Feds Take Further Aim at Trade Secrets Protection with Similarities to NJ Law

Mitchell Boyarsky and Elizabeth Cowit

New Jersey Law Journal, June 27, 2016

On May 11, the Defend Trade Secrets Act of 2016 (DTSA), providing a private right of action for trade secret misappropriation, became law. The DTSA amends the Economic Espionage Act of 1996 (EEA), which authorizes criminal prosecution of trade secret theft and creates a national mechanism to combat such theft. The DTSA is intended to coexist with trade secret protections as afforded by state statutes and common law, such as those available in New Jersey. The result is an array of legal recourse for trade secret owners (TSOs) and practitioners. The DTSA took effect immediately.

Before the DTSA was enacted, state law governed civil lawsuits for trade secret theft, with 48 states, including New Jersey, adopting some form of the Uniform Trade Secret Act (UTSA). New Jersey's Trade Secrets Act (NJTSA), N.J.T.S.A. 56:15-1 et. seq.,was enacted on Jan. 5, 2012.

State law disparities resulted in inconsistent outcomes for TSOs, making it difficult for them (particularly companies with multistate operations) to comply with varying legal requirements and to pursue misappropriation claims against individuals overseas. The DTSA now creates both marked procedural advancements and hurdles subsequent to the NJTSA.

Prior Government Efforts to Deter Trade Secret Theft

The DTSA extends recent federal legislation to deter trade secret theft and provides recourse for harm. On Dec. 28, 2012, the Theft of Trade Secrets Clarification Act of 2012 (TTSCA) became law, expanding the EEA's definition of trade secrets.

The TTSCA was Congress' response to *United States v Aleynikov*, 676 F.3d 71 (2d Cir. 2012),where the Second Circuit held that, although a computer programmer breached his confidentiality agreement with his employer when he misappropriated computer code for his employer's proprietary trading system, he could not be criminally charged under the EEA. The court reasoned that, because the employer's system was used internally, was not sold

commercially, and was never intended to be licensed or sold to anyone, the system was neither "produced for" nor "placed in" interstate or foreign commerce and, therefore, not protected by the EEA.

The TTSCA broadened the EEA's definition of trade secrets to include those "related to" a product or service in, or intended for use in, interstate or foreign commerce, even when such trade secrets are not directly used in the product or service—meaning that protected trade secrets now encompass technical know-how that is not part of a product or service. Thus, the misappropriation of the type of trade secret at issue in *Aleynikov* is now illegal.

Shortly after the TTSCA's enactment, the Foreign and Economic Espionage Penalty Enhancement Act of 2012 became law on Jan. 14, 2013, increasing the maximum criminal penalties for foreign economic espionage and directing the U.S. Sentencing Commission to consider higher offenses for trade secret crimes. Public Law No. 112-269. These acts reflect a continued concern regarding trade secret theft, particularly in the computer age, wherein countless valuable trade secrets susceptible to theft reside in cyberspace.

The DTSA

Trade secrets, as defined by the DTSA, include "financial, business, scientific, technical, economic, or engineering information … 'if'… the owner has taken reasonable measures to keep such information secret and … the information derives independent economic value … from not being generally known to"… the public. 18 U.S.C. §1839(3). Typically, trade secrets include confidential formulas, techniques, client lists, marketing strategies and pricing information, which provide a competitive advantage to TSOs and often take years and significant expense to develop. Until the DTSA's enactment, a company victimized by trade secret theft (in contrast to other intellectual property harm) lacked a private federal right of action.

The DTSA applies to trade secrets related to products or services used in, or intended for use in, interstate or foreign commerce; protects misappropriations or threatened misappropriations of trade secrets (occurring after May 11, 2016); and provides a three-year limitations period. 18 U.S.C. §1836. A "misappropriation" occurs by "improper means," which involves "theft, bribery, misrepresentation, breach … of duty to maintain secrecy or espionage through electronic or other means." The DTSA, however, excludes "reverse engineering," "independent derivation"

and "any other lawful means of acquisition" from its definition of misappropriation. 18 U.S.C. §1839(6).

Courts may issue an injunction for an actual or threatened misappropriation of a trade secret, but may not enjoin an employee from entering into a new employment relationship. Although courts may impose conditions on new employment, those conditions must be based on evidence of threatened misappropriation and "not merely on information the person knows," also called "inevitable disclosure." 18 U.S.C. §1836 (b)(3)(A)(i)(I). The injunction cannot conflict with applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business. *Id*. §1836 (b)(3)(A)(i)(II).

Courts may award damages for actual loss caused by the misappropriation and/or damages for unjust enrichment or, alternatively, reasonable royalties for unauthorized trade secret use. Courts may also award attorney fees and exemplary damages (up to double actual damages) for "willful and malicious" misappropriation. Conversely, courts may award attorney fees to defendants for bad faith claims of misappropriation. *Id*. §1836 (b)(3)(D).

