Articles + Publications | September 13, 2019

How Safe Is That Harbor? The Impact Of The Defend Trade Secrets Act's Whistleblower Immunity Provision On A Trade Secret Owner's Ability To Protect Its Trade Secrets

Client Alert

WRITTEN BY

William M. Taylor | Callan G. Stein

Download the publication here

Imagine that your company has just commenced an internal compliance investigation in response to an allegation that the company is violating various federal laws. The next day, a longtime employee with access to the company's crucial trade secrets is seen removing duffle bags of documents. Moreover, the IT department examines his network activity and reports that he has downloaded thousands of documents onto a thumb drive.

Shortly thereafter, an attorney for the employee contacts your litigation department and states that the employee has indeed taken documents and files with the company's trade secrets. Further, the employee will not return the information because under the federal Defend Trade Secrets Act (DTSA), he is immune from liability under any federal or state trade secret laws because he has disclosed the company's trade secrets "solely for the purpose of reporting or investigating a suspected violation of the law."

Is the employee in fact immunized from liability for his acquisition and disclosure of your trade secrets? One might assume yes based on the DTSA's whistleblower immunity provision, but the answer is actually more complicated and will depend on a number of factors. As further analyzed below, the whistleblower immunity provision is actually quite narrow and should be understood as a public policy-based exception within the context of the overall scheme of state and federal laws that prohibit misappropriating and disclosing trade secrets. Indeed, the few decisions addressing the immunity provision to date have declined to find immunity at a case's early stages and have instead required the disclosing party (who seeks to rely on immunity) to establish each of the elements of the immunity through discovery, including, most notably, that the disclosure was, in fact, "solely for the purpose of reporting or investigating a suspected violation of the law."

A second crucial question is whether the DTSA's immunity provision prevents your company from taking steps to retrieve and protect the trade secrets that the employee has taken. Based on the DTSA's language, and the few cases that have analyzed the immunity provision thus far, the answer to this question is a resounding "no." Even in the context of legitimate whistleblowing activity, the law arms companies that have been the victims of trade secret theft with various tools to limit the possible harm caused by the misappropriation and to prevent further disclosure of the trade secrets. Below, we discuss these tools and certain strategies for using them that trade

secret owners should employ to ensure that their trade secrets are not revealed to the public and/or their competitors.

The DTSA's Protections for Trade Secrets

Enacted in 2016, the DTSA recognizes that trade secrets are a valuable form of intellectual property and, therefore, provides for criminal and civil penalties against those who misappropriate trade secrets.[1] In private civil actions, a company that has been the victim of a trade secret misappropriation may ask the court to enter an order (called an injunction) that prevents any actual or threatened misappropriation, requires affirmative actions to prevent harm to the trade secret, and (in exceptional circumstances) requires payment of a royalty to the trade secret owner.[2] The court may also award the trade secret owner money damages, exemplary damages and attorney fees.[3] Finally, trade secret owners may, in extraordinary circumstances, apply to a court *ex parte* (*i.e.*, without notifying the alleged perpetrator of the misappropriation) for an "order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[4]

The DTSA broadly identifies information that can qualify as a trade secret, provided that the information delivers a competitive advantage and the owner takes steps to protect it. The DTSA defines a "trade secret" 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.

(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.[5]

The DTSA punishes the "misappropriation" of trade secrets, which it defines 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

(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.

(II) Knowledge of the trade secret had been acquired by accident or mistake.[6]

In sum, the DTSA clearly describes both what secrets it protects (any nonpublic information from which a company derives competitive advantage, so long as the company takes steps to maintain the secrecy) and from what it protects those secrets (the improper theft or disclosure of that information).

The DTSA's Immunity for Whistleblowers

During the final stages of the legislative process, the drafters of the DTSA added a provision that provides immunity to individuals who misappropriate trade secrets for the purpose of whistleblowing. The purpose of including this provision was "to ensure that employers and other entities cannot bully whistleblowers or other litigants by threatening them with a lawsuit for trade secret theft."[7] As Senator Leahy explained in support of the provision, it "protects disclosures made in confidence to law enforcement or an attorney for the purpose of reporting a suspected violation of law and disclosures made in the course of a lawsuit, provided that the disclosure is made under seal."[8]

The immunity provision, titled "Immunity From Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing," is strongly worded to convey the power of the whistleblower protection being afforded. It states:

(1) **Immunity**.—An individual **shall not be held criminally or civilly liable** under any Federal or State trade secret law for the disclosure of a trade secret that—

(A) is made—

(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and

(ii) solely for the purpose of reporting or investigating a suspected violation of law; or

(B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.[9]

