

# ■ Winning Strategies for Trade Secret Litigation

David L. Greenspan – McGuireWoods LLP – [dgreenspan@mcguirewoods.com](mailto:dgreenspan@mcguirewoods.com)  
Nicholas D. SanFilippo – McGuireWoods LLP – [nsanfilippo@mcguirewoods.com](mailto:nsanfilippo@mcguirewoods.com)  
Kristopher A. Boushie, CPA, ABV, CFF, CVA, CFE –  
NERA Economic Consulting – [Kristopher.Boushie@nera.com](mailto:Kristopher.Boushie@nera.com)



## What are the Essential Elements to a Claim for Misappropriation of Trade Secrets? ■ ■ ■

Trade secret misappropriation was traditionally a tort claim at common law. In 1979, the Uniform Trade Secrets Act (the “Act”) was published. Since then, 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted some form of the Act.<sup>1</sup> Moreover, in some circumstances, an act of misappropriation can also be a federal crime.<sup>2</sup> But what is a trade secret and what acts violate the law?

To qualify as a trade secret, information must satisfy two elements: it must derive independent value from not being generally known to, or readily ascertainable through appropriate means by, other persons who might obtain economic value from its disclosure or use; and, it must be the subject of reasonable efforts to maintain its secrecy. If these elements are satisfied, then an owner of the trade secret must prove that the information at issue was wrongfully acquired—that the information was misappropriated.

In some cases, a trade secret may be obtained by lawful means (such as independent discovery, reverse engineering, and, more frequently, inadvertent disclosure resulting from the failure to take

reasonable protective measures). Unlike patents, trade secrets have no finite statutory life. In principle, as long as a trade secret maintains the definitional requirements of the Act, the owner can sue for misappropriation of trade secrets whenever it occurs.

## How Does Trade Secret Litigation Most Often Arise? ■ ■ ■

One can hardly listen to the news without encountering a report of hacking, whether it is a full-scale attack, like recently suffered by Sony Pictures Entertainment, or a point-of-service hack of customer payment information, like recently suffered by Target. Trade secret litigation rarely follows from such theft, because the perpetrators of such attacks are either beyond the reach of the courts or possess insufficient assets to advance a civil claim. Another category of trade secret litigation comes from the concerted efforts of one company to discover the trade secrets of its competitor. Here, there is a spectrum of conduct between lawful efforts to reverse engineer information and industrial espionage.

Somewhere on this spectrum is “employee raiding,” the effort to gain access to knowledge, information, and/or skills by recruiting a competitor’s employees. If a review of published trade secret opinions is an indication of frequency, most trade secret cases are coupled with employee mobility claims. An employee leaves one employer for another: What did she take with her? How did she take it? What can she use? These are the questions that often

<sup>1</sup> <http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act>.  
<sup>2</sup> See e.g., *Economic Espionage Act of 1996*, 18 U.S.C. §§ 1831-39 (2014). In addition, both houses of Congress have proposed legislation that would make the theft of trade secrets a federal crime. “Senators Coons, Hatch introduce bill to combat theft of trade secrets and protect jobs,” <http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs>, last accessed July 16, 2014.

form the basis for multi-count litigation against former employees and, in many cases, their new employer.

## Strategic Considerations Regarding Trade Secret Cases – Pre-Litigation ■ ■ ■

Proactive initiatives to increase the secrecy and protection of trade secrets are essential to winning a trade secret claim. Indeed, it is an essential element of the cause of action without which no claim can stand. Therefore, companies should consider multiple preventative measures to ensure trade secret protection.

Employers should evaluate their physical and network security protections. From locks, key cards, and restricted access areas to network security infrastructure, investment in these protections will help keep outsiders from getting “in” and keep insiders from taking information “out.” Demonstrating that reasonable measures were taken to maintain the secrecy of information is essential to proving the second element of the definition of a trade secret.

Businesses should also adopt policies and procedures that focus on maintaining confidentiality. These policies may include confidentiality policies, codes of conduct, and information technology policies. These policies should both prohibit the acts the company wants to avoid and state the precautions each employee must take to ensure the continued confidentiality of the company’s information. Importantly, the policies and procedures must be consistently enforced.

