The trade secret whistleblower

By R. Mark Halligan, Esq., FisherBroyles LLP

JANUARY 16, 2024

What is whistleblowing?

Whistleblowing is the lawful disclosure of information that the discloser (the "whistleblower") reasonably believes evidences wrongdoing to an authorized recipient.

Section 18 USC 1833 of the Defend Trade Secrets Act (DTSA) grants whistleblower "immunity" from liability for the confidential disclosure of a trade secret to the government or in a court filing under seal.

The DTSA provides that 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 is made in confidence to a Federal, State or local government official, either directly or indirectly, or to an attorney; and solely to report or investigate a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other administrative proceeding, if such filing is made under seal.

Section 18 USC 1833 of the Defend Trade Secrets Act grants whistleblower "immunity" from liability for the confidential disclosure of a trade secret to the government or in a court filing under seal.

There is also a separate provision in Section 18 USC 1833 that addresses the use of trade secret information in an anti-retaliation lawsuit. The DTSA provides that an individual who sues for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the information in the court or administrative proceedings, if the individual files any document containing the trade secret under seal; and does not disclose the trade secret, except under court order.

The legislative intent for these two provisions was to protect legitimate whistleblower activities for obtaining legal advice and making disclosures to appropriate authorities about suspected unlawful activities. The immunity provisions in 18 USC 1833 are strictly limited to trade secret disclosure issues designed to protect the secrecy of the alleged trade secret information.

There are trade secret identification issues in play. The evaluation whether alleged confidential information constitutes a trade secret requires consideration of the Restatement of Torts six-factor test:

Factor 1: The extent to which information is known outside the company (the more extensively the information is known outside the company, the less likely that it is a protectable trade secret).

Factor 2: The extent to which the information is known by employees and others involved in the company (the greater the number of employees who know the information, the less likely that it is a protectable trade secret).

Factor 3: The extent of measures taken by the company to guard the secrecy of the information (the greater the security measures, the more likely that it is a protectable trade secret).

Factor 4: The value of the information to the company and competitors (the greater the value of the information to the company and its competitors, the more likely that it is a protectable trade secret).

Factor 5: The amount of time, effort and money expended by the company in developing the information (the more time, effort and money expended in developing the information, the more likely that it is a protectable trade secret).

Factor 6: The ease of difficulty with which the information could be properly acquired or duplicated by others (the easier it is to duplicate the information, the less likely that it is a protectable trade secret).

The putative whistleblower cannot download thousands of files onto a thumb drive and then claim whistleblower immunity for the entire thumb drive. The DTSA immunity is strictly limited to trade secrets. Asserting the whistleblower immunity defense (with no segregation of the trade secrets) puts the putative whistleblower at risk of contractual violations of non-disclosure agreements and civil causes of action for conversion and theft.

Another critical issue in a whistleblower analysis relates to the acquisition of the trade secret. How did the putative whistleblower obtain access to the trade secret information? If the evidence establishes that there was a wrongful acquisition of the trade secret information, then the whistleblower immunity defense disappears, and the putative whistleblower now becomes a trade secret misappropriator.

The DTSA sets forth the following "rule of construction" in a whistleblower case: "Nothing in 18 USC 1833 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." In short, Section 18 USC 1833 is not a license to steal.

A whistleblower immunity defense is an affirmative defense. The putative whistleblower has the burden of proof to establish whistleblower immunity under 18 USC 1833 and failing to do so will likely result in a finding of trade secret misappropriation. This is a fact-intensive analysis that cannot be resolved at the pleading stage.

If the evidence establishes that there was a wrongful acquisition of the trade secret information, then the whistleblower immunity defense disappears, and the putative whistleblower now becomes a trade secret misappropriator.

Allowing the use of trade secret information in an anti-retaliation lawsuit is designed to protect an individual who sues for retaliation by an employer for reporting a suspected violation of law; the individual may disclose the trade secret to his or her attorney and use the trade secret information in the court proceeding if the trade secret information is filed under seal and the trade secret is otherwise not disclosed except under court order. Once again, trade secret identification issues require the Restatement of Torts six-factor test to ferret out the "trade secrets" at issue. The same stakes apply.

If the plaintiff can prove the existence of trade secret information used solely to litigate the anti-retaliation lawsuit, then the disclosure of the trade secret information under seal or under court order will not be actionable. But if the plaintiff fails to prove the anti-retaliation lawsuit, the plaintiff will be exposed to breach of nondisclosure agreements and trade secret misappropriation claims.

The DTSA requires the employer to provide notice of whistleblower immunity to the employee in all contracts or agreements with the employee. The DTSA expands the definition of an employee to include individuals performing work as a contractor or consultant of the employer. An employer shall be considered in compliance if there is a whistleblower policy with cross-reference to a policy document that sets forth the employer's reporting policy for a suspected violation of law. If the employer does not comply with the notice requirement, the employer cannot be awarded exemplary damages or attorney fees in a trade secret misappropriation lawsuit.

The assertion of a whistleblower defense in a trade secret misappropriation lawsuit or in an anti-retaliation lawsuit that involves trade secrets is a difficult task that poses high risks. Failing to establish the existence of trade secrets can destroy these DTSA protections and transform the putative whistleblower and the anti-retaliation plaintiff into trade secret thieves.

R. Mark Halligan is a regular contributing columnist on trade secrets law for Reuters Legal News and Westlaw Today.

About the author

R. Mark Halligan is a partner at **FisherBroyles LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He teaches Advanced Trade Secrets Law in the LLM program at University of Illinois Chicago School of Law and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on January 16, 2024.