Bloomberg BNA

Daily Labor Report®

The Defend Trade Secrets Act: A Powerful New Tool for Employers

Trade Secrets

Given the immense value of trade secrets to American companies, the prospect of trade secret theft is a serious threat. The Defend Trade Secrets Act provides a new, powerful tool to combat trade secret theft in federal court. In this Bloomberg Law Insights article, Michael Renaud, Bret Cohen, and Nicholas Armington of Mintz Levin Cohn Ferris Glovsky and Popeo PC examine the provisions and protections of the DTSA, and explain the aspects of the law that employers and trade secret owners must be aware of in order to fully take advantage of the newest tool to combat trade secret theft.

By Michael Renaud, Bret Cohen, and Nicholas Armington

Michael T. Renaud is Division Head for the Intellectual Property Section at Mintz Levin Cohn Ferris Glovsky and Popeo PC, and serves on the firm's Policy Committee. Michael has extensive experience litigating patent cases in U.S. District Courts, the International Trade Commission, and before the Federal Circuit. He also has a great deal of experience litigating trade secret cases.

Bret Cohen is co-chair of the Employee Mobility, Non-Competes & Trade Secrets Practice at Mintz Levin Cohn Ferris Glovsky and Popeo PC. His practice includes representing employers in employment litigation, including claims arising under state common law, breach of contract, wrongful termination, defamation claims and has an extensive national experience litigating non-compete, non-disclosure, and trade secret claims.

Nicholas W. Armington is an associate at Mintz Levin Cohn Ferris Glovsky and Popeo PC, where his intellectual property practice focuses on patent and trade secret litigation.

Trade secrets provide significant value for American companies. Take, for example, the formula for Coca-Cola. The exact formula for the popular soft-drink is a closely guarded secret, and Coca-Cola's exclusive ability to make its soft-drink is extremely valuable—indeed, it is the foundation of Coca-Cola's entire business. Given the immense value of trade secrets to American companies, the prospect of trade secret theft is a serious threat. The Defend Trade Secrets Act provides a new, powerful tool to combat trade secret theft in federal court. This article examines the provisions and protections of the DTSA, and explains the aspects of the law that employers and trade secret owners must be aware of in order to fully take advantage of the newest tool to combat trade secret theft.

A Federal Cause of Action

The DTSA amends the Economic Espionage Act (EEA) to create, for the first time, a federal civil cause of action for trade secret misappropriation. Under the DTSA, a party whose trade secrets were stolen can bring an action in federal court to stop any ongoing theft, prevent further theft, and seek damages for a theft that has already occurred. Specifically, a trade secret owner may bring a civil action in federal court for misappropriation where ''the trade secret is related to a product or service used in, or intended for use in, interstate of foreign commerce.''

Until the passage of the DTSA, trade secret actions were governed entirely by state trade secret law, which

generally involved application of a version of the Uniform Trade Secrets Act (UTSA)—a model act created by the Uniform Law Commission, and adopted by the vast majority of U.S. states (Massachusetts and New York being the only exceptions). Bringing suit under the DTSA allows a party to avail itself of the federal courts, which is advantageous where federal courts may be more adept to address highly complex technical issues arising in trade secret cases. While the DTSA provides trade secret owners with a new federal cause of action, it does not preempt existing state trade secret law regimes. Practically, this means that a trade secret owner can bring co-pending state and federal claims for trade secret misappropriation. Because UTSA or common law based state trade secret laws may provide slightly different relief than the DTSA, it is important that litigants consider bringing co-pending state and federal trade secret claims so as to gain full protection under the available causes of action.

What is a Trade Secret?

A trade secret is any commercially valuable information that is not publicly known where reasonable effort is taken to preserve its confidentiality. The DTSA defines ''trade secret'' broadly as ''all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.''

This definition does not differ significantly from the definition for trade secret in the UTSA, and it contains the familiar requirements of the UTSA that the trade secret ''derives independent economic value, actual or potential, from not being generally known,'' and that the trade secret owner has undertaken reasonable efforts to keep the information secret.

