WHITE PAPER

Trade Secrets are Increasingly Important and More at Risk than Ever ©

The Value of Trade Secret Management Software in Litigation

Trade Secret Engine™

September 2022

CONTENTS

Executive Summary

Trade Secrets are Increasingly Important and More at Risk Than Ever

Courts regularly assigning awards amounting to $10's of millions of dollars, greater than 50% of former employees admit to taking confidential information with them when leaving their previous employer, data is ubiquitous, the great resignation is going strong, and employees work from home more than ever before. These are just some of the factors underlying the dramatic increase in trade secret misappropriation and disclosure, potentially costing corporations billions of dollars or worse.

Trade secret misappropriation litigation is more necessary, more prevalent, and increasingly difficult to litigate. This trend will continue to escalate for a variety of reasons. At a macro level, the continued digitization of intellectual property, including technical, financial, and marketing information, along with the ubiquity of employees working from home and employee mobility are just two of the many critical factors.

The Rising Importance of Trade Secrets in the IP Portfolio

Changes in patent law

Changes in patent law, including the shrinking universe of subject matter eligible for patent protection, have resulted in a renewed focus on increasing and protecting trade secret portfolios.

A Shift in Protection

Traditionally, inventors have used patents to protect innovations that, by their nature, cannot be kept secret or hidden. However, this appears to be changing amid recent patent case law and the fact that courts are finding certain types of previously patentable inventions to be invalid. Examples include the 2012 decision in **Mayo v. Prometheus**, 566 U.S. 66, the 2013 decision in Association for Molecular Pathology v. Myriad Genetics Inc. and the 2014 decision in Alice Corp. Pty. Ltd. v. CLS Bank International. These, in addition to other recent decisions, illustrate **an evolution of patent law that may lead to a shift** wherein companies opt to protect what were once patent-eligible materials, innovations and confidential/proprietary processes and information via trade secret protection instead of patents.

IP Reform

In general, patents are harder to get, easier to contest and more difficult to maintain than in the past. At the root of these trends, are several **fundamental changes to U.S. patent law and practices:**

- It's generally harder to get patents now than in the past
- Patent ineligibility is more prevalent
- More inventions are considered obvious in view of prior art
- It's easier to challenge patent validity
- Elimination of patents via IPR at USPTO is more common
- It is harder to prove patent infringement today
- Courts are more readily dismissing cases pre-trial via rule 12(b)(6)

The Crown Jewels are Seriously at Risk

Several prevailing conditions related to the corporate and legal environments in which we operate, have led to a "Perfect Storm" driving greater trade secret misappropriation.

Trade Secret Misappropriation Is Exploding for Several Reasons

HOW EMPLOYEES & DATA INTERACT:

- **Working from home.** While statistics are not widely available yet, the shift to working from home growing out of the pandemic is expected to result in a tsunami of misappropriation of trade secret litigations in the next few years.
- **The Great Resignation** – More people are leaving their jobs than ever in the past 20 years of tracking this statistic. Workforce mobility means employees can move to competitors within their industries and easily take confidential electronic information with them on exit. This will only add to the misappropriation of trade secrets.
- Over 50% of employees that leave their jobs admit to **taking confidential info with them.** More than half of them think it's OK to do so.
- **Confidential information is everywhere** in today's organization and it's easy to access and copy.
- **Data sources** are more diverse and voluminous than ever before.
- When **data is spread** across the enterprise, it's easier to steal and harder to track and manage.

The Legal Landscape Has Shifted

Fundamental Changes in legislation, the expectations of judges, common practices related to protection of intellectual property and the evolution of the law itself, all lend themselves to an increase in the importance of trade secrets to companies relative to previous methods of protecting intellectual property assets.

In addition to the increase in trade secret litigation, several key changes to the legal landscape are impacting corporate and legal strategies including:

- **A Higher Bar** – The requirements by the courts/judges to qualify for leveraging the court system to defend your valuable assets have become more stringent
- **China** – Enforcement of patents by organizations marketing their products/services globally can have consequences in regard to accessing certain important markets.
- **Required Preventative Measures** – In accordance with demands by the courts, companies are becoming more sophisticated around developing and implementing trade secret protection policies, procedures and technology.
- **The Have's and Have Not's** – Companies that are taking action to protect and defend their trade secrets have a decided advantage and can use that advantage in an offensive or defensive manner.