Moreover, an employee is expressly permitted to use trade secrets in an anti-retaliation lawsuit, provided that he or she "files any document containing the trade secret under seal; and . . . does not disclose the trade secret,

except pursuant to court order."[10]

Another notable feature of the DTSA is its notice requirement. This notice requirement arguably increases the odds of external whistleblowing activity because it requires employers to provide written notice of the immunity to employees "in any employee contract governing the use of trade secrets or other confidential information."[11] There are penalties for noncompliance with this notice requirement; an employer that fails to provide notice may not be awarded the exemplary damages or attorney fees that are available under the DTSA in an action against an employee to whom notice was not provided.[12]

Despite these strong protections for whistleblowers, the DTSA does set important limitations on the whistleblower's conduct. For instance, the DTSA's immunity provision expressly does not grant *carte blanche* permission for a person to violate other laws in securing trade secrets before disclosing them. Instead, the DTSA states that "[e]xcept as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, **such as the unlawful access of material by unauthorized means**."[13] Moreover, in the context of disclosures to government officials or an attorney, the disclosure must be "solely for the purpose of reporting or investigating a suspected violation of law."[14]

When Whistleblowing May Involve the Disclosure of Trade Secrets

As explained above, trade secrets can cover a broad array of information, with examples including business methodologies, customer information, financial information, business and marketing plans, formulas (including algorithms), computer programs, personnel information, and pricing.

Unsurprisingly, a company's trade secrets — *i.e.*, its most secret and valuable information — can also serve as supporting evidence for a whistleblower action. By definition, a whistleblower is only entitled to recovery if he or she alleges violations of law that are otherwise unknown, *i.e.*, that are based on nonpublic information. Depending on the conduct at issue, this nonpublic information may include trade secrets.

As a result of this nonpublic information requirement, the vast majority of whistleblower cases against companies are brought by former or current employees (*i.e.*, "insiders"). Whistleblowers come in many shapes and forms, and there is no single explanation for why certain employees end up bringing allegations of wrongdoing to government prosecutors. Some individuals are motivated by the promise of a financial windfall — *e.g.*, whistleblowers who disclose a company's violations of the federal False Claims Act (in what are known as *qui tam* cases) are entitled to an award of up to one-third of any governmental recovery (which in many cases can be tens of millions of dollars). Other whistleblowers bring claims because they are upset with, or distrustful of the company — *e.g.*, individuals who repeatedly raised allegations internally but were ignored or, worse, individuals who were terminated or demoted for raising complaints.

Regardless of the whistleblower's motivation, though, the moment he or she contacts an attorney or provides information to a government prosecutor, the company loses the ability to control the situation, and the chances of a government investigation and/or interference increase exponentially.

Judicial Interpretations of the DTSA's Whistleblower Provision

To date, there have been precious few judicial interpretations of the DTSA's whistleblower provision, and, thus, the state of the jurisprudence on this topic remains very much in flux. However, two federal courts on opposite sides of the country — one in Massachusetts and the other in California — have provided some brief analysis of the substance of the provision. Although neither court dissected the immunity in detail, there are nonetheless important lessons that can be gleaned from these decisions.

The federal court in Massachusetts was the first court to address this provision in *Unum Group v. Loftus*.[15] That case involved a lawsuit by a company in the business of providing financial protection benefits (Unum) against a former employee (Loftus) for stealing trade secrets. Specifically, Unum alleged that, after Loftus was interviewed by Unum's in-house counsel as part of an internal investigation into its claims practices, Loftus removed boxes of confidential company documents from the premises. These documents, Unum alleged, contained trade secrets, such as "customer and employee information, and . . . protected health information."[16]

Loftus moved to dismiss the Unum complaint on DTSA immunity grounds, claiming that he removed the documents for the purpose of reporting a violation of law by Unum. Specifically, Loftus claimed that he "handed Unum's documents over to his attorney to pursue legal action against Unum for alleged unlawful activities."[17]

The California case, *1-800 Remodel, Inc. v. Bodor*,[18] presented a similar fact pattern. That case was, once again, brought by a company (1-800 Remodel) against a former employee (Bodor) for theft of trade secrets. In this case, the company had investigated Bodor based on suspicion that she was overstating her hours. When Bodor learned of this investigation, she forwarded confidential documents to her personal email account and deleted many other files from her work computer. 1-800 Remodel terminated her and brought suit for theft of trade secrets. Bodor moved to dismiss, claiming that she was immune under the DTSA because she took the documents in order to report the company to the California Department of Consumer Affairs Contractors State License Board.