On an employee level, companies should consider the propriety of requiring employees to sign restrictive covenants. Non-competition agreements, non-disclosure agreements, and confidentiality provisions are subject to state-specific law. What is enforceable differs from state to state. Drafting enforceable restrictive covenants is often an integral aspect of trade secret litigation because not only do effective restrictive covenants tend to show the company used reasonable efforts to maintain the confidentiality of their information, but covenants also provide additional leverage for the company in the event that trust is broken. Restrictive covenants, such as non-disclosure agreements, should also be carefully considered when sharing proprietary information with other companies as part of a cooperative or evaluative initiative.

It is important to regularly monitor employees’ activities. Although many companies take steps to ensure they are not hiring a high-risk employee, fewer take steps to monitor employees once they are employed. Monitoring can take the form of e-mail and weblog review, and reminding employees of their responsibility to safeguard information and company-owned electronic media.

If an employer suspects that a current or former employee has stolen trade secrets, the employer should immediately image and store any company electronic media to which the employee

had access, suspend any automatic deletion protocol, store the original electronic media in a manner so as not to disturb any metadata, and conduct a forensic analysis of the images. In trade secret cases, forensics and electronic media management, done early and correctly, can be the single most critical factor in winning the case. A trained forensic investigator can determine whether a recently separated employee moved large quantities of files to a thumb drive on his last day of employment, whether he was emailing files to his personal email account, or whether he was using special software to cover his tracks.

## Litigating Trade Secrets Cases – From Filing through Discovery ■ ■ ■

Although generally difficult to obtain, a preliminary injunction, temporary restraining order, or exclusion order to prevent continued use or disclosure of the company’s trade secrets during the pendency of the litigation can change the entire course of the litigation. In order to obtain a preliminary injunction, a litigant has to show that it has suffered or will suffer irreparable harm and that monetary damages are insufficient to make the litigant whole. In addition, the litigant must act quickly to protect its rights by marshaling its evidence of trade secret theft as early as possible. This is where thorough and timely forensics are most important, as the court will very likely hold a hearing at which it will analyze the evidence of the theft to determine if there is a likelihood of success on the merits. If the litigant can prove that trade secrets were taken through forensic evidence, there is a good chance the court will impose a preliminary injunction. Once a preliminary injunction is in place, the defendant finds itself in quite a quandary by having to ensure that none of the trade secrets are being used or disclosed. This can have a substantial impact on the defendant’s business, which can often lead to settlement soon after the preliminary injunction is entered.

**Venue.** No trade secret litigation should be filed without giving consideration to the venue—state court/which state, federal district court, The International Trade Commission (“ITC”), or international forums. One of the advantages a plaintiff has in these cases is that it may use the time before filing to conduct forensics, marshal its evidence, and prepare its discovery requests. The defendant is often forced to catch up while defending the case. For this reason, plaintiffs in trade secret cases are often benefited by filing in the appropriate venue with the shortest discovery time and fastest time to trial. Consideration should also be given to whether state or federal court is more appropriate given the amount of damages and the citizenship of the litigants.

**Domestic Versus International Forums.** The first place the potential trade secret plaintiff should consider filing is in the United States, whether in state or federal court. The U.S. has a robust set of laws that address the issue of trade secret theft. Federally, the Computer Fraud and Abuse Act prohibits accessing

a computer system without authority and taking information therefrom.<sup>3</sup> In addition, the Economic Espionage Act makes the theft or misappropriation of a trade secret a criminal act.<sup>4</sup> Nearly every state has adopted some form of the Uniform Trade Secrets Act, which provides robust protections for trade secrets. Even if the theft of trade secrets does not violate federal law, litigation in district court is still possible under certain conditions.

If quick resolution and keeping a foreign misappropriator out of the market are primary goals, then the ITC may be an appropriate forum. An ITC action can be filed against a foreign entity, even when the misappropriation both occurs and is practiced outside of the U.S.<sup>5</sup> Success at the ITC will likely result in the exclusion of the foreign misappropriator's product from the U.S. market.

While the U.S. court system is often the best choice for filing a trade secret case, it is not the only option. Recently, the European Union proposed the Directive on Trade Secrets, which would provide rights and remedies similar to those provided by the Uniform Trade Secrets Act.<sup>6</sup> If the Directive is adopted, the European Union would become a viable place to maintain a trade secrets case where filing in the U.S. is not possible (e.g., where personal jurisdiction cannot be exercised over the potential defendant). In addition, World Trade Organization member nations who have signed the Agreement on Trade Related Aspects of Intellectual Property Rights are required to provide protection for trade secrets.<sup>7</sup> Any decision to file a trade secret litigation outside the United States should be accompanied by a specific and thorough examination of the proposed venue nation's laws and legal system.

