PLI Current

The Journal of PLI Press

Vol. 6 (2022)

# Your Trade Secret May Be at Risk: What Should You Do in the Early Stages of a Trade Secret Dispute?

**Leigh Ann Buziak**

*Blank Rome LLP*

**Seth Gerber**

*Morgan, Lewis & Bockius LLP*

Litigating trade secret disputes is typically intense, fast paced, and hotly contested. The aggrieved party may have been betrayed by a trusted former employee or a potential business partner, or has been subjected to hacking or other nefarious means of obtaining sensitive business information, such as theft, bribery, misrepresentation, breach of a duty of confidentiality, or espionage. Lawyers need to mobilize their resources with alacrity and marshal their evidence so that they can promptly dispatch the appropriately swift legal response to protect valuable business information, whether through a cease-and-desist letter, rushing into court to seek an emergency temporary restraining order, or expedited discovery to aid in a motion for a preliminary injunction.

Knowing what to do, what steps should be taken, and what your legal options are is critical to implementing your strategy and achieving your client's objectives to protect their confidential, proprietary, and trade secret information. Quickly.

This article addresses what should be done *before* filing a lawsuit when there has been misappropriation or there is a potential threat to improperly acquire, use, or disclose your client's trade secrets. Part I discusses the statutory background for U.S. trade secrets law; part II addresses common threats to companies' trade secrets; part III provides suggested techniques to assess threats through investigative techniques; and part IV discusses potential outcomes to resolving trade secret disputes. This article also briefly touches on the use of forensics to detect and reduce risks when employees depart your client's company or are joining as new employees and going through an onboarding process.

## I. Statutory Background

United States trade secrets law developed from state court opinions. By 1979, these court decisions were memorialized in a Uniform Trade Secrets Act ("UTSA"), which has been adopted in 49 states and the District of Columbia. In 1996, the U.S. Congress enhanced trade secret protections by enacting the Economic Espionage Act ("EEA"). This statute allows federal prosecutors to pursue criminal charges arising from the theft of a trade secret for the benefit of a foreign entity and trade secret theft intended to confer an economic benefit to another party.

Trade secret owners can also seek exclusion orders from the International Trade Commission ("ITC") to ban the importation of goods into the United States that embody stolen trade secret information, even if the misappropriation occurs outside of the United States.[1]

In 2016, the U.S. Congress once again reacted to the continued threat of misappropriation of trade secrets by enacting the federal Defend Trade Secrets Act ("DTSA").[2] The DTSA provides a private civil right of action in federal court if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.[3] Under the DTSA, an owner of trade secrets may seek an emergency seizure order or an injunction to prevent actual or threatened

[1] 19 U.S.C. § 1337.

[2] 18 U.S.C. § 1836.

[3] 18 U.S.C. § 1836(b)(1).

misappropriation and recover an award of damages for actual loss or unjust enrichment, or a reasonable royalty, as well as attorneys' fees and an award of exemplary damages in the amount of two times the damages if the trade secrets were willfully and maliciously misappropriated.[4] Some courts have relied on the extraterritoriality provision of the EEA to allow DTSA claims to proceed concerning overseas misappropriation if an act in furtherance of the offense was committed in the United States.[5]

## II. Typical Scenarios Threatening Your Client's Trade Secrets

Scenarios which lead to trade secret disputes include external threats from hackers and foreign governments, internal threats from departing employees or your client's contractors or licensees, and deal-gone-bad situations where trade secrets are exchanged pursuant to a non-disclosure agreement in connection with a potential transaction and the receiving party improperly retains and uses that information after the deal is called off. While there are certainly other scenarios which can lead to trade secret disputes, based on our common experience, these three scenarios present the biggest threats.

### *A. External Threats*

One of the biggest threats to your client's trade secrets comes from foreign governments, which FBI Director Christopher Wray emphasized in remarks to business leaders in London in July 2022.[6] One of the ways the U.S. government has tried to combat such external threats from foreign governments and external actors is through the passage of the DTSA. The DTSA expresses Congressional concern about

---

[4] 18 U.S.C. § 1836(b)(3).