Although minor, the differences in the definition of ''trade secret'' between the DTSA and UTSA will not always be insignificant. Indeed, litigants have already attempted to take advantage of the differences in definition. For example, in *RF Micro Devices, Inc. v. Xiang*, No. 1:12CV967 (M.D.N.C. July 14, 2016), the defendant was accused of stealing trade secrets owned by RF Micro Devices, Inc. for the benefit of a competing Chinese company. In a separate criminal action, the defendant pleaded guilty to criminal misappropriation of trade secrets under the EEA. However, the civil case was brought under North Carolina trade secret law, which has a slightly different definition of trade secret than that found in the EEA. Relying on this slight difference, the defendant argued that the ''bar for what qualifies as a trade secret is higher under North Carolina law, and as such, his guilty plea cannot by itself establish liability under [North Carolina law].'' Because the DTSA does not preempt existing state trade secret law, federal and state trade secret law is destined to coexist for the foreseeable future. Parties should be aware of and take advantage of the differences between state and federal trade secret statutes where possible.

Maintaining Secrecy of Trade Secrets Through Reasonable Efforts

The DTSA requires that trade secret owners take ''reasonable measures to keep [trade secret] information secret.'' The ''reasonable measures'' requirement is not unique to the DTSA, and trade secret owners should continue to follow best practices to maintain secrecy of their proprietary information and ensure protection of state and federal trade secret laws. The below list gives examples of reasonable steps to protect your trade secrets:

• Identify and label trade secret information as ''confidential''

o Provide notice to those inside and outside your company that trade secret information is in fact confidential.

o Don't over-designate company material—not every piece of information related to a company will warrant a confidentiality label and over-designation will dilute the effectiveness of the confidentially label.

• Establish companywide policies for handling confidential information

o Provide employees with a handbook setting forth policies and conduct periodic trainings.

o Inventory trade secrets and track which employees have access to trade secret information.

o Regularly audit trade secret information.

• Require employees to sign confidentiality and nondisclosure agreements as part of their employment agreement

o Prohibit employees from (1) disclosing confidential information beyond that specifically authorized and (2) disclosing confidential information after the end of employment.

o Develop standard confidentiality clauses for use in employee, contractor and supplier agreements.

• Adopt reasonable security measures

o Put physical and network security measures in place (including implementation of IT security standards such as ISO 27001, CO-BIT, NIST Framework, etc.).

o Take timely corrective action if security is compromised.

o Conduct due diligence on suppliers, business partners, and customers.

The above provides some key actions to consider when establishing your company's procedure for protecting its trade secrets, but is not an exhaustive list. Your company's trade secret asset management plan should be devised with the help of an attorney familiar with the best practices for trade secret protection.

Definition of Misappropriation under the DTSA

The definition of ''misappropriation'' under the DTSA does not differ from the definition for this term under the UTSA, and is as follows:

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

  DLR ISSN 0418-2693

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake.

There is a three-year statute of limitation for claims under the DTSA. This period begins when ''the misappropriation. . .is discovered or by the exercise of reasonable diligence should have been discovered.''

The DTSA generally applies to trade secret misappropriation that occurs on or after the date of the enactment of the Act (May 11, 2016), or began before the Act's enactment and continued after the Act took effect. This aspect of the DTSA has already been litigated. In *Arms v. Unified Weapon Sys.*, No. 8:16-cv-1503-T-33AEP (M.D. Fla. Sept. 27, 2016), the court examined ''whether [a trade secret] owner may recover under [the] DTSA when the misappropriation occurs both before and after the effective date, assuming the entire misappropriation is within the 3-year limitations period.'' Defendant argued that claims under the DTSA must be dismissed because the DTSA became effective only after the events at issue and any continuity of misappropriation should be treated as one misappropriation that began before the DTSA's enactment. The court disagreed, explaining that ''at the least,'' the language of the Act suggests that the DTSA applies to any act of misappropriation occurring after the effective date, noting that Congress omitted from the DTSA language in the UTSA indicating that continuing misappropriation that began before the effective date of the statute was not redressable under the UTSA.

