WINSTON & STRAWN LLP

ARTICLE

‘Reasonable Measures’ For Protecting Trade Secrets: A Primer

FEBRUARY 27, 2019

This article originally appeared in Law360. *Reprinted with permission. Any opinions in this article are not those of Winston & Strawn or its clients; the opinions in this article are the authors’ opinions only.*

In the past year, numerous companies across industries—including a fund administrator, software provider, boat maker and a provider of surgical training programs—have walked into a courtroom as plaintiffs, believing (and potentially even able to prove) that their valuable corporate secrets had been stolen, only to have their cases dismissed based on a finding that the allegedly stolen information did not constitute a “trade secret” because they failed to take sufficient measures to protect the information.

And, these victims are not alone. Alarmingly, an analysis we conducted of cases filed from 2009 through 2018 showed that courts dismissed claims in 11 percent of disputed trade secret cases because the plaintiff-company failed to take “reasonable measures” to protect the stolen information, as is required to meet the definition of a “trade secret.”

To help companies avoid this painfully sobering outcome, this article offers practical guidance regarding what the undefined “reasonable measures” requirement might mean under U.S. trade secret laws.

Reasonable Measures Are Required, but Not Defined

Trade secrets enjoy significant legal protections, including under the federal Defend Trade Secrets Act (18 U.S.C. § 1836), the U.S. Uniform Trade Secrets Act, as enacted by the various states, and the EU Trade Secrets Directive (EU 2016/943). Under the Economic Espionage Act (18 U.S.C. § 1833), it is also a federal crime in the United States to steal a company’s trade secrets.

In general, to constitute a trade secret under these various laws (which each have their own nuances), the information must (1) have economic value; (2) because it is not generally known; and (3) the owner has taken reasonable measures to keep the information a secret. Unfortunately, however, there is no clear standard for what types of reasonable measures a company must take to meet this last element.

Moreover, because Congress only passed the federal Defend Trade Secrets Act in 2016, and countries in Europe were only required to implement the EU directive by June 2018, the law surrounding the meaning of this requirement is still being developed and evolving, leaving companies trying to satisfy a nebulous legal standard which, if not met, can leave their valuable assets unprotected.

Statistics compiled by Lex Machina regarding U.S. trade secret cases from 2009 to the fall of 2018 show that, while a large number of cases result in consent judgments, defendants have significant success prevailing in *contested cases*, with defendants prevailing in 54 percent of the contested cases from 2016 to the fall of 2018. Alarmingly, defendants are winning many of these cases, not because the plaintiff failed to plead or prove theft, but because the plaintiff-victim failed to demonstrate that the allegedly stolen information met the definition of a trade secret.

In many of those cases, courts have found that the allegedly stolen information at issue did not constitute a "trade secret" because the plaintiff failed to sufficiently identify the trade secret, failed to protect the trade secret, or had publicly disclosed the purported trade secret. Particularly troubling is the fact that there was a specific finding that the plaintiff had not taken sufficient measures to keep the information a secret in 11 percent of the contested trade secret cases during that period.

This means that these plaintiffs could not obtain protection under the trade secret laws—regardless of whether theft occurred and regardless of how valuable the information allegedly stolen was—because of their own failure to take sufficient steps to protect their information.

These statistics, which should serve as a wake-up call to all companies, probably underestimate how many companies find themselves unable to seek remedies under the trade secret laws after theft occurs because many such victims have opted not to pursue litigation at all or tried to seek remedies through other channels. The takeaway is that companies need to be proactive now—*before* any theft occurs—by taking protective steps which will maximize the potential legal remedies available if theft does occur (many of which will also likely minimize the chance that theft occurs).

What Are Reasonable Measures?

So, what measures are "reasonable" enough to earn trade secret protection? There are no bright-line rules when it comes to whether particular measures are "reasonable," as it will always be a fact-specific inquiry based on a particular company's circumstances.