The DTSA authorizes ex parte seizure of property (from the party accused of misappropriation) when necessary to preserve evidence or prevent dissemination of a trade secret. To prevent abuse, a seizure order (which exceeds the protections offered by state law) exists for "extraordinary circumstances," which include: (a) instances where a TRO would be inadequate because the party subjected to it would evade, avoid or not comply with it; (b) immediate and irreparable injury would occur without the TRO; and (c) the harm to the applicant of denying the TRO outweighs the harm to the person against whom the seizure is sought and to third parties. *Id*. §1836 (b)(2).

The DTSA places strict requirements on courts issuing seizure orders. The order must be narrowly crafted to protect the trade secret, and the seizure must "minimize any interruption of the business operations of third parties" and, "to the extent possible," to "the legitimate business operations of the person accused of misappropriat[ion]." *Id*. §1836 (b)(2)(B)(ii). Security must be provided, and the court will act as a custodian to secure seized property. *Id*. §1836 (b)(2)(B)(vi) and (b)(2)(D). The court may appoint a special master to "locate and isolate all misappropriated trade secret information" and "facilitate the return of unrelated property and data to the person"

subject to the seizure. *Id*. §1836 (b)(2)(D)(iv). The court must also conduct a hearing within seven days after issuing the order. *Id*. §1836 (b)(2)(B)(v).

The DTSA grants immunity from criminal and civil liability to an individual who discloses a trade secret to a government agency or to an attorney solely to report or investigate a suspected violation of law. *Id*. §1833(b)(1), (2). Immunity also attaches if the trade secret is disclosed in a lawsuit by an individual claiming retaliation against an employer for reporting a violation of the law, provided the trade secret is filed under seal. *Id*. §1833 (b)(2).

Importantly, beginning May 11, 2016, employers must notify employees (as well as consultants and contractors) of the DTSA's immunity requirements in agreements governing the use of trade secrets or confidential information (or by reference to company policy providing notice). *Id*. §1833 (b)(3). Without such notice, the employer may not recover exemplary damages and attorney fees.

The DTSA does not preempt state law. Thus, TSOs may bring lawsuits under the DTSA and/or the NJTSA, along with certain common law claims, for misappropriations in violation of New Jersey law.

Comparison with NJTSA

The NJTSA defines misappropriation similar to the DTSA definition, with an important exception, i.e., a clause in the NJTSA definition may suggest a higher burden than that under the DTSA to show one form of misappropriation concerning disclosure or use of a trade secret without the TSO's consent. *See* N.J.T.S.A. §56:15-2. To prove such a claim, the DTSA requires that before a material change of position (i.e., receipt of some type of benefit), the person who disclosed or used the trade secret knew or had reason to know that it was a trade secret, and knowledge of it had been acquired by *accident or mistake*. 18 U.S.C. §1839(5)(B)(iii)(II) (emphasis added). The NJTSA, however, limits this type of claim by defining misappropriation to include situations wherein the party who disclosed or used the trade secret knew it was a trade secret and that knowledge of it had been acquired by "*improper means*"—not by accident or mistake. N.J.T.S.A. §56:15-2(2)(c). Such variation may or may not prove significant over time.

The NJTSA, as does the DTSA, authorizes claims for actual or threatened trade secret theft and provides for injunctive relief and damages, including actual damages and unjust enrichment.

N.J.T.S.A. §56:15-3. Both statutes permit a court to order a reasonable royalty for misappropriation. Significantly, the NJTSA does not provide for the extraordinary seizure mechanism or immunity available under the DTSA.

While both statutes authorize punitive or "exemplary" damages for willful and malicious misappropriation, the DTSA caps such damages at twice the amount of actual damages. 18 U.S.C. §1836(b)(3)(D), N.J.T.S.A. 56:15-4. Similar to the DTSA, a court under the NJTSA may award reasonable attorney fees and costs to the prevailing party—including for the defense of a bad faith claim. *Id*. §56:15-6. Both laws provide a limitations period of three years from the time the theft was or should have been discovered. *Id*. §56:15-8.

Alternate Common Law Protections Recognized By Court

In *SCS Healthcare Mktg. v. Allergan USA*, 2012 WL 6565713 (Ch. Div. Dec. 7, 2012), the plaintiff brought claims under the NJTSA and common law. The court ruled the NJTSA did not preempt the plaintiff's common law claims at least to the extent the confidential information did not rise to the level of a trade secret. Separate from this case, inevitable disclosure is recognized in New Jersey.

Next Steps

Employers should continue to identify trade secrets, safeguard their secrecy and evaluate current trade secret protection programs. Given the DTSA's notice requirement, employers must review and, where necessary, revise their agreements and restrictive covenants, applications, offer letters, handbooks and policies containing provisions for trade secret protections to include the mandatory notice (of 18 U.S.C. §1836(b)(3)) to preserve the ability to seek exemplary damages and attorney fees.