WINSTON & STRAWN LLP

BLOG

Federal Court Rules That Companies Must Adequately Protect Their Information to Claim Theft of Trade Secrets

MARCH 25, 2019

On March 4, 2019, a judge in the Northern District of Illinois denied a Motion for a Preliminary Injunction in a federal Defend Trade Secrets Act (DTSA) case, finding, among other things, that Plaintiff Camel Grinding Wheels (CGW) failed to adequately protect its files containing pricing, customer, and supplier information and was therefore unable to show that the information qualified as a "trade secret." Specifically, the Judge held that CGW did not "employ data security measures reasonably consistent with its claim that the information at issue was valuable," particularly because it failed to show that it treated the information at issue with any special or different protections than other files at the company. *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 2019 WL 10443322, at *10 (N.D. Ill. March 4, 2019). In doing so, the Court sent a clear message that companies must employ sufficient protective measures if they want to avail themselves to the protections of federal trade secret law.

To bring a successful civil claim under the DTSA, the plaintiff must show that the alleged trade secret is "sufficiently secret to impart economic value because of its relative secrecy." Additionally, the plaintiff must make "reasonable efforts to maintain the secrecy of the information." *Id.* at *6 (internal citation omitted); *see also* 18 U.S.C. § 1839(3). In this case, the Court found that CGW did not take enough "affirmative measures to prevent others from using the information" that it was claiming was a trade secret. *Abrasic 90 Inc.*, 2019 WL 10443322, at *10. Specifically, the Court pointed out that CGW did not: (1) require its officers or employees to sign non-disclosure agreements (except its President, for a brief period of time), (2) instruct employees that the information at issue was confidential, (3) require password protection or encryption for the files, (4) include a "confidential" or "proprietary" label on the documents, (5) only allow "need-to-know" employees to access the information, or (6) ask employees, upon their exit from the company, if they possessed any of the information at issue or instructed them to "return or delete such information." *Id.* at *9. When taken together, the Court found an "almost total failure to adopt even fundamental and routine safeguards for the information at issue." *Id.* at *7. The Court further explained that "[p]erhaps the most telling evidence" was that CGW "took no measures to protect [the purported trade secret information] that were in any way different (much less more exacting) than the steps that it took to protect information that was indisputably not a trade secret." *Id.* at *10.

Notably, the Court acknowledged that Defendant-competitor Weldcote probably used the information at issue, but CGW's failure to implement basic security features was one of several reasons preventing it from successfully asserting a claim under DTSA. In denying the Motion, the Court also pointed to CGW's "failure to establish that Weldcote's access to the information at issue is likely to cause CGW to suffer irreparable harm." *Id.* at *11.

TIP: It is important for companies to implement sufficient protections, such as nondisclosure agreements, password encrypted files, and limited access lists, to ensure that their valuable documents and ideas can be considered "trade secrets"—and thus qualify for certain legal protections—in future litigation.

2 Min Read

Author

Steven Grimes

Related Locations

Chicago

Related Topics

Trade Secrets

Workplace Privacy

Data Breach

Related Capabilities

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Related Regions

North America

Related Professionals

Steven Grimes

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.