That said, we can learn from courts who have addressed this issue to provide a framework for companies as they strive to protect their assets. To that end, we analyzed all of the cases from 2009 through the end of 2018 in which, a court found that the plaintiff had not taken reasonable measures to protect the purported trade secret. Below is a summary of some guidance that can be gleaned from those decisions.

Little or No Protections Are—Not Surprisingly—Insufficient

In cases where plaintiff-companies could not point to specific protective steps they had taken to protect their trade secrets—not surprisingly—defendants prevailed, via a motion to dismiss, summary judgment or at trial.[1]

What is somewhat surprising, however, is that these companies had spent the money, time, reputational impact and capital, to assert trade secret claims without understanding whether they had taken specific enough protective measures to qualify the stolen information as a trade secret. What this may indicate is that many companies (and their counsel) have not robustly analyzed this element, and instead improperly assumed that the value of the information at issue would make it apparent to a court that the information constituted a "trade secret."

But, that is not the law. Rather, a company needs to be able to articulate, with specificity, the measures it took to protect the allegedly stolen information if it hopes to overcome the threshold challenges to claims over that theft.

Protective Steps Beyond Normal Business Practices May Be Required

Protective measures that are applied equally to *all* of a company's information may not be sufficient. Some courts have indicated that they want to see a company go above and beyond normal business practices to protect their trade secrets.[2] For example, a court in the Northern District of Illinois recently granted a motion to dismiss after finding that the plaintiff had done "nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information."[3]

The court found it problematic that there was no allegation that the plaintiff treated the alleged trade secret as "any more confidential than all of [plaintiff's] internal information."[4] In other words, courts may look to see a company stratify or differentiate between how it treats data, based on how important or valuable that information is to the company. This is also a crucial step in setting up a company's trade secret management program, as this prioritization helps focus a company's resources and attention.

A Confidentiality Agreement Helps, but May Not Suffice

Companies may find false comfort in the fact that they utilize nondisclosure or confidentiality agreements. While such agreements (if well-drafted and enforceable) may provide a contractual remedy if trade secrets are stolen, such agreements—alone—are typically insufficient to meet the "reasonable measures" requirement.[5]

In fact, some courts have specifically stated that such agreements—without more—are not enough to meet the requirement.[6] On the other hand, many courts have pointed to the lack of a confidentiality agreement when finding that a company did not take sufficient protective measures.[7] The clear takeaway here is that courts view confidentiality agreements as a solid protective measure as part of a larger protection strategy, but not sufficient in and of themselves.

Failing to Limit Access for Departing Employees May Be Deemed Unreasonable

The time when an employee leaves a company is a high-risk moment for trade secret theft. Perhaps believing that companies should recognize this, courts have noted a company's failure to cut off an employee's access to company data in support of finding that the company did not take reasonable measures.[8]

For example, the U.S. Court of Appeals for the Eleventh Circuit recently upheld a finding that the plaintiff had not taken reasonable measures because, among other things, it never asked the defendant to delete information from his personal devices after he ceased working for the plaintiff.[9] A district court in North Carolina similarly granted summary judgment in favor of the defendant in part because the plaintiff allowed each employee to take certain information with him when he left.[10]

To avoid these same fates, companies should assess their protocols for limiting or terminating access to valuable data after an employee submits his/her resignation notice as well as their internal processes for ensuring the return or destruction of company data when an employee departs.

The Recipient of Trade Secrets Must Understand Their Confidential Nature

In the cases we reviewed, many courts considered whether the purported trade secret was marked as a "trade secret" or as "confidential" when determining whether it deserved trade secret status.[11] Additionally, when

documents were not marked as confidential, some courts found that this lack of designation did not put the defendant on sufficient notice that he was obligated to keep the document confidential.[12] Thus, a lack of marking cut against plaintiffs in many cases.