As discussed in more detail below, both of these federal courts ultimately denied the defendants' motions to dismiss and allowed the employers' suits for theft of trade secrets to proceed. In fact, to date, there has been only a single instance of a defendant succeeding even in part on a DTSA immunity claim, and that occurred in a Pennsylvania case that presented a unique and narrow set of circumstances. In *Christian v. Lannett Co.*,[19] a terminated employee (Christian) brought discrimination charges against her former employer (Lannett). The DTSA immunity arose when Lannett asserted counterclaims that Christian had stolen and disclosed trade secrets in violation of the DTSA on two occasions. The first was Christian's initial theft of 22,000 pages of confidential documents. This occurred *before* the DTSA was passed. The second was Christian's disclosure of those same documents during the discovery phase of the litigation. This disclosure took place *after* the DTSA was passed.

The court determined that the DTSA did not, as a matter of law, apply to the initial alleged theft of trade secrets that predated its enactment. That left only the second, post-enactment disclosure during discovery and within the context of the employee's discrimination lawsuit. The court ruled that the employee was immune from liability for this disclosure because it occurred within the context of a lawsuit.

How Trade Secret Owners Should Address the Whistleblower Immunity Provision

The DTSA's immunity provision has real teeth. A whistleblower will almost certainly be immune from liability under federal and state trade secrets laws if he or she meets the provision's requirements. Nonetheless, even in a

potentially valid whistleblower situation, the DTSA does not seek to destroy the trade secrets, nor to prevent the trade secret owner from taking steps to protect the secrets during the pendency of the case.

First, it is important to understand that the immunity provision seeks to preserve the confidentiality of the trade secrets, even while recognizing that limited disclosures may occur during the whistleblower investigation process. To be eligible for immunity, the whistleblower must have made the disclosure *in confidence* to law enforcement authorities or an attorney. Similarly, if the disclosure is made in a complaint or other document, the filing must be made under seal. Thus, even the immunity provision recognizes the importance of strictly limiting a disclosure to only those who "need to know" for the purpose of conducting the whistleblower investigation.

Second, the provision itself, and the manner by which it has been interpreted so far, encourage a trade secret owner to move very quickly when it learns of a misappropriation. In both *Unum* and *1-800-Remodel*, the trade secret owners got to the court first and filed civil complaints against the perpetrator employees for misappropriation. When the defendant employees asserted the immunity provision as affirmative defenses, both judges were dubious (at the pleadings stage) of whether the misappropriations were, in fact, exclusively linked to any whistleblowing activity.

This was largely because, when faced with the question of whether immunity applied, the judge in each case was constrained by the facts pled in the four corners of the complaint, *i.e.*, the facts that the *companies* chose to include. In both cases, because the complaints were carefully pled by the companies, they did not contain sufficient allegations about the whistleblowing activity to permit the judge to rule that the defendants had met all of the necessary elements for immunity to apply. In contrast, the employee in *Lannett* got to the court before the company, filed her own claims for various violations of federal law, and succeeded in her immunity defense to the employer's misappropriation counterclaim.

Third, the whistleblower immunity provision does not prevent a trade secret owner from using certain tools at its disposal, including requesting court orders/injunctions and seeking *ex parte* seizure of the trade secrets. In *Unum*, for instance, the court entered an order requiring the employee to take several steps to protect the secrets during the pendency of the case, including delivering to the court all documents he had taken, destroying all copies of all documents he had taken, and providing an affidavit stating the circumstances under which the employee had provided documents to any third party. Notably, the court ordered this relief despite knowing that the defendant may have a future need for the documents to prove his own case. The court noted that, in such an event, the defendant could seek the documents in discovery.

Fourth, the immunity provision protects a whistleblower from liability flowing from *disclosure* of trade secrets (provided that the disclosure complies with the statute), but does not protect the whistleblower from liability that may flow from the method by which he or she *acquired* the trade secrets. The statute explicitly recognizes this disclosure/acquisition dichotomy. The immunity provision states that "[e]xcept as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means."[20]

While this subsection has not yet been the subject of litigation, both *Unum* and *1-800-Remodel* suggest that defendants may be liable for their acts in illegally acquiring trade secrets. In *Unum*, the court found that the company was likely to succeed on the merits of its conversion claim based on the employee's taking of the

documents without authorization and for refusing to return those documents. Similarly, in *1-800-Remodel*, the company's claim under the Computer Fraud and Abuse Act (CFAA) survived the employee's motion to dismiss where the employee took a laptop without authorization and forwarded confidential and proprietary information to her personal email address. The court also questioned the applicability of the DTSA immunity to the CFAA claim because the employee did "not establish that the CFAA is a 'trade secret law' that is subject to [the DTSA immunity provision]."[21]

Fifth and finally, a trade secret owner should be prepared to aggressively test the purported whistleblower's contention that he or she meets each and every one of the immunity provision's elements. On its face, the provision will not apply unless (1) liability against the individual is sought under a federal or state *"trade secret law"*; (2) the individual disclosed the trade secret *in confidence*; (3) to a government official or an attorney; (4) for the *sole* purpose of making a report; (5) based on the individual's suspicion that the law was broken. This will not be an easy task for an individual claiming immunity, especially at the motion to dismiss stage, where the decision is bound by the allegations the trade secret owner asserts in the complaint (as discussed above).