Trade Secret Misappropriation Litigation Is Steadily Increasing

There are several reasons for the increase in Trade Secret Misappropriation litigation:

The DTSA

The DTSA has given employers a means of remedying these misappropriations in federal court, and since the statute's inception, federal trade secret litigation continues to trend up.

Cases

Since the advent of the Defend Trade Secrets Act (DTSA) in 2016, trade secret disputes in federal court remain strong. 7,732 lawsuits involving trade secrets claims have been filed in federal court since the DTSA's effective date of May 11, 2016. In 2021 alone, 1,253 new actions were filed. Since the beginning of 2022, at least 139 new trade secrets disputes have been filed in the U.S. federal court system.

Theft

Another huge factor in the amount of litigation related to trade secret misappropriation is the massive increase in the commission of trade secret **theft by employees.** As discussed, this is based on the access employees have to data and their willingness to take it with them when leaving an employer. Advancements in technology have made it easier for employees to misappropriate their employer's trade secrets to use for their own purposes.

Awards

Over the past three decades, damages in litigation which include trade secrets have totaled approximately $3 billion, with the five largest awards each being over $100 million. The trend of significant awards is unlikely to abate as trade secret suits continue to provide monetary, as well as injunctive, recourse to companies whose valuable business information has been stolen.

Collaboration

In today's ultracompetitive markets, companies bear significant research-intensive costs to develop new products and processes. In many industries, collaboration can be beneficial, allowing companies of all sizes to enhance their research and development, product portfolio, and marketing channels. As an example, according to the Winter 2021 BDO Biotech Brief, collaboration has been crucial for biotech companies in recent years, and it is only getting more important. BDO reported that at the time of the study, 50% of biotech companies planned to collaborate on commercialization in 2021.

While all of this collaboration will no doubt lead to profitable and beneficial outcomes, it can also lead to both intentional and unintentional exposure of a company's confidential information. Without the proper protections in place, a company seeking to collaborate can quickly find itself deprived of some of its most valuable assets – its trade secrets.

Another major factor in the increase in litigation is the expansion of what is considered **Confidential Information.** There has been a significant influx of cases recently involving trade secrets and/or confidential information related to:

- Computer technology, programming methods and source code
- Customer lists
- Proprietary pricing
- Supplier relationships
- Proprietary Designs

This is a shift from what was previously considered to be confidential information in the past and has also contributed to an increased in case volumes.

As Litigation Increases, So Does the Bar to Access the Courts

As the acceptance of trade secrets as a means to protect certain types of intellectual property has increased, so has the courts' demand that litigants come to the courthouse well prepared. The pre-filing investigation and preparation of a trade secret misappropriation lawsuit typically consists of complex tasks that involve many factual issues. Failure to be adequately prepared can have grave consequences.

Federal Courts Are Enforcing Higher Standards for Redress

To adequately allege the existence of a trade secret, the plaintiff must describe the trade secret with **sufficient particularity** to separate it from matters of general knowledge in the trade or of special knowledge of those persons skilled in the trade.

- Since the enactment of the Defend Trade Secrets Act (DTSA) on May 11, 1996, the federal district courts have been laser-focused on the deployment of the Twombly/Iqbal pleading standards to dismiss trade secret misappropriation lawsuits before the parties pursue futile claims.

- Trial judges recognize that trade secret misappropriation claims are often filed without an adequate pre-filing investigation, and the U.S. district courts are becoming increasingly intolerant of the plaintiff using the discovery process to create a "trade secret" after-the-fact and spending millions of dollars on a "fishing expedition" that would not have occurred if the plaintiff had conducted an adequate pre-filing investigation before filing the lawsuit for trade secret misappropriation.

Drafting a complaint containing lots of artificial labels, legal conclusions or just a formulaic recitation of the elements of a trade secret misappropriation claim will not likely survive a FRCP Rule 12(b)(6) motion to dismiss that applies the Twombly/Iqbal pleading requirements. The increased demand for the courts by corporate litigants as a means to remediation and resolution is compelling judges to be more demanding of the litigants appearing before them. These demands often come in the form of more stringent pre-filing investigations and a consideration of FRCP Rule 12(b)(6).