On the flip side of the coin, however, confidentiality-marking policies can create real risks. A court in the Northern District of Illinois recently summarily dismissed a federal trade secret claim because the plaintiff had a policy requiring all confidential and trade secret information to be labeled as such, yet the stolen information was not labeled.[13] The court held that a reasonable jury could conclude that the defendant did not have a duty to maintain the secrecy of that information.

The issue of marking, or not marking, information is tricky, as often the practical realities of the workplace run counter to the lofty ideals of company policies and procedures. As such companies need to thoughtfully consider practical realities when developing and deploying their policies to seek to balance the requirement that employees must be sufficiently on notice of the confidentiality of the information in question, with the risk that employees may not always mark each and every document.

One Size Does Not Fit All

Because companies only need to take "reasonable" measures, those measures will differ between companies and, perhaps even between divisions within a company. In fact, a court in the Northern District of Illinois recently explained that "reasonable steps for a two or three person shop may be different from reasonable steps for a larger company."[14]

Importantly, apart from just employing a tailored protection program, companies should be able to "show their work" to explain why and how the program was designed relative to the company's size, circumstances, technological capabilities and the nature of its trade secrets.

Conclusion

The data shows that many trade secret cases were won or lost long before even being filed based on what the victim-company did (or did not do) long before the theft occurred. Because trade secret litigation is likely going to continue to increase, and trade secret theft is becoming an unfortunate reality that most companies will experience at some point, both in-house and external counsel need to help companies proactively — and thoughtfully — implement protective measures *now*, before theft occurs.

To best assist companies with this nuanced task, counsel will need to, among other things, benchmark against peer programs and understand the industry norms, monitor the evolving jurisprudence regarding what types of "reasonable measures" companies must take, and manage trade secret programs as part of a fulsome risk management and continuous improvement process similar to other enterprise risks within the organization.

---

[1] See, e.g., Solid Wood Cabinet Co. v. Partners Home Supply, No. 13-cv-3598, 2015 WL 1208182 (E.D. Pa. March 13, 2015) (granting summary judgment in favor of defendants finding no evidence of protective steps); International Mezzo Technologies Inc. v. Frontline Aerospace Inc., no. 3:10-cv-397, at *18 (M.D. La. Sept. 25, 2014) ("Although [the report at issue] was marked as proprietary and confidential, the plaintiff did not introduce evidence to demonstrate its affirmative efforts to maintain the secrecy of the information contained in the report."); SortiumUSA LLC v. Hunger, No. 3:11-cv-1656-M, 2013 WL 11730655, at *23 (N.D. Tex. March 31, 2013) (granting a motion to dismiss based on plaintiff's failure to mark the information as confidential, require the defendant to execute a confidentiality agreement, and "its failure to plead any other steps to protect the secrecy").

[2] See, e.g. Dryco LLC v. ABM Indus. Inc. , No. 07-cv-0069, 2009 WL 3401168 (N.D. Ill. Oct. 16, 2009) (finding insufficient plaintiff's contention that specific protective measures were not required when it was custom in the industry to keep the information confidential).

[3] Opus Fund Servs. (USA) LLC v. Theorem Fund Servs. LLC , No. 17-cv-923, 2018 WL 1156246, at *5 (N.D. Ill. March 5, 2018).

[4] Id. at *6.

[5] See, e.g., Coynes (granting summary judgment for the defendant when the plaintiff failed to show any steps to maintain confidentiality beyond having the defendant sign a non-disclosure agreement).

[6] See, e.g., Opus at *3 ("While 'an agreement restricting the use of information may be considered a reasonable step to maintain secrecy of a trade secret,' such an agreement, without more, is not enough."); Bison Advisors LLC v. Kessler, No. CV 14-3121 (DSD/SER), 2016 WL 4361517, at *4 (D. Minn. Aug. 12, 2016). ("The law is clear that the mere existence of a confidentiality agreement is insufficient to establish that the covered information is a trade secret.").