[5] *See, e.g.*, Micron Technology, Inc. v. United Microelectronics Corp., Case No. 17-cv-06932-MMC, 2019 WL 1959487 (N.D. Cal. May 2, 2019); *see also* Jeffrey A. Pade & Thomas A. Counts, *Trade Secrets Litigation Concerning Foreign Acts*, 85 DEF. COUNSEL J. 1 (2018).

[6] *See* FBI Director's London Visit Reinforces Commitment to U.K. Partnership, FBI (July 6, 2022), https://www.fbi.gov/news/stories/director-visits-united-kingdom-for-meetings-with-uk-counterparts-070622; Christopher Wray, Director, FBI, Director's Remarks to Business Leaders in London, FBI (July 6, 2022), https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622.

trade secret theft "around the world," which reflects an intent by Congress to not limit the DTSA's application to acts occurring within the U.S.[7] Furthermore, "some courts have concluded that [the EEA's] extraterritorial provisions also apply to the DTSA"[8] and cover misappropriation claims based on "conduct occurring outside the United States" where (i) the "offender" is a natural person who is a citizen or permanent resident alien of the U.S., or an "organization" organized under the laws of the U.S. or a state or political subdivision thereof; or (ii) "an act in furtherance of the offense was committed in the United States."[9]

### B. Internal Threats

With the click of a mouse or use of a USB thumb drive, employees, including high-ranking executives, with access to sensitive, valuable business information can pose a serious threat to your client's trade secrets. Given the broad scope of what type of information can qualify as trade secrets—including business, scientific, technical, economic, or engineering information—companies should restrict access to trade secrets to employees who have a need to know such information in order to perform their job functions. But even with implementing reasonable measures under the circumstances to protect the secrecy of such sensitive, valuable information, the internal threat posed by employees who may opt to start a competing enterprise, solicit away customers for a competitor, or duplicate your client's products, is significant.

For example, in May 2022, Appian Corporation, a cloud computing firm, won a $2.03 billion verdict in Virginia state court for misappropriation of trade secrets.[10]

---

[7] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, § 5 (May 11, 2016) (codified at 18 U.S.C. § 1836).

[8] The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach* (Mar. 2021), https://thesedonaconference.org/node/9804.

[9] 18 U.S.C. § 1837 (1996); *see* Micron Tech., Inc. v. United Microelectronics Corp., No. 17-cv-06932-MMC, 2019 WL 266518, at *3 (N.D. Cal. Jan. 18, 2019) (motion to dismiss granted where complaint did not sufficiently allege facts to support a finding that recruitment efforts in the U.S. were made in furtherance of any act of misappropriation); Vendavo, Inc. v. Price f(x) AG, No. 17-cv-0630-RS, 2018 WL 1456697, at *7 (N.D. Cal. Mar. 23, 2018) (granting motion to dismiss given the territorial and temporal limits of the DTSA).

[10] Appian Corp. v. Pegasystems Inc. & Youyong Zou, No. 2020-07216 (Va. Cir. Ct. Fairfax Cty. May 9, 2022).

Appian filed claims against Pegasystems Inc. and an individual, Youyong Zou, an employee of a government contractor, Serco, which used Appian software. Zou was a former developer for Appian. At trial, Appian submitted evidence that, among other things, Zou disclosed Appian's trade secrets to Pegasystems in violation of Zou's confidentiality restrictions. The jury concluded Pegasystems engaged in misappropriation of trade secrets as well as violations of the Virginia Computer Crimes Act.[11]

The Appian multi-billion-dollar trade secret verdict is just one recent example of the threat posed by former employees. In 2014, the FBI warned that "[e]conomic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing threat of cyber-enabled trade secret theft. The employee who poses an insider threat may be stealing information for personal gain or may be serving as a spy to benefit another organization or country."[12] The FBI has also warned about foreign governments sponsoring talent recruitment programs, or talent plans, to bring outside knowledge and innovation back to their countries, including by stealing trade secrets.[13]

### C. Failed Acquisitions and Shady Business Partners

The deal-gone-bad scenario is a common one. Two companies open discussions about a potential investment or acquisition, and they enter into a non-disclosure agreement ("NDA") to facilitate due diligence and the exchange of confidential and

---

[11] Trial Transcript, Appian Corp. v. Pegasystems Inc. & Youyong Zou, No. 2020-07216 (Va. Cir. Ct. of Fairfax Cty. May 5, 2022). *See also* Kate Andrews, *McLean-Based Appian Wins $2B Verdict in Trade Secrets Lawsuit*, VIRGINIA BUSINESS (May 10, 2022), https://www.virginiabusiness.com/article/mclean-based-appian-wins-2b-verdict-in-trade-secrets-lawsuit/#:~:text=Appian%20Corp.%2C%20a%20cloud%20computing,sued%20Massachusetts%2Dbased%20Pegasystems%20Inc.