Courts have concluded that there cannot be a threatened or actual misappropriation of information that is not a statutory trade secret. If there is no "trade secret" then there cannot be a cause of action for trade secret misappropriation. Since there is no public registry for trade secrets, information assets must be validated in a court of law as statutory trade secrets.

There is no exact definition of a trade secret due to the vast spectrum of information that could qualify as a trade secret and the wide array of factual circumstances that could be determinative or fatal to the classification of a piece of information as a trade secret. Therefore, the courts require proof of several elements in order to establish a trade secret. This is known as the EONA proofs. Foremost among these requirements, and table stakes to get into court, is the ability to identify what is the trade secret in question?

The elements of the EONA proofs that have to be established by the plaintiff in order to proceed in court include:

- Existence – proof of existence of the trade secret. What is it?
- Ownership – proof that the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.
- Notice of – the plaintiff must show that the defendants had actual, constructive, or implied notice of the alleged trade secret
- Access to – the plaintiff must prove that the defendant had access to the alleged trade secret

Proving the **existence** of a trade secret involves a **six factor test** which includes:

1. The extent to which the information is known outside the business.
2. The extent to which the information is known inside the business.
3. The extent of measures taken to guide the secrecy of the information.
4. The value of the information to the business and to competitors.
5. The amount of time, effort, and money expended to develop the information.
6. The ease or difficulty with which the information could be properly acquired or duplicated by others.

In **Arconic Inc. v. Novelis Inc.** the special master and court engaged in repeated efforts to have the Plaintiff, Arconic, identify its claimed trade secrets and confidential information in order for the case to proceed. After multiple requests, the court found that Arconic's trade secrets claims lacked merit, would not survive summary judgment and dismissed the case with prejudice because "a party cannot succeed on a trade secrets claim, if the party cannot identify with reasonable particularity, what its trade secrets are."

This case is a good example of many of the trends discussed above and the challenges that companies face today in protecting their trade secrets. It also drives home the fact that corporate management needs to be prepared to defend their intellectual property in court if necessary. Specifically, companies need internal systems (policies, practices, technologies and procedures) that provide a way to manage trade secrets and trade secret metadata.

The Problem

The Problem: Rampant Trade Secret Misappropriation Combined with Stringent Court Requirements Puts Corporations in A Perilous Situation

Given all the changes in the way companies operate, including the digitization and ubiquity of data, the mobility of employees and how they interact with confidential information, it's not surprising that misappropriation of that data is much more common than ever before. However, what really makes the current situation so treacherous for companies that fail to take action to prepare themselves, is the explosive growth of this act coupled with the gravity of the consequences for being unprepared.

A failure to take proactive measures to prevent trade secret misappropriation can certainly be harmful, but a failure to implement a system that enables you to litigate for the defense of these vital assets, leaves your company with little to no recourse and could prove disastrous.

As discussed, to seek injunctive and/or monetary relief for misappropriation of trade secrets requires the ability to identify with reasonable particularity, what their trade secrets are. This may sound like an easy task but it often proves to be a fatal flaw in the litigation strategy. Here's what's really involved:

What Happens If Preventative Measures Fail?

If preventative measures fail and valuable trade secrets are misappropriated, the organization will be compelled to rely on the court system for injunctive relief, remediation and/or compensation.

Critical Trade Secret Information

To be prepared for misappropriation litigation, legal counsel needs to know several key facts about their trade secrets including:

- How many trade secrets the company possesses.
- Which ones are most important.
- What measures have been taken to protect them.
- Who had had access to them.
- When were they accessed and updated last.
- Which ones came from third parties.
- Which ones needed to be destroyed once collaboration ended.

A trade secret must be managed like other property assets. However, trade secret management differs because it first requires the identification of the alleged trade secret. Because millions of bits of information within a company can qualify as proprietary trade secrets, the classification and ranking of trade secrets is a critical exercise.

Organizations that are not prepared to provide the court with this type of information will likely not succeed on a trade secrets claim or even have access to the courts if their trade secrets are stolen.