[7] See, e.g., Hill Holiday Connors Cosmopulos Inc. v. Greenfield, No. 6:08-cv-03980-GRA, 2010 WL 11530748 (D.S.C. April 8, 2010), Deegan v. Strategic Azimuth LLC, 768 F. Supp. 2d 107 (D.D.C. 2011), Bumper Man Inc. v. Smit, No. 3:15-cv-02434-BF, 2016 WL 9251782, at *1 (N.D. Tex. Sept. 12, 2016), rev'd in part, No. 3:15-cv-02434-BF, 2017 WL 78508 (N.D. Tex. Jan. 5, 2017), Cardiovascular Support v. SpecialtyCare Inc., No. 3:13-cv-1171, 2015 WL 687242, at *7 (M.D. Tenn. Feb. 18, 2015), aff'd sub nom. Cardiovascular Support Perfusion Reliance Network, LLC v. SpecialtyCare, Inc., 629 F. App'x 673 (6th Cir. 2015), Warehouse Sols. Inc. v. Integrated Logistics LLC, No. 1:11-cv-02061-RLV, 2014 WL 12647878 (N.D. Ga. July 7, 2014), aff'd, 610 F. App'x 881 (11th Cir. 2015).

[8] See, e.g., Orthofix Inc. v. Hunter, 55 F. Supp. 3d 1005, 1013 (N.D. Ohio 2014), rev'd on other grounds and remanded, 630 F. App'x 566 (6th Cir. 2015) (noting that "when [defendant] left the company, [plaintiff] did not engage in meaningful efforts to seek the return of any trade secret information defendant might possess"); FormFactor Inc. v. Micro-Probe Inc., No. 10-cv-3095 PJH, at *11 (N.D. Cal. June 7, 2012) (noting that the plaintiff allowed the defendant to store business information on personal devices and "did not request that defendant returned company data when leaving company").

[9] See Yellowfin Yachts Inc. v. Barker Boatworks LLC, 898 F.3d 1279, 1299 (11th Cir. 2018).

[10] See Capitol Comm'n Inc. v. Capitol Ministries, 2013 WL 5493013, at *3 (E.D.N.C. Oct. 2, 2013).

[11] See, e.g., OTR Wheel Engineering Inc. v. West Worldwide Services Inc., No. CV-14-085-LRS (E.D.Wash. Nov. 30, 2015) ("There was no 'Confidential' designation on the single document produced by Plaintiff regarding the alleged trade secret."); SortiumUSA at *22 (explaining that the drawings at issue did "not bear any restrictive warning as to their alleged confidentiality or instructions to the persons working on them to safeguard their alleged secrecy"); Convolve Inc. v. Compaq Computer Corp., 527 F. App'x 910 (Fed. Cir. 2013) (finding that the information lost any "trade secret status" when it was disclosed without markings required under the non-disclosure agreement).

[12] See, e.g., Orthofix at 1012 (explaining that no one explained to the defendant "what information was deemed 'confidential' under the employment agreement" or that the specific information at issue was confidential); McIntyre v. BP Expl. & Prod. Inc., No. 3:13-cv-149, 2015 WL 999092, at *4 (D. Alaska March 5, 2015), aff'd, 697 F. App'x 546 (9th Cir. 2017) ("it does not allow for the proprietor of an alleged trade secret to unilaterally create a confidential relationship without the knowledge or consent of the party to whom the secret is disclosed").

[13] See Call One Inc. v. Anzine, 2018 WL 2735089 at *9 (N.D. IL. 2018).

[14] Puroon Inc. v. Midwest Photographic Res. Ctr. Inc., No. 16-cv-7811, 2018 WL 5776334, at *7 (N.D. Ill. Nov. 2, 2018).

10+ Min Read

Related Locations

Chicago

Related Topics

Law360

Trade Secrets

Privacy and Data Security

Related Capabilities

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Compliance Programs

Related Regions

North America

Related Professionals

Steven Grimes