Client Alert

May 2016

Defend Trade Secrets Act

Yesterday, President Obama signed into law the Defend Trade Secrets Act (DTSA), creating for the first time a federal civil cause of action for trade secret misappropriation. Until now, US companies that fell victim to state-sponsored espionage or light-fingered employees heading out the door to competitors had to resort to trade secret claims based in state law. Now that trade secrets have joined the ranks of other forms of intellectual property with original jurisdiction in federal district courts, plaintiffs are guaranteed the certainty of rules, standards, practices and services found in the federal judiciary, including subpoenas, discovery and witness depositions across state lines. In addition to allowing injunctions and damages previously available under state laws governing trade secret theft, the DTSA creates an *ex parte* procedure for seizing property in extraordinary circumstances to prevent disclosure of trade secrets.

Background for Law's Passage

The impetus for developing a federal civil remedy was the growing threat of trade secret theft in the United States. Although the Economic Espionage Act (EEA) allowed criminal claims of trade secret theft, it was unrealistic to expect the Department of Justice to bring charges in every trade secret case. Trade theft victims had the option of asserting state trade secret misappropriation claims, which were based on the Uniform Trade Secrets Act (UTSA). A few states, however, have not passed trade secret acts (Massachusetts, New York and North Carolina), and the states where a claim could be made present a patchwork of different local procedures and practices, lacking the ease of interstate discovery inherent to the federal system. While plaintiffs could end up in federal courts based on diversity or piggybacked onto claims of patent or copyright infringement (when not preempted), the need for greater certainty led to this legislation, which modifies the EEA to include a federal civil claim for trade secret theft.

Requirements for Trade Secret Theft Claims

The requirements for establishing a claim trade secret misappropriation under the DTSA are similar to those under the UTSA. The DTSA uses the EEA's definition of trade secrets, namely "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,[1] whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…." 18 USC § 1839(3). In order for the information to qualify as a secret, the owner must have "taken reasonable measures to keep such information secret…." *Id.* The subject of the trade secret must derive "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…." *Id.* Misappropriation is defined to be the acquisition, disclosure or use of another's trade secret that was acquired by "improper means," which includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means"

[1] The express reference to "programs and code" is significant, since at least one court of appeals has suggested that programs and code are not trade secrets as defined by the UTSA. *See United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998).

but not reverse engineering or independent derivation. § 1839(5), (6). Representative Goodlatte, chairman of the House Judiciary Committee, suggested "one could argue that even a foreign government's policies to require forced technology transfer is a form of 'misappropriation.'" Press Release, Rep. Goodlatte (April 20, 2016) (*available at* https://judiciary.house.gov/press-release/chairman-goodlatte-opening-statement-markup-trade-secrets-legislation/). The jurisdictional requirements for a federal trade secrets misappropriation claim are based on the EEA, meaning that they must relate "to a product or service used in, or intended for use in, interstate or foreign commerce." § 1836(b)(1). Plaintiffs must file suit no later than three years after the misappropriation was discovered or should have been discovered by exercising reasonable diligence. § 1836(d). Continued use of stolen trade secrets remains a single act of misappropriation. *Id.* Since the DTSA does not preempt state trade secret theft laws, a plaintiff can still choose to seek any alternative remedies that state laws might offer. *See* § 1838. Unlike with the UTSA, a plaintiff must be the owner of the trade secret at issue in the case. § 1836(b)(1). Since this requirement is not found in the UTSA or any state trade secret laws, we must wait and see what showing will be required to establish ownership of the trade secret, which itself is governed by a complex patchwork of state laws.