To have a command of this information, companies need a system that enables them to identify, index, manage and ultimately defend their valuable trade secrets. It's equally important that a system to mitigate the risk of misappropriation is put in place before the theft is committed. If a company waits until the misappropriation occurs and they are compelled to litigate, it will likely be too late. A **trade secret management system** is the solution. Such a system positions the company to react quickly, be prepared to litigate and, if necessary, seek injunctive relief in the form of an ex-parte seizure order. Having an organized, comprehensive and predefined process, by which the organization records and manages its trade secrets, will provide a highly strategic advantage over an adversary that does not possess the wealth of irrefutable evidence and information such a solution delivers.

A trade secret management system is crucial for any company with reliance on trade secrets. These types of solutions provide value to a company when it is litigating to defend its trade secrets as a plaintiff and when it is protecting its assets that are under attack via a fishing expedition, as a defendant.

For plaintiffs who have been the victim of trade secret misappropriation, these programs are a critical component in securing legal recourse in the courts and being able to protect and defend their company's trade secrets by achieving the following:

- Overcoming any FRCP Rule 12(b)(6) motion to dismiss
- Compliance with stricter pleading standard announced in Twombly
- Arming Plaintiff's counsel with specific and plausible evidence of misconduct or misfeasance by the Defendant
- Access to critical, irrefutable, substantiated evidence about the trade secret(s)

For defendants, being sued by a competitor for theft of trade secrets (whether frivolous or not) can result in significant and possibly crippling consequences which include:

- Massive legal fees
- Overwhelming discovery demands/requirements
- A fishing expedition – Use of discovery to obtain competitive intelligence on the rival's business and/or trade secrets
- Defamation of the defendant's reputation – effectively discouraging association/engagement with the defendant by clients, collaborators or other organizations in the market

For defendants, a trade secret management system makes it considerably more difficult for a plaintiff armed only with vague factual allegations to launch expensive trade secret misappropriation litigation.

Whether the victim of trade secret misappropriation or being accused of such behavior, organizations today need an internal system that provides the foundation for securing legal recourse in the courts so that they can protect and defend their company's valuable trade secrets. More specifically, they need a program that facilitates the identification, classification, protection, and valuation of trade secrets

Conclusion: Approximately 85% of the assets of corporations today are non-tangible as compared to 15% thirty years ago. Given this fact, coupled with the previously outlined facts and trends relating to the dynamics of today's corporate environment, it's understandable that more and more legal executives and legal counsel see trade secrets playing an increasingly important role in the portfolio of corporate intellectual property assets.

Because of this evolution, it is imperative that corporate boards and senior management take preemptive measures to shore up the policies, practices, technologies and procedures that govern their trade secrets, so that these valuable assets are protected and defendable.

As more companies rely on trade secrets instead of patents for the protection of their intellectual property, those that are well positioned to access and prevail in the courts will have a decisive advantage relative to other firms in their industries that do not. The key to being prepared, prevailing in court and ultimately protecting your hard earned, valuable and often critical trade secrets, is a Trade Secret Management System.

The Solution: A Comprehensive Trade Secret Management System

What Does a Trade Secret Management System Do?

Companies need a comprehensive trade secret management software solution that enables companies to identify, classify, validate, score and ultimately defend their trade secrets. Organizations that don't track the metadata and history of their trade secrets will face significant challenges defending them in court. A trade secret management software solution will enable companies to collect and compile the metadata related to its trade secrets and to maintain essential information related to the history of these assets, thereby providing the foundation for a robust protection and defense of valuable trade secrets.

Protecting and Defending an Organization's Trade Secrets

A trade secret management software solution **should support three essential requirements** related to protecting and defending an organization's trade secrets in court:

1. The software should enable the company to **validate the existence of its trade secrets** by documenting what it is, when it was created, when it was updated, who had access to the trade secrets and when they had access.
2. It should provide the company with **a systematic method to inventory and manage** their trade secrets.
3. The system should **assign a Defendability Factor** to each trade secret. This helps a company determine which trade secrets should be highlighted to the court and serves as a support to litigation.

Trade Secret Asset Classification

The foundation of a successful trade secret management program is the facilitation of trade secret **asset classification**. This allows trade secret assets to be identified and ranked, so that the level of security matches the level of importance of the trade secret asset. Security, without identification and classification, is flawed. In contrast, securing data after identification and classification of the trade secret assets makes it much easier for the internal security ecosystem to enforce trade secret protection policies and to prohibit unauthorized access, unauthorized disclosure, and unauthorized use.