For example, on the basis of the four corners of the complaint, individuals seeking immunity will have a difficult time establishing that the disclosure of trade secrets was "solely for the purpose of reporting or investigating a suspected violation of the law." In *Unum*, the court rejected the defendant's immunity argument in part because, based on the record (*i.e.*, the complaint filed by Unum), it was not clear "whether [Loftus] used, is using, or plans to use, those documents for any purpose other than investigating a potential violation of law."[22] Moreover, the *Unum* court likewise noted that Loftus had not filed a lawsuit against his employer based on the trade secrets at issue, and there was nothing reflecting the importance and contents of the documents he had taken.

The court's analysis in *1-800 Remodel* followed this same line of reasoning, but expanded it to other necessary elements for immunity as well. In rejecting the employee's immunity claim, the court noted that the record (which, again, was composed only of the complaint drafted by the trade secret owner) did not "reveal the precise nature of the complaints Defendant threatened to — and later did — file . . . or whether the complaints she did file were made 'in confidence.'"[23]

Conclusion

The DTSA's immunity provision, including the notice requirement, may ultimately prove to both increase the likelihood of whistleblowing activity and embolden would-be whistleblowers through its grant of immunity. While trade secret owners must, of course, address the ramifications of the whistleblower activity, they must not lose sight of the fact that trade secrets are, by definition, a competitive advantage that can easily be lost through disclosure to the public and/or competitors. And trade secret owners should *not* be scared off from pursuing their rights as vigorously as possible by the DTSA's immunity provision. In fact, the DTSA and the immunity provision make it even more critical than ever before for trade secret owners to act quickly and decisively to prevent their trade secrets from unnecessarily being held hostage, even during the whistleblower process.

Endnotes

[1] 18 U.S.C. §§ 1832, 1836.

[2] 18 U.S.C. § 1836(b)(3)(A).

[3] 18 U.S.C. § 1836(b)(3)(B) – (D).

[4] 18 U.S.C. § 1836(b)(2)(A)(i).

[5] 18 U.S.C. § 1839(3).

[6] 18 U.S.C. § 1839(5).

[7] P. Menell, The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History, 1 Bus. Entrepreneurship & Tax. L. Rev. 398 (2017).

[8] 162 CONG. REC. S1636-37 (daily ed. Apr. 4, 2016).

[9] 18 U.S.C. § 1833 (emphasis added).

[10] 18 U.S.C. § 1833(b)(2).

[11] 18 U.S.C. § 1833(b)(3).

[12] 18 U.S.C. § 1833(b)(3)(C).

[13] 18 U.S.C. § 1833(b)(5) (emphasis added).

[14] 18 U.S.C. § 1833(b)(1)(A)(ii).

[15] 220 F. Supp. 3d 143 (D. Mass. 2016).

[16] *Id.* at 146-147.

[17] *Id.* at 147.

[18] 2018 U.S. Dist. LEXIS 2250000 (C.D. Cal. 2018).

[19] 2018 U.S. Dist. LEXIS 52793 (E.D. Pa. 2018).

[20] 18 U.S.C. § 1833(b)(5).

[21] *1-800 Remodel*, 2018 U.S. Dist. LEXIS 2250000, at *18 n.9.

[22] *Unum*, 220 F. Supp. 3d at 147.

[23] *1-800 Remodel*, 2018 U.S. Dist. LEXIS 2250000, at *17.

William Taylor is a partner in the firm's Trial and Dispute Resolution Practice Group, a seasoned and trial-ready team of advocates who help clients analyze and solve their most emergent and complex problems through negotiation, arbitration and litigation. Callan Stein is a partner in the Health Sciences Department, a team of 110 attorneys who collaborate across disciplines to solve complex legal challenges confronting clients throughout the health sciences spectrum.

RELATED INDUSTRIES + PRACTICES

- False Claims Act + Other Whistleblower Actions
- Noncompete + Trade Secrets
- White Collar Litigation + Investigations