New *Ex Parte* Seizure Provision

Under the DTSA, victims of trade secret theft may file an *ex parte* request "in extreme circumstances" for "the seizure of property necessary to prevent the propagation or dissemination of" allegedly misappropriated trade secrets. § 1836(b)(2)(A)(i). Because one "can't unring the bell" once trade secrets are disclosed to the interested public, a federal court may order the seizure of property if the alleged thief is likely to evade, avoid or otherwise not comply with a preliminary injunction under FRCP 65. § 1836(b)(2)(A)(ii). Before a court may issue such an order, the plaintiff must also prove that (a) it will be immediately and irreparably harmed without the requested seizure, (b) the harm to the applicant of denying the application outweighs the legitimate interests of the seizure's target and substantially outweighs the harm to third parties who may be harmed by the seizure, (c) the applicant is likely to succeed in showing that the trade secret was misappropriated, (d) the seizure's target has actual possession of the trade secret and the property to be seized, (e) the seizure application describes the material to be seized and its location with reasonable certainty, (f) the seizure's target "would destroy, move, hide, or otherwise make such matter inaccessible to the court" if given notice of the lawsuit and (g) "the applicant has not publicized the requested seizure." § 1836(b)(2)(A) The seizure order, *inter alia*, must schedule a hearing within seven days of the seizure and require the applicant to post a bond sufficient to protect the seizure's target from damages resulting from a wrongful or excessive seizure. § 1836(b)(2)(B). The seizure must be led by federal law enforcement, representatives of the plaintiff-applicant may not participate in the seizure and the court may appoint a special master, bound by a nondisclosure agreement, to oversee the seizure process. § 1836(b)(2)(D)(iv), (E). At the seizure hearing, the plaintiff-applicant has the burden of proving sufficient findings of fact and conclusions of law to support the seizure order. § 1836(b)(2)(F)(ii).

Remedies for Trade Secret Misappropriation

The default remedy under the DTSA is an injunction to prevent actual or threatened misappropriation, although imposition of a reasonable royalty is available "in exceptional circumstances." § 1836(b)(3)(A). Damages may also be awarded for actual losses and unjust enrichment (without double recovery), with a reasonable royalty being available in the alternative. § 1836(b)(3)(B). Willful and malicious misappropriation can merit up to double damages, and attorney's fees are available for claims or motions to terminate made in bad faith. § 1836(b)(3)(C), (D). The DTSA prohibits issuance of an injunction that conflicts with state laws forbidding restraints on non-compete clauses for former employees. § 1836(b)(3)(A)(i)(II). It also does away with the Inevitable Discovery Doctrine, requiring evidence of threatened misappropriation, not merely the likelihood that a former employee will eventually use the trade secret while employed by a competitor. § 1836(b)(3)(A)(i)(I). Unlike the UTSA, the DTSA does not include express limits on the terms for injunctions, such as termination if and when the trade secret becomes publicly available or "the temporal advantage over good faith competitors gained by a

misappropriator," potentially opening the door for "punitive perpetual injunctions." *See* Uniform Trade Secrets Act with 1985 Amendments § 2 cmt. (1985) (*citing Elcor Chem. Cop. v. Agri-Sul, Inc.*, 494 S.W.2d 204 (Tex. Civ. App. 1973)).

Additional Provisions

Additional provisions of DTSA extend beyond protecting victims of trade secret theft. The new law grants immunity from misappropriation claims for individuals assisting government officials investigating suspected violations of the law. § 1833(b)(1). Individuals claiming that they were terminated for reporting suspected law violations may similarly disclose trade secrets to their attorneys and in court filing under seal during antiretaliation lawsuits. § 1833(b)(2). The attorney general must submit a biannual report to the Judiciary Committees of the House and Senate describing trade secret theft in the United States, the government's efforts to limit such theft and recommendations of legislative and executive branch actions that should be undertaken. DTSA § 4 (2000). Additionally, the Federal Judicial Center must develop a set of best practices for the civil seizure provisions, with recommendations for how best to seize and secure information and associated storage media. *Id.* § 6.

Conclusion

Recent developments have emphasized the need for a unified cause of action for trade secret protection. Cyber theft of corporate trade secrets continues to be a significant issue facing companies in the United States, whether from sophisticated petty criminals to state-sponsored espionage. Patent protection is increasingly becoming more difficult to obtain, given court-issued limitations on patent-eligible subject matter affecting business practices and biotechnology. Given the reality that trade secrets may be the best vehicle for maintaining critical information within a company, the Defend Trade Secrets Act represents an important advancement in protecting such valuable trade secrets, opening the federal courts to civil remedies directed to trade secret theft.

Contacts

John Gary Maynard, III
jgmaynard@hunton.com

Dr. Paul T. Nyffeler
pnyffeler@hunton.com