[12] News Release, Combating Economic Espionage and Trade Secret Theft, Statement for the Rec., Testimony of Randall C. Coleman, Assistant Dir., Counterintelligence Div., Fed. Bureau of Investigation, Statement Before the Senate Judiciary Comm., Subcomm. on Crime and Terrorism, Washington, D.C. (May 13, 2014), https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft.

[13] News Release, FBI, The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans (last visited Nov. 9, 2022).

trade secret information. After the opening of the kimono by the target company, the parties decide to go their separate ways, the target company requests that the other side destroy and return all of the confidential information, and rather than complying with the terms of the NDA, the receiving party uses the confidential information to hire away employees, solicit customers, or copy the disclosing party's products. Another possibility is the target company attempts to use the disclosure of its confidential and trade secret information as a weapon in litigation to attempt to forestall the acquiring company from exploiting products or technology it was independently developing.

Your U.S.-based client's trade secrets may also be put at risk by business partners, licensees, or manufacturers, especially if they are located overseas. For example, FBI Director Wray recently noted that certain foreign governments require U.S. and U.K. companies to partner with foreign businesses, partners that often turn into competitors.[14] Certain foreign governments have passed laws to loosen the rights and the security of companies operating in those countries by, among other things, requiring certain data to be stored in those countries or allowing the foreign governments to force employees in those countries to assist in their intelligence operations. Thus, companies must be especially cautious about their business partners, licensees, and manufacturers.

## III. Tips for Early Assessment of Risks Involving Trade Secret Information

When a party has taken trade secret information from your client, or your client has allegedly taken trade secret information, you must carefully examine the facts and relative strengths and weaknesses of the client's legal position. Evaluating the following information during the initial investigation will aid in assessing the business risk and formulating a strategy for resolving the issue.

**Assess Any Agreements and Access to Confidential Information.** As an initial matter, a determination must be made as to the scope of the information the misappropriating party had access to, what information could possibly be at risk, and the importance of this information to the business. This often involves analyzing

[14] *See* FBI, *supra* note 6. *See also* Kylie Bielby, *U.S. and U.K. Join in Warning on China's Multipronged Threat to the West, Including Cyber*, HOMELAND SECURITY TODAY (July 11, 2022), https://www.hstoday.us/featured/u-s-and-u-k-in-joint-warning-on-chinas-multi-pronged-threat-to-the-west/.

electronic devices, accounts, email, databases, folders, and the like to determine if any information may have been wrongly or improperly exfiltrated from these sources, which sometimes requires forensic analysis, as discussed below.

Another important first step is to assess any agreements that are in place to protect the information that may be at issue, including confidentiality agreements or, importantly, any non-compete or non-solicitation provisions that may provide additional options. It is critical to quickly get a handle on what obligations are owed to whom concerning the specific information, whether there are any additional causes of action or remedies that may be available, any required notice or return of property provisions, and the applicable forum and procedure for any dispute concerning the information.

**Assess Risk of Use or Disclosure of Trade Secrets by Misappropriating Party.** After gaining an understanding of the information at issue and the nature of the agreements in place, it is then critical to evaluate how and why it would damage the business if the information were to be used or disclosed. This step usually includes detailed fact-gathering interviews to identify the competitive landscape and risks, the relevant market and competitive pressures, the roles and responsibilities of the party misappropriating the information, the importance of the information at issue, and what the misappropriating party could potentially do with the information. This analysis will measure and assess the risk of irreparable harm to the business and level of response required (e.g., letter or litigation).

