

Intellectual Property

Federal DTSA: New Weapon in the Battle to Protect Trade Secrets

Bridget E. Montgomery and Casey A. Coyle, The Legal Intelligencer

May 27, 2016

On May 11, President Obama signed the Defend Trade Secrets Act of 2016 (DTSA) into law. The legislation, an amendment to the Economic Espionage Act of 1996, grew out of the Obama administration's determination to protect U.S. corporations from increasing incidents of economic and industrial espionage by foreign competitors and governments, particularly through cyberinvasion into electronic storehouses of business information. The DTSA promises to be a benefit to all employers faced with the theft of trade secrets by departing employees.

The DTSA creates, for the first time, a federal private cause of action for theft of trade secrets—whether products, services, or electronically stored information—to be used or intended to be used in interstate commerce. Under state law causes of action, employers could prosecute employee theft of trade secrets cases in federal court only if federal diversity jurisdiction was present, or perhaps under the federal Computer Fraud and Abuse Act, which has provided limited relief. With the federal rules on corporate citizenship, employers frequently were limited to state court. Now, employers will be able to bring a claim for theft of trade secrets in federal court under the DTSA as a matter of federal question jurisdiction, thus eliminating the need to satisfy the requirements for diversity jurisdiction.

But the DTSA does more than create federal question jurisdiction for theft of trade secrets. With the added prospect of liability under the Racketeer Influenced and Corrupt Organizations Act (RICO), the inclusion of an ex parte seizure of property remedy and the establishment of whistleblower immunity, the DTSA promises to reshape the landscape of trade secrets law for decades to come.

RICO Liability

Perhaps the most compelling feature of the DTSA (and one oddly overlooked in much of the writing on this much anticipated legislation) is that it expressly adds theft of trade secrets to the list of prerequisite predicate offenses under RICO. To establish a civil RICO claim, the plaintiff must have been injured by "racketeering activity," that, in turn, requires that the conduct, among other requirements, constitute a violation of certain enumerated statutes—the "predicate acts"—set forth in Section 1961(1) of the statute.

If the conduct does not fall within the enumerated offenses set forth in Section 1961(1), it cannot serve as the indispensable predicate act for a civil RICO claim. Historically, some courts treated trade secrets theft as falling within one of RICO's enumerated predicate acts, while others did not. Thus, no matter how egregious a pattern of wrongful conduct, some courts declined to extend RICO liability to employee theft of trade secrets. The DTSA changes that and provides the promise of a consistent—and reasonable—approach to theft of trade secrets under RICO.

Now, when faced with a current or former employee's theft of trade secrets, an employer may have at its disposal all of the remedies provided under the DTSA, as well as all of the remedies available under a civil RICO claim. This is a potential game changer for employers. Why? Because a plaintiff can recover treble damages under a civil RICO claim. And because employee theft of trade secrets can now be routinely accorded the criminal status it deserves.

Seizure of Property Clause

The vast majority of state trade secrets law, including the Pennsylvania Uniform Trade Secrets Act (PUTSA), emerged as a state legislative adoption of the Uniform Trade Secrets Act (UTSA). The DTSA also is modeled after UTSA in many respects. Notably, however, the DTSA contains an express seizure remedy that does not exist under UTSA.

Under the DTSA, a court may issue an order, upon an ex parte application, providing for the seizure of property as "necessary to prevent the propagation or dissemination" of stolen trade secrets. Such property would include laptops, external hard drives, and other portable electronic devices containing stolen trade secrets. A seizure order is a significant weapon against the possibility—indeed, the likelihood—that such information will be further disseminated or used by the perpetrators in the future. Thus, the seizure order is a valuable new tool that an employer may use to mitigate the impact of an employee's theft of its trade secrets.

Issuance of a seizure order is not automatic—there are conditions to be satisfied. The complaining party must first submit an affidavit or a verified complaint, which must establish sufficiently, among other things, the likelihood that an immediate and irreparable injury will occur if the seizure is not ordered, and the person against whom seizure would be ordered has actual possession of a trade secret and the property to be seized. The complaining party must also post security sufficient to cover any damages that a person may suffer as a result of wrongful, excessive, or attempted wrongful or excessive seizure. If a seizure order is granted, the party must then present evidence at a hearing substantiating the findings of fact and conclusions of law that support the order. The hearing must take place within seven days of the issuance of the seizure order. If the party fails to meet its burden at the hearing, the seizure order is dissolved or modified appropriately.