DTSA Application Overseas

The terms of the Economic Espionage Act, which the DTSA modified, suggest that the DTSA can be used to address trade secret misappropriation where the theft occurred outside of the United States. Specifically, the EEA includes a provision indicating that the law applies to conduct occurring outside of the United States if the offender (1) is a citizen or permanent resident of the United States, (2) is a United States corporation, or (3) if ''an act in furtherance of the offense was committed in the United States.'' The DTSA's amendment of the EEA did not change this provision, suggesting that the DTSA is applicable to trade secret misappropriation taking place overseas.

The option to apply the DTSA to overseas conduct will be immensely valuable as overseas trade secret theft continues to proliferate. The increased threat of trade secret theft overseas is a result of the lack of strong IP rights protection in many foreign countries. Overseas application will be especially useful to address economic and corporate espionage originating in China. ''Chinese actors are the world's most active and persistent perpetrators of economic espionage.'' https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. Compounding this threat is the reality that ''[s]ignificant structural and institutional impediments undermine effective IPR enforcement in China[, including] a lack of coordination among government agencies, insufficient resources for enforcement, local protectionism, and a lack of judicial independence.'' https://www.usitc.gov/publications/332/pub4199.pdf. The DTSA's ability to address trade secret misappropriation overseas is valuable whether the theft occurs in China or another country with weak IP protections.

Civil Seizure Mechanism

The DTSA includes a civil seizure mechanism by which a court may direct federal marshals to seize property necessary to prevent the dissemination of stolen trade secrets. Using this tool, an American company can quickly prevent distribution of misappropriated trade secret information. This remedy does not exist in any state trade secret law.

Civil seizure can only be employed in ''extraordinary circumstances,'' however, and there are several predicates to its use. For example, the application must show that a temporary restraining order or preliminary injunction would be inadequate and that the individual against whom seizure is ordered would destroy or hide the misappropriated trade secret material if ordered to preserve or return it. The applicant must also show that the person against whom seizure is ordered is actually in possession of the stolen trade secret and must describe the material to be seized and provide its location. Once seized, the trade secret information remains under the court's control until a seizure hearing, during which the party who obtained the seizure order has the burden to prove the facts underlying the order.

The civil seizure mechanism has not yet been used, but its first use may be in the context of the theft of digitally stored trade secrets. This would follow the trend of early DTSA cases in which the misappropriated trade secrets have been stolen by employees using digital means. This is not surprising, given the ubiquitous connectivity of the modern workplace and increasing popularity of cloud storage services in the business context.

In one recent case, the DTSA was put to use by Monsanto Company and The Climate Corporation (collectively, ''Monsanto'') in *Monsanto Co. v. Chen*, No. 4:16-cv-876 (E.D. Mo.), after a former employee used technical expertise to steal valuable confidential information. In June 2016, the employee, a data scientist, announced his resignation and admitted that he was considering an offer to serve as Director of Resource Management and Bioinformatics for a competing Chinese seed company. Following this announcement, Monsanto performed a review of the employee's company-issued computer and discovered that it was loaded with highly sophisticated and unauthorized software that could be used to perform reconnaissance, seek vulnerabilities in the system, exfiltrate data, and conceal activity on the device. Additionally, following resignation, the employee's unique login credentials were used to remove dozens of files containing proprietary material from Monsanto's secure servers.

In seeking a temporary restraining order and preliminary injunction, Monsanto argued that there was a substantial likelihood that it would succeed on the merits because the former employee used improper means to covertly acquire highly valuable trade secret information that Monsanto had taken reasonable steps to keep confidential. Monsanto also argued that it would suffer irreparable harm if the former employee was not prevented from disclosing trade secrets to the seed com-

pany in China because the stolen material related to strategy, sensitive products, and confidential research. The Court granted a TRO and preliminary injunction directing the former employee to (1) return all trade secret information, (2) disclose the persons with whom the trade secret information was shared, and (3) identify all cloud storage locations where trade secret information was kept. For a further discussion of this case, see https://www.globalipmatters.com/2016/08/24/industrial-espionage-and-the-defend-trade-secrets-act.