Courts have recognized various types of harm as a result of trade secret misappropriation, for example, lost customers, loss of market share, loss of goodwill, and exclusive time on the market.[15] However, courts have also found that a party

[15] *See* FMC Corp. v. Taiwan Tainan Giant Indus. Co., Ltd., 730 F.2d 61, 63 (2d Cir. 1984) ("[I]t is clear that the loss of trade secrets cannot be measured in money damages. . . . A trade secret once lost is, of course, lost forever."); Finkel v. Cashman Prof'l, Inc., 270 P.3d 1259, 1263 (Nev. 2012) (holding that interference with business including use of trade secrets was irreparable harm requiring injunctive relief); ReadyLink Healthcare v. Cotton, 24 Cal. Rptr. 3d 720, 732 (Ct. App. 2005) (affirming preliminary injunction against solicitation of employees and customers using stolen information); Prysmian Cables & Sys. USA, LLC Prysmian v. Szymanski, 573 F. Supp. 3d 1021, 1044 (D.S.C. 2021) ("the loss of a trade secret is difficult to measure in monetary damages because once the secret is lost, it is indeed lost

seeking to protect trade secrets has been unable to articulate any cognizable irreparable harm requiring injunctive relief.[16] As a result, it is important to understand the irreparable nature of any harm at issue early in the case so appropriate action can be taken.

**Assess Relative Value of Litigation Costs and Business Needs.** Litigation is costly and distracting but may be the only option for appropriate relief under some circumstances. When determining how to deal with a trade secret issue, consider if the employee or business deal at the center of the dispute is worth the cost of litigation, whether bringing or defending against it. Discuss with the client the strengths and weaknesses of potential litigation as well as available remedies and likely outcomes; and keep in mind that trade secret litigation typically occurs within a specific industry or market, meaning additional risks and benefits might apply if the litigation involves ongoing business relationships or the company's customers. There may be value in litigation to protect important legitimate business interests and ensuring competitors understand that the business will protect its rights. It may be an industry where litigation is frequent and expected, or one where cooperation is the norm and litigation to resolve issues would not be respected. There may be other reputational and market-based considerations and competitive pressures that influence the decision to litigate and must be assessed in determining the endgame for any trade secret dispute.

**Assess Forensic Evidence, As Applicable.** Whether bringing or defending a claim for misappropriation of trade secrets, the forensic evidence available from electronic devices and about electronic documents is vast and helpful to determine what

---

forever" and thus "threatened disclosure of a trade secret supports the imposition of injunctive relief."); Life Spine, Inc. v. Aegis Spine, Inc., No. 19 CV 7092, 2021 U.S. Dist. LEXIS 47323, at *78-79 (N.D. Ill. Mar. 15, 2021) (finding that loss of customers from a finite pool constituted irreparable harm).

[16] *See* DTC Energy Grp., Inc. v. Hirschfeld, 912 F.3d 1263, 1271 (10th Cir. 2018) (holding that "the district court did not abuse its discretion when it found that DTC had not shown a sufficient probability of irreparable harm from Defendants' past misconduct"); Pers. Wealth Partners, LLC v. Ryberg, No. 21-cv-2722 (WMW/DTS), 2022 U.S. Dist. LEXIS 9981, at *10 (D. Minn. Jan. 18, 2022) (conclusory allegations regarding harm were insufficient to support injunctive relief); InfoArmor Inc. v. Ballard, No. CV-21-01844-PHX-SMB, 2021 U.S. Dist. LEXIS 224237, at *15 (D. Ariz. Nov. 19, 2021) (finding no evidence of irreparable harm from use of confidential information).

happened—or did not happen, as it were—in a trade secret case and, in most circumstances must be taken into consideration when assessing the case.[17]

## IV. Options for Finding the Appropriate Resolution

Because trade secret cases necessarily occur in the business context, various methods can be used to obtain the optimal business result while preserving and protecting rights. Initially, those rights are usually asserted by letter or litigation and preexisting business terms may resolve concerns about the misuse of misappropriated information.

### *A. Letter or Litigation*

It is extremely common for trade secret disputes to be raised in the initial instance through a letter. The tone of the letter and the nature of the response often frames the trade secret dispute and how it will be resolved. The initial letter may be a gentle reminder to the recipient of their obligations to protect and return trade secret information and to not disclose or use it without authorization. Or the letter may be incendiary, threatening imminent litigation unless certain conduct immediately ceases and desists. It may be important in certain circumstances—for example, if it is clear that information has been compromised but unclear whether it has been used—to send a letter reserving rights in case a future development reveals that trade secret information has likely been used.