Isn't It Dangerous to Put All of Our Crown Jewels in One Place?

By aggregating and analyzing the trade secret metadata, the system should construct a repository of information about the trade secrets. This is **not** a library of confidential trade secrets information, but instead provides an itemization of this information. Because the actual trade secrets are never inventoried in the system, it does not generate additional risk to the information. Instead, the software solution should facilitate the development of a critical and strategic resource, which

will serve as the foundation for the protection of the trade secrets and, if necessary, supports the successful prosecution of the misappropriation of those critical assets.

The Software Solution and Blockchain

The solution should be integrated with Blockchain. This is a crucial element of the value proposition of the software because it can assist at various stages of the life cycle of a trade secret, notably when it comes to the "reasonable measure of protection" and enforcement of a trade secret, i.e., the ability to prove that the information has been kept secret in the event of a misappropriation litigation.

Creating a trade secret inventory, and recording who had access to the information, have traditionally been considered "reasonable steps" in maintaining confidentiality. Recording trade secret metadata on a blockchain will fulfill this requirement under the EU Trade Secrets Directive and equivalent laws elsewhere.

Another huge benefit of the ability to Blockchain, is that since Blockchain enables the recording of time stamped and "hashed" (encrypted) information in a secure and immutable environment, it can prove the existence and ownership of a trade secret at a certain time (e.g., if X asserts that it created the same trade secrets prior to competitor Y).It also ensures the authenticity of the data stored in the system.

Registering trade secrets on a blockchain creates an indisputable, verifiable record of creation that meets the required evidentiary standards in a trade secret misappropriation lawsuit and may significantly strengthen a party's legal position.

Audit Trail

Providing the proper tools for litigation is an essential element of a robust trade secret management program. A trade secret management system should provide a complete audit trail of information collected as well as the changes made over time to that information, all in accordance with the court-accepted methods of ensuring the accuracy and integrity of the data are provided.

The Defend Trade Secrets Act (DTSA)

The DTSA creates a new paradigm. Sometimes, the protection of trade secret assets requires emergency actions. Once lost, a trade secret is lost forever. In these circumstances, the DTSA requires that the plaintiff (the trade secret owner) file suit and successfully obtain a DTSA ex parte seizure order before the defendants know the suit has been filed. Otherwise, without the element of surprise, the defendants–often with several clicks of a computer mouse –can transfer the trade secrets outside the country and destroy the evidence of trade secret theft by running data and file destruction software.

To take advantage of this robust provision of the DTSA, the trade secret owner must be able to move faster than the trade secret thief. Standard operating procedures of simply retaining outside counsel to investigate and litigate will often result in a long-gone trade secret.

If management waits until the trade secret theft occurs to identify what the trade secret is and investigate the evidence of misappropriation, the actual trade secret assets will be long gone before counsel can provide the U.S. district court with the proofs necessary to obtain an ex parte seizure order. The potential result could be catastrophic.

To avoid this, senior executives and those charged with the governance of the company, need to take reasonable measures to protect the corporate trade secret assets from a variety of threats, including deliberate or accidental exposure/leakage, insider theft, external misappropriation or foreign economic espionage.

The Defend Trade Secrets Act provides powerful provisions for ex parte seizure orders, but companies cannot take advantage of these provisions unless effective trade secret management protocols (as discussed above) are in place.

Conclusion – Forewarned is forearmed

In light of the DTSA and all of the trends threatening a company's trade secret assets, organizations would be well served to adopt policies, practices, technologies and procedures for the identification, classification, protection, and valuation of the company's trade secrets.

To put it all into perspective, a recent report by **AIPLA** in their **Report of the Economic Survey**, conducted in 2021, the mean cost to litigate a trade secret misappropriation case (involving risk of greater than $25 million) inclusive of discovery, pre-trial, trial, post-trial and appeal, was $4.6 million, and with first and fourth quartile of respondents reporting litigation costs of $1.5 million and $8 million, respectively.

Putting a trade secret management system in place before an actual or threatened misappropriation occurs, will go a long way to protecting a company's crown jewels and put the organization in a stronger position to discourage malicious behavior by bad actors, prevail in court and ultimately help management sleep better at night.