**Discovery Issues—Liability Related.** The proper and thorough use of forensic analysis and immediate focus on the prevention of spoliation is of critical importance in trade secret discovery. Spoliation is the destruction or modification of evidence that may be relevant to litigation after the duty to protect that evidence has arisen. The duty of preservation arises once a party knows or has reason to know that the evidence is or may be relevant to a potential future litigation.<sup>8</sup> Thus, the plaintiff in a trade secret case should put a hold in place internally, since it may possess much of the evidence, as soon as it believes there is a likelihood that it is going to proceed with its case.

In some cases, such as where a plaintiff quickly marshals its evidence and heads to court to seek a preliminary injunction, the first time a defendant's duty to preserve arises is when it is served with the complaint (or becomes aware that one has been filed against it). In most cases, however, it is recommended that a plaintiff who has decided to file a trade secret action send any

and all potential defendants a litigation hold notice informing the potential defendants that the plaintiff is contemplating suit and that the defendants are required to preserve any and all potential evidence. Triggering the duty to preserve early on can mitigate any spoliation issues and increase the possibility of negotiating a settlement. Conversely, spoliation can lead to contentious and protracted litigation and sanctions, and should be avoided.

Another discovery issue in trade secret litigation, particularly in the government contracting space, is the handling of classified, secret, and top secret and otherwise protected documents (e.g., unclassified, for official use only). Where there is theft of classified government information, a civil trade secret lawsuit is of least concern. However, where the theft was not of classified information, but trade secrets that relate to a classified product or service, litigants may find that classified documents are responsive to discovery requests. In this case, the litigant in possession of the government-classified documents will find itself in a dilemma, especially if it is ordered to produce the documents. It cannot turn over the documents or it will run afoul of federal law governing the handling of classified information. It also cannot disobey a court requiring their production. In this situation, a plaintiff in possession of classified documents should, if possible, narrowly tailor its claims to ensure that no claim is made related to the theft of classified documents or information. In the alternative, the litigant should expect a pitched battle from defense counsel and be prepared to drop parts of claims should it be ordered to produce classified documents.

**Discovery Issues—Damages Related.** While liability-related discovery is of paramount importance, the question of damages is a key component in obtaining an injunction or temporary restraining order. The focus of damage discovery is related to the types of monetary relief available to the owner of the trade secrets.

The trade secret owner is entitled to damages, which “can include both the actual loss caused by misappropriation and the unjust enrichment caused by the misappropriation that is not taken into account in computing actual loss.”<sup>9</sup> The Act prohibits double counting of the loss to the owner and the unjust benefits to the misappropriator.<sup>10</sup> In place of actual damages or unjust enrichment, damages can be measured by a reasonable royalty for the unauthorized disclosure or use of a trade secret.<sup>11</sup> In the case where the misappropriation was willful and malicious, “the court may award exemplary damages in an amount not exceeding twice any [damage] award....”<sup>12</sup>

<sup>3</sup> 18 U.S.C. § 1030(a).

<sup>4</sup> 18 U.S.C. § 1831(a).

<sup>5</sup> *Tianrui Group Co. v. ITC*, 661 F.3d 1322, 1337 (Fed. Cir. 2011). Selecting the ITC as a forum requires that the misappropriated trade secret(s) be used in the manufacture of goods being imported into the U.S. Further, the U.S. claimant must produce evidence that the importation of the good produced using unfair practices threatens to “destroy or substantially injure” a domestic industry. See *TiaRui* and §1337(a)(1)(A).

<sup>6</sup> COM(2013) 813 final, 2013/0402 (COD), see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0813:FIN:EN:PDF>.

<sup>7</sup> [http://www.wto.org/english/tratop\\_e/trips\\_e/t\\_agm0\\_e.htm](http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm).

<sup>8</sup> See, e.g., *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

<sup>9</sup> Uniform Trade Secrets Act with 1985 Amendments, pp. 9-10.