A dissolved seizure order may prove costly. The DTSA creates a separate cause of action for damage caused by wrongful seizure, under which any person who suffers damages by reason of wrongful or excessive seizure is entitled to certain damages. Those damages include lost profits, punitive damages in instances where the seizure was sought in bad faith, and - reasonable attorney fees, subject to a limited exception. And the amount of security posted with the court does not limit in any way the damages recoverable in an action for damage caused by wrongful seizure.

In short, even though the availability of a seizure order goes a long way toward mitigating the impact of the theft of an employer's trade secrets, such an order is not without its own challenges and risks. In appropriate circumstances, however, it stands to offer significant additional protection to wronged employers.

Whistleblower Immunity

Similar to many federal statutes, the DTSA contains a provision for whistleblower immunity. Specifically, the DTSA prohibits an individual from being held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret where: (1) the disclosure is made "in confidence to a federal, state, or local government official, either directly or indirectly, or to any attorney" and "solely for the purpose of reporting or investigating a suspected violation of law" or (2) the disclosure is made "in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal."

The DTSA requires an employer to provide notice of the immunity afforded under the statute in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information." If the employer fails to supply this notice, the employer is barred from recovering exemplary damages or attorney fees under the statute, in any action against an employee to whom such notice was not provided.

While this notice requirement may prevent some employers from availing themselves of all of the remedies provided under the DTSA, an employer's failure to provide the requisite notice may prove inconsequential in most cases. This is because the DTSA does not categorically pre-empt any and all federal and state trade secret laws. Instead, the DTSA only pre-empts a federal or state trade secret law to the extent that it would make an individual criminally or civilly liable for disclosing a trade secret to a government authority for the purpose of reporting or investigating suspected illegal activity.

Consequently, absent a whistleblower scenario, an employer may pursue remedies for theft of trade secrets under both the DTSA and its state counterpart, PUTSA. Therefore, and given the similarities between the remedies available under the DTSA and PUTSA, an employer's failure to provide the notice mandated by the DTSA may have relatively minor ultimate negative consequences.

Other Remedies

With the exception of the seizure order, the remedies available under the DTSA are substantially the same as those available under the PUTSA. The DTSA provides for: (1) injunctive relief; (2) damages for actual loss caused by the misappropriation; (3) damages for any unjust enrichment caused by the misappropriation that is not addressed in computing damages for actual loss; (4) in lieu of damages by other methods, a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret; (5) double damages if the trade secret is "willfully and maliciously" misappropriated; and (6) reasonable attorney fees to the prevailing party, where the trade secret was "willfully and maliciously" misappropriated or, conversely, if the claim of misappropriation was made in bad faith.

Going Forward

With the passage of the DTSA, the time is ripe for employers to establish or reassess internal practices designed to protect against theft of trade secrets and to ensure that the new remedies available under the DTSA are preserved. Employers can start by issuing to employees the required whistleblower immunity notice.

At the same time, employers should establish periodic reviews of their internal realities, such as identifying business property of any type that constitutes a trade secret, staying abreast of risks specific to the employer's industry, evaluating data security measures, and developing the means to detect likely violators. All of these are helpful business practices that will help employers protect against an employee's theft of trade secrets. When thefts do occur, however, the DTSA positions employers to obtain prompt and effective redress in federal court. •

Bridget E. Montgomery is a member at Eckert Seamans Cherin & Mellott, in the commercial litigation group. Her experience covers complex contract, trade secrets, employment, construction, intellectual property, shareholder, and class actions disputes before state and federal courts, agencies, and arbitration panels. Casey A. Coyle is a senior associate in the commercial litigation group, who concentrates his practice on complex commercial litigation, class action, and appellate cases in federal and state courts. Coyle Montgomery
