WINSTON & STRAWN LLP

ARTICLE

To Mark Or Not To Mark: Mitigating Trade Secret Theft Risk

AUGUST 22, 2019

This article was originally published 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 author's opinions only.

With the federal Defend Trade Secret Act now being over 2 years old, Lex Machina Inc.'s finding that trade secret cases have increased 30% since 2016, and trade secret cases being highlighted in the news across industries, from the recent verdict against technology company Huawei Technologies Co. Ltd. to a startup company obtaining a $91 million verdict against L'Oreal USA Inc., companies need to make sure they are best positioned to minimize the chance of trade secret theft occurring and to maximize their ability to seek legal remedies if theft occurs.

One issue that can impact both of these imperatives and that warrants a hard look by companies is how and whether trade secrets should be marked as such.

Practical realities, and evolving trade secret law, are calling into question a long-standard approach proscribed, if not followed, by many (if not most) companies: requiring employees to mark all confidential and/or trade secret documents as such.

Contrary to the instinct of many lawyers (both in-house and outside counsel), the best practice for a company — at least when it comes to protecting its trade secrets — may be to not have strict policies requiring marking of each and every confidential and/or trade secret document as such. To be clear, we are not saying that confidentiality marking practices and policies are without value (they can be very valuable, if well drafted), nor are we advocating that all companies should cease having a confidentiality marking policy.

But, the waters are actually muddier than many lawyers probably realize when it comes to whether and how to utilize confidentiality marking policies, particularly when it comes to protecting corporate trade secrets. This article will wade through these murky waters and attempt to provide some clarity as to how companies should be thinking about and developing their confidentiality marking policies.

Marking documents as confidential can help prevent theft or misuse.

Marking documents as confidential can potentially stop trade secret theft or misuse before it occurs by providing notice to users regarding the sensitive nature of the information included within the documents. Simply marking

documents as confidential can provide a well-timed nudge to employees, agents, and others with access to sensitive information to proceed with caution and serve as a reminder of their obligations to safeguard that particular information.

When an employee sees that a document has been marked as confidential, that employee may be more likely to exercise care when disseminating that information — both internally and especially to third parties. Similarly, marking documents as confidential can be an important part of shaping and creating a corporate culture that encourages and demands careful conduct and conscientious engagement in the workplace.

Marking documents as confidential can help win a trade secret theft claim.

To constitute a trade secret under the Defend Trade Secrets Act and the Uniform Trade Secrets Act (which has been adopted in some form by 49 states), a trade secret owner must have taken reasonable measures to protect the information. Many courts have cited the existence of a confidentiality marking policy or the presence of confidentiality markings on a document as a factor supporting a finding that reasonable measures were taken.

Many courts have also found that such markings put an alleged thief on notice that the thief had an obligation to protect and not take or disseminate the information, which can help support a claim that the thief knew what he or she was doing was wrong. Accordingly, the implementation of a well-tailored confidentiality marking policy, if followed, is one way to bolster a trade secret claim if theft occurs.

But, requiring marking may prevent trade secret theft claims for unmarked documents.

As helpful as a confidentiality marking policy can be, it can also create real risks. In recent cases, courts have looked unfavorably upon trade secret claims where the plaintiff had a policy requiring confidentiality marking — yet the stolen documents in question were not marked.[1]

For example, in one case in the U.S. District Court for the Northern District of Illinois, the court granted summary judgment in favor of the defendant on the question of misappropriation because the information at issue was not marked, even though the plaintiff's policies required employees to label all confidential information and trade secrets as confidential/trade secrets.[2]

Thus, if a policy requires marking and the stolen document was not marked, a court may determine that the defendant had no duty to maintain secrecy of that information — a finding that can wholly undermine a victim's trade secret claim. This risk is particularly troubling given the day-to-day realities of requiring employees to consistently and correctly mark all confidential and/or trade secret documents appropriately. In setting these policies, companies must take into account the practical realities of whether the confidentiality marking policies will actually be followed and the real-world consequences that can result from lofty corporate marking policies that are not followed.

And, a company can take reasonable measures without requiring marking.

Importantly, a court can still find that a trade secret owner took sufficient reasonable measures to protect its information even if it did not have a marking policy or the document at issue was not marked. The question of "reasonable measures" will be decided on a case-by-case basis.

A district court in Alabama, for example, denied a motion to dismiss theft of trade secret claims after finding that, even though the purported trade secrets were not marked, the plaintiff had taken reasonable measures to protect the assets at issue, including containment on a password-protected server and discussion with the defendant employee about the need to keep the information confidential.[3]

On the flip side, even some documents that are marked as confidential have not been found to be protected as trade secrets because other actions taken by the purported owner did not suggest reasonable measures. For example, one court held that documents marked as confidential — but disclosed to third parties without a confidentiality or nondisclosure agreement in place — were not protected.[4]

Thus, while a confidentiality marking policy can be a powerful tool when properly used, it is neither independently sufficient nor necessary to protect confidential company information.

Conclusion

There is no one-size-fits-all approach to marking. Because the question of whether information qualifies as a trade secret — in particular, whether reasonable protective measures have been taken — is a very fact-intensive inquiry, companies must proceed thoughtfully in making decisions about how to approach marking. One possible approach is to include language in a marking policy indicating that the presence or absence of marking is not dispositive of the protected status of the document. Such an approach could keep a thief from being absolved from misusing a document that has not been properly marked.

Given the reality that employees may not always follow whatever marking policy exists, the implementation of other protective measures can be especially important in persuading a court that the information qualifies as a trade secret. Companies need to take a thoughtful approach to how they craft their policies — and train their employees — regarding how to mark documents and what marking (or lack of marking) means.

[1] See, e.g., Call One, Inc. v. Anzine, 2018 WL 2735089 (N.D. Ill. Jun. 7, 2018); see also Abrasic 90 v. Weldcote Metals, Inc., 2019 WL 1044322 (N.D. Ill. Mar. 4, 2019).

[2] Call One, 2018 WL 2735089 at *9.

[3] S. Field Maint. & Fabrication LLC v. Killough, 2019 WL 360515 (M.D. Ala. Jan. 29, 2019).

[4] Hospitality Mktg. Concepts, LLC v. Six Continent Hotels, Inc., 2016 WL 9045853, at *5 (C.D. Cal. May 2, 2016).

6 Min Read

Related Locations

Chicago

Related Topics

Trade Secret

Defend Trade Secrets Act

Data Privacy

Global Privacy & Data Security Task Force

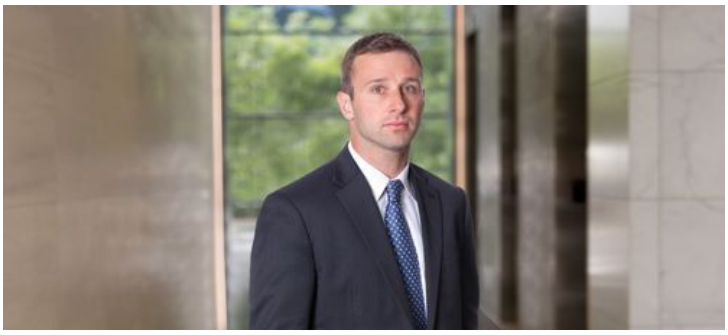
Related Capabilities

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Technology, Media & Telecommunications

Related Professionals



Steven Grimes