A cease-and-desist letter may also demand the return and accounting of any outstanding property, including a certification that the party no longer has any information or property, such as company-issued computers, smartphones, and USB devices, as well as assurances regarding the party's future job position or business, to assess potential risks to trade secrets. Depending on the circumstances and if litigation is imminent or expected, the letter may also contain a litigation hold notice.

If litigation is necessary, carefully assess jurisdiction, venue, and procedure and whether to seek a temporary restraining order or a preliminary injunction and

---

[17] For more details on forensic examination and the helpful assistance that it can provide in these types of cases, *see* Jim Vaughn & Mike Bandemer, *Digital Forensics in Trade Secret Investigations*, in TRADE SECRET LITIGATION AND PROTECTION: A PRACTICE GUIDE TO THE DTSA AND THE CUTSA (Randall E. Kay et al. eds., 2022).

expedited discovery. Procedures for injunctive relief differ in the federal and state courts as well as in arbitration. And immediate injunctive relief may not be necessary in every situation; the party seeking to protect its information may instead decide to monitor for damages arising from the suspected misappropriation. In other circumstances, it may be necessary to make a criminal referral to the United States Department of Justice or, if the facts justify it, seek *ex parte* relief under the DTSA.

### B. Potential Terms of Resolution

Depending on the particular facts of the case, trade secret disputes may be resolved without litigation if the trade secrets have not yet been used or disclosed and the party has not yet breached any of its obligations. An aggrieved party may be satisfied by receiving certifications from the relevant parties that they have not used, disclosed, transferred, or received any of the confidential information. Additionally, the dispute may be resolved by developing a protocol (with or without the help of an independent forensic examiner) whereby devices containing trade secret information are removed or remediated.[18]

The more complicated situations, of course, involve intentional misappropriation or actual disclosure of the trade secret to a third party. In these situations, the parties may be forced into litigation and expedited discovery to determine what occurred before they can consider any resolution. Depending on the circumstances, the parties may be able to reach agreement on appropriate stipulated court orders to preserve and protect information, which may provide even more solace and protection to the party from whom information was appropriated. A court order is enforceable through contempt sanctions, which can also be a valuable protection against future misappropriation and use of the trade secrets.

## V. Takeaways and Helpful Preventative Steps

Clients and counsel can take affirmative steps to ensure that the early stages of a trade secret dispute are handled as seamlessly as possible. First, it is helpful when the business has already implemented protocols to ensure that its confidential and proprietary information is classified, identified, and maintained as secret within the company. Second, the company's agreements, including confidentiality provisions, should be up to date and reviewed to ensure they are enforceable to the maximum of the state law under which the business is operated. Finally, the company should audit

[18] *See id.*

and check its security measures in light of potential threats to its trade secret information and protect accordingly to demonstrate that it has taken reasonable measures to safeguard its information.

---

**Leigh Ann Buziak** concentrates her practice in business disputes, with a concentration in handling difficult employment, unfair competition, and related intellectual property issues. She focuses her practice on drafting, negotiating, and litigating restrictive covenants, pursuing departing employees for theft of trade secrets, business relationships, proprietary business information, and defending companies from accusations of the same. Leigh Ann also provides strategic advice and counsel in employment matters, litigation risks, and investigations. Leigh Ann has developed substantial experience in working with developing digital evidence, including forensic investigations.

**Seth M. Gerber** is an accomplished trial lawyer who focused on trade secret and noncompete matters. Seth's cases cover a broad range of confidential and trade secret information from customer lists to sophisticated, innovative technologies, including semiconductors, electric fracking equipment, and custom-engineered parts for aerospace, space, and military industries. Seth has experience in cross-border litigation and forensic investigations. He also counsels clients with respect to defining, classifying, and protecting their confidential, proprietary, and trade secret information. Seth has successfully defended complex mass raid cases to verdict after lengthy jury trials, and obtained and defeated ex parte applications for temporary restraining orders and motions for preliminary injunction in jurisdictions across the United States.

Leigh Ann and Seth presented Your Trade Secret May Be at Risk: What Should You do in the Early Stages of a Trade Secret Dispute? at PLI's Advanced Trade Secrets 2022: New Risks, New Challenges, New Ideas

---