the trade secret status of the information.
- *Access:* The defendant had access to the information, i.e., did not independently develop the information.

These four proofs are unique to trade secret litigation. The likelihood of success on each of the EONA proofs depends upon actions that the information owner takes *before* the misappropriation occurs.[20]

In order to use evidence to satisfy such proofs, the rules of evidence require authentication of the evidence. The proponent must produce separate evidence to support a finding that the proffered item of evidence is what the proponent claims it is.[21]

The litigation of trade secret disputes is fact intensive. The existence of a trade secret is a question of fact; whether the defendant had access to the trade secret is a question of fact; the timeline of events is a question of

fact; ownership of the trade secret is a question of fact.

In an automated TSAM system, many factual disputes can be eliminated by using hash codes and blockchains, which the courts recognize as self-authenticating based on the underlying technology.

Digital forensics experts routinely use hashing methods to verify that copies of digital evidence match the original data from which the copies are made, i.e., their hashes or "fingerprints" match. The hashing algorithm called Message-Digest 5 (MD5) produces a 32-character alphanumeric fingerprint. The simple action of changing the letter *o* to the number 0 changes the hash code.

A blockchain is a set of entries, each of which is mathematically linked to the one before by hash codes. The next entry in a blockchain contains the new data, the current timestamp, and a hash code from the last entry's hash code with the new data and timestamp. Blockchaining provides all the benefits of using hash codes without the necessity for a third-party timestamping authority. The timestamp is built into the blockchain. Blockchains are immutable and tamper-proof.

Using hash codes and blockchain technologies in an automated TSAM system is revolutionary. Once trade secret metadata is entered into the blockchain, there is no possibility of records being altered or falsified. You cannot go backward—blocks only go forward. Proof of the existence of a trade secret, ownership, notice, and access can now instantly be proven by production of the timestamped blockchain digital records on any date of interest in a trade secret misappropriation lawsuit.[22]

The Economic Valuation of Trade Secret Assets

Automated trade secret asset management also permits the trade secret owner to move forward to the fourth stage: valuation of the trade secret asset.

The economic valuation of trade secret assets has perplexed the intellectual property bar for years. The economic and legal issues are seemingly inextricably intertwined.

However, collecting metadata on the trade secret asset in the automated TSAM system provides critical data that allows the trade secret owner to evaluate the three factors necessary to calculate the net present value of a trade secret asset:

1. The total amount of expected future cash flow;
2. The discounted basis of that future cash flow as a present value; and
3. The probability of the future cash flow occurring.

Using an automated TSAM system, values can be assigned to each of the three factors for each SFP (or any other bundle of trade secret assets). The economic value of the trade secret is then calculated by *multiplying* these

three factors together.[23]

The key point to recognize is that the economic valuation of a trade secret asset is not confined to the value of the information content per se. Instead, the value of a trade secret asset is a function of *both* the content of the trade secret information and the stewardship and protection of the trade secret asset. Without proper stewardship, the trade secret status of the information will be forfeited and the economic value of the information will drop to zero.[24] However, identifying and ranking the trade secret asset and cataloging the reasonable measures taken to protect the secrecy of the information in the automated TSAM system will increase the probability of future cash flows, and concomitantly increase the economic valuation of the trade secret asset.[25]

Conclusion

Automated trade secret asset management will unleash the economic value of trade secret assets and will usher in another period of extraordinary growth in intellectual property law in the twenty-first century. Using the power of the computer to create a "card catalog" of metadata about the company's trade secret assets validates the existence of trade secret assets and permits the inventory, analysis, tracking, and valuation of trade secret assets. As a litigation support tool, automated trade secret asset management dramatically increases the likelihood of success in trade secret litigation and dramatically reduces the legal fees and costs incurred in trade secret litigation.

Endnotes

1. Baker McKenzie, The Board Ultimatum: Protect and Preserve. The Rising Importance of Safeguarding Trade Secrets 3 (2017), http://www.euromoneythoughtleadership.com/TheBoardUltimatum.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *See* R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, 6 Landslide, no. 1, Sept./Oct. 2013, at 12.

7. *Id.*

8. *Id.*

9. *Id.*

10. *See* Donal O'Connell & David Cohen, *Fiduciary Duty with Respect to Trade Secret Asset Management*, Seyfarth Shaw: Trading Secrets (Nov. 2, 2018), https://www.tradesecretslaw.com/2018/11/articles/trade-secrets/fiduciary-duty-with-respect-to-trade-secret-asset-management/.

11. *See, e.g.*, R. Mark Halligan & Richard F. Weyand, Trade Secret Asset Management 2018: A Guide to Information Asset Management including RICO and Blockchain (2018).

12. *Id.* at ch. 18.

13. *Id.*

14. *See, e.g.*, Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714 (7th Cir. 2003).

15. *See* Restatement (First) of Torts § 757 cmt. b (Am. Law Inst. 1939).

16. Halligan & Weyand, *supra* note 11, at ch. 12.

17. *Id.* at ch. 18.

18. *Id.*

19. *Id.*

20. *Id.* at ch. 3.

21. Fed. R. Evid. 901.

22. *See* Halligan & Weyand, *supra* note 11, at ch. 18.

23. R. Mark Halligan & Richard F. Weyand, *The Economic Valuation of Trade Secret Assets*, J. Internet L., Feb. 2006, at 19.

24. *Id.*

25. *Id.*

ENTITY:

INTELLECTUAL PROPERTY LAW SECTION

TOPIC:

INTELLECTUAL PROPERTY

Authors

R. Mark Halligan

R. Mark Halligan is a partner at FisherBroyles, LLP. He has litigated numerous cases regarding the misappropriation, protection, and enforcement of trade secrets. He also teaches trade secret law and advises clients on best practices relating to the identification, protection, and valuation of trade secret assets.