Cases where an employee uses external digital storage devices and/or cloud storage services to store misappropriated trade secrets may be candidates for use of the civil seizure mechanism, especially if it is clear that the employee may not fully comply with a TRO or preliminary injunction. Regardless of the form of the misappropriated trade secret (digital, physical, or otherwise), to make civil seizure effective, trade secret owners must be prepared to quickly explain to the court what information has been stolen, who stole it, and where it is being kept. A well-developed trade secret asset management plan will greatly assist in this process.

Other Remedies

Once a court finds that misappropriation has occurred, it may grant an injunction to prevent potential future misappropriation. Notably, any such injunction cannot prevent an individual from entering into an employment relationship, and any conditions placed on employment must be based on actual evidence of threatened misappropriation and not merely on the individual's knowledge. Additionally, an injunction cannot ''conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade or business.'' This provision will be especially important in cases proceeding in California where there are strong protections against restraint from engaging in one's profession.

Following a finding of misappropriation, a court may also award damages. In ''exceptional circumstances that render an injunction inequitable,'' the court may condition future use of the trade secret on the payment of a reasonable royalty. A company may additionally be entitled to exemplary damages or attorney's fees where an employee is found to have misappropriated trade secrets and where the whistleblower notice provision has been satisfied (discussed further below).

Whistleblower Immunity and Notice Requirement

Employers must be cognizant of the notice provision within the whistleblower immunity section of the DTSA, because compliance with this provision may impact whether an employer is entitled to certain relief under the statute. The DTSA's whistleblower immunity protects employees from civil or criminal liability for a confidential disclosure of trade secrets to an attorney or government official ''solely for the purpose of reporting or investigating a suspected violation of law,'' or in a filing made under seal. To take advantage of exemplary damages and attorney's fees under the statute, employers must advise their employees of the existence of the whistleblower immunity. Companies can satisfy the notice requirement by providing notice of the immunity in an employment agreement that governs the use of trade secret information or by cross-referencing a policy document that includes a statement about the DTSA's whistleblower immunity. The DTSA defines employee to include full-time employees as well as ''any individual performing work as a contractor or consultant for an employer.'' Employers should consider revamping their confidentiality and other employment agreements to include notice of the whistleblower immunity provided for in the Act.

Conclusion

The DTSA provides a new tool to protect against and remedy trade secret misappropriation perpetrated either domestically or abroad. In addition to providing litigants direct access to federal courts when filing trade secret claims, the Act provides new mechanisms not previously available under state law, such as civil seizure, for use in stopping trade secret theft. Connectivity in the workplace is now ubiquitous and there is no shortage of cases where employees have stored misappropriated trade secrets using cloud storage devices and other external media. *See, e.g., Earthbound Corp. v. Mitek USA, Inc., No. C16-1150 RSM (W.D. Wash. Aug. 19, 2016)* (granting TRO where former employee allegedly misappropriated trade secrets using Dropbox and Google Drive); *Frisco Medical Ctr., L.L.P. v. Bledsoe*, No. 4:12-cv-37 (E.D. Tex. Nov. 30, 2015) (forensic examination of former employee's computer equipment revealed that numerous files containing trade secret information were uploaded to employee's Dropbox account and that USB storage devices were attached to computer before Dropbox was uninstalled). Given the prevalence of these cases, it's likely that a case involving trade secret theft using digital means may be the first in which the DTSA's civil seizure mechanism is employed. To be prepared to use the civil seizure mechanism, employers should have in place a comprehensive trade secret asset management plan that will help to quickly identify when a trade secret is misappropriated and by whom, so that remedial action can be taken immediately.

  DLR ISSN 0418-2693