<sup>10</sup> *Id.*, p. 10.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

To obtain lost profits damages, the evidence must support a nexus between the misappropriation of the trade secret and lost sales. There should be sufficient discovery to isolate whether there were other factors that could be responsible for the sales being lost to the misappropriator. Depending on the facts and circumstances of the case, this causal link can be difficult to show. Even when the misappropriator's sales can be directly linked to the use of the trade secret, evidence should support the assumption that the trade secret owner would have made the sales absent the misappropriation. Lost profits discovery can be extensive and should focus on sales volumes and revenues, cost of sales and related costs, customers, market conditions, competitors, and substitute products or services.

In matters where an entire product-line workforce joins a competitor, taking with it proprietary knowledge, damages may be equal to the lost business value of the product line. Where possible, the damage expert should disaggregate damages to show damages for each separate claim asserted (e.g., misappropriation of trade secrets, breach of contract, tortious interference of a contract, etc.). Disaggregation of damages is helpful should the client not prevail on all counts. This is not to say that the measure of damages for separate claims cannot be the same, but not additive, for different illegal acts.

As mentioned above, the Act also allows for the trade secret owner to claim the unjust enrichment realized by the misappropriator. The discovery focus for a claim of unjust enrichment is considerably less extensive than for lost profits. The starting point for a claim of unjust enrichment is the misappropriator's revenue related to products produced using the trade secrets. Typically, the burden is on the misappropriator to show costs, although discovery should include requests for direct and indirect cost information.

The Act allows, "[i]n lieu of damages measured by any other methods...for a reasonable royalty..."<sup>13</sup> Evidence supporting a royalty should be provided for both the royalty rate and the royalty base.<sup>14</sup> This can be provided by looking at licenses for similar know-how as licensed in or out by the parties, or through third-party agreements.

Comments to the Act state that "a monetary recovery for trade secret misappropriation is appropriate only for the period in which information is entitled to protection as a trade secret, plus the additional period, if any, in which a misappropriator retains an advantage over good faith competitors because of misappropriation."<sup>15</sup> Evidence should be produced that supports how long the trade secret has been maintained, unsuccessful attempts to reverse engineer the trade secret, and the time and cost associated with replicating the trade secret to help prove the length of this additional period.

**Attorneys' Fees.** The Uniform Trade Secrets Act permits a court to award attorneys' fees to a victorious litigant where "(i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists."<sup>16</sup> Clearly, this is a double-edged sword. While a plaintiff may win fees where it can prove willful and malicious misappropriation, it must be sure not to bring a trade secret claim prior to assembling sufficient information. Where a plaintiff is able to make a convincing case that it will be able to demonstrate a willful and malicious appropriation, the settlement prospects for the case increase tremendously.

## Conclusion ■ ■ ■

Although trade secret litigation, like all litigation, has the potential to be a long and painful process, there are a number of steps businesses can take to increase the likelihood of achieving a favorable outcome.

David L. Greenspan is a Partner in the Labor & Employment group at McGuireWoods LLP. Mr. Greenspan is a trial lawyer whose practice focuses on proactive counseling and aggressive litigation of employee mobility disputes and complex employment matters and works with his clients to identify and resolve issues before they become adversarial in nature. Mr. Greenspan can be reached at +1.703.712.5096 or [dgreenspan@mcguirewoods.com](mailto:dgreenspan@mcguirewoods.com).

Nicholas D. SanFilippo is an Associate in the Labor & Employment group at McGuireWoods LLP. Mr. SanFilippo represents employers in litigation arising from the employment relationship. Mr. SanFilippo can be reached at +1.703.712.5378 or [nsanfilippo@mcguirewoods.com](mailto:nsanfilippo@mcguirewoods.com).

Kristopher A. Boushie, CPA, ABV, CFF, CVA, CFE is a Vice President in NERA's Intellectual Property Practice. He has over 30 years of experience in financial and litigation consulting, with an emphasis on forensic valuation issues, and over 20 years of experience focused on intellectual property matters. Mr. Boushie can be reached at +1.202.466.9282 or [Kristopher.Boushie@nera.com](mailto:Kristopher.Boushie@nera.com).

This article is intended for general information purposes only and is not intended to provide, and should not be used in lieu of, professional advice. The publisher assumes no liability for readers' use of the information herein and readers are encouraged to seek professional assistance with regard to specific matters. Any conclusions or opinions are based on the specific facts and circumstances of a particular matter and therefore may not apply in all instances. All opinions expressed in these articles are those of the authors and do not necessarily reflect the views of Stout Risius Ross, Inc. or Stout Risius Ross Advisors, LLC.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> Uniform Trade Secret Act § 4.