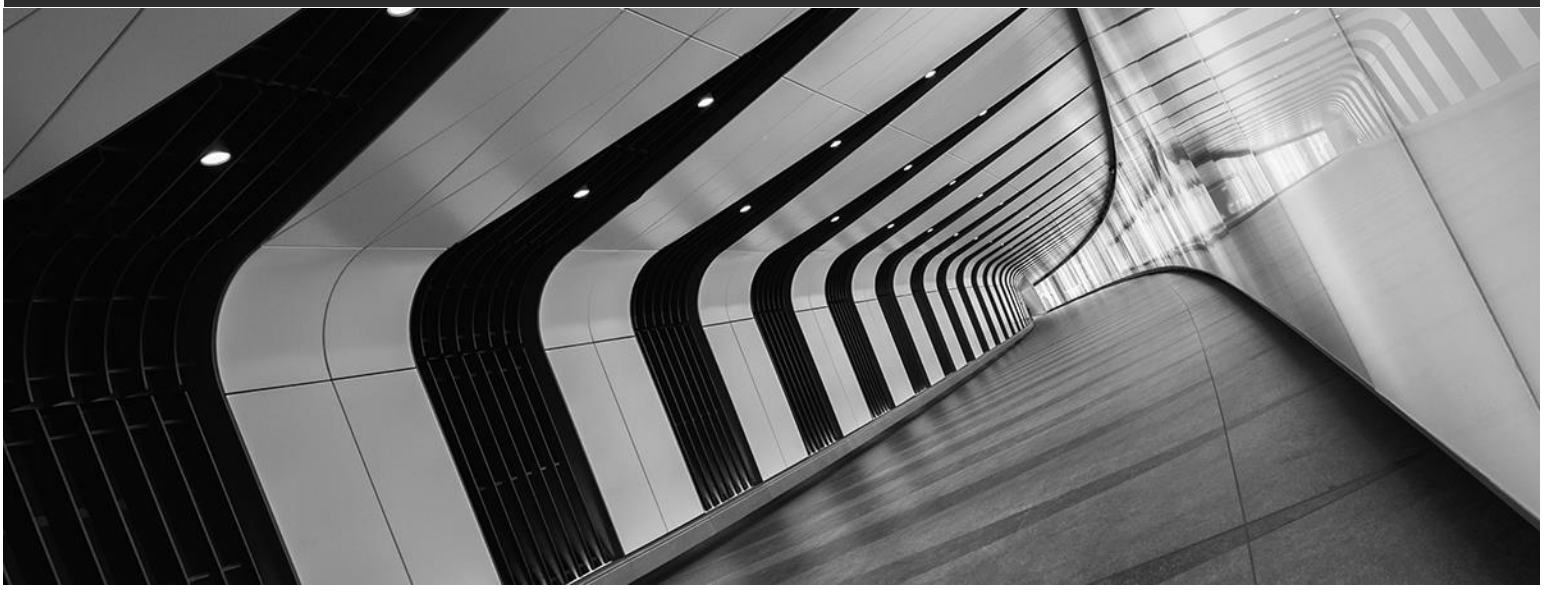
GT GreenbergTraurig

# Proactive Trade Secret Protection: Your Company's Best Investment?



**"There are only two categories of companies affected by trade secret theft—those that know they've been compromised and those that don't know it yet." —Attorney General Eric Holder, speaking at the Administration Trade Secret Strategy Rollout on Feb. 20, 2013.**

**By Jordan Grotzinger | June 12, 2018 | The Recorder**

Five years later, has anything changed? Of course, the most significant change in the law since former U.S. Attorney General Eric Holder's speech was the enactment of the federal Defend Trade Secrets Act in 2016, which largely federalized the Uniform Trade Secrets Act and provided some new enforcement tools, including ex parte seizure. But with constant development of new, valuable trade secrets and evolving technology, there is no reason to think Holder's warning carries any less weight today. Given this reality, do companies do enough to proactively protect what often is their most valuable asset—their trade secrets? Inevitably, for many businesses, the answer is probably not.

**How are trade secrets protected?**

Under both DTSA and the UTSA, for an asset to be a trade secret, it must (1) derive independent economic value from its secrecy, and (2) be subject to reasonable measures to keep it secret. Broadly speaking, these measures usually include some combination of agreements, company policies and technology. Whether these efforts are sufficient is subject to a case-by-case determination. If a court deems these efforts to be insufficient, the asset will not be considered a trade secret and will not be protected as such. Therefore, the protections that businesses impose for these assets are critical.

**What measures are sufficient?**

Confidentiality agreements or clauses, if specific enough, often are held to be sufficiently protective to preserve trade secret status. For example, companies with trade secrets frequently negotiate with other companies about the development of those trade secrets, potential partnerships and related issues. Specific nondisclosure agreements between the companies have been held to be sufficient.

Similarly, confidentiality agreements with employees limiting employees' access to confidential or proprietary information upon termination of employment are often deemed acceptable.

The level of specificity of such agreements can be a fine line to walk. On the one hand, companies generally will not precisely identify the trade secrets at issue in the agreement because (1) they don't want to disclose the trade secret in an agreement that might have to be enforced in open court, and (2) such agreements should be broad enough to cover trade secrets that may not have been developed yet. On the other hand, the more vague the agreement, the higher the risk that a court will find the agreement to be insufficiently protective.

Thus, for example, a nondisclosure agreement with employees prohibiting disclosure of confidential information such as pricing techniques and controlling access to that information through fingerprint scanners has been held to be sufficient. However, if an agreement is too vague for a court to determine what matter the agreement encompasses, a court is more likely to rule that the agreement is insufficient to provide trade secret status to that matter.

Policies designed to limit access to trade secrets can be enough. For instance, limiting employee access to trade secrets on a need-to-know basis can support trade secret protection. Companies should always put these policies in writing because that will ensure stronger proof of the policy than any unwritten practice.

Of course, with cybersecurity an increasing concern, technological protection is more important than ever. Protections including passwords, firewalls and encryption can be sufficient. Other technologies like fingerprint access can enhance protections. Because the sufficiency of protections is assessed on a case-by-case basis, the stronger those protections, the better. Companies should require more complex

passwords and that they be changed with frequency. Measures like firewalls and encryption should be regularly tested, upgraded and improved when possible. And because of the rapid evolution of technology—and in turn potential misappropriators' ability to access trade secrets—companies should view their technological protections as subjects of constant re-evaluation and improvement.

The above is by no means an exclusive list of sufficient protections. There are countless and creative ways to protect trade secrets. In short, companies need to stay ahead of the misappropriators. A company should never consider its trade secret protection "finished." Rather, as a practical matter, it is a constant work in progress.

**How can companies invest in proactive trade secret protection?**

Whether a company is one of "those that know they've been compromised [or] those that don't know it yet," every company with trade secrets should act proactively to protect these key assets. If you don't have agreements or policies in place, you are exposed and should implement them immediately. If you already have such agreements and policies, you should review them on a regular basis to ensure that they (1) are current under the law, and (2) adequately address your current trade secrets. For example, if your trade secrets have evolved to the point that the language in an agreement or policy does not appear to specifically apply to your current trade secrets, the language should be updated. And your counsel should monitor case law and advise you of any case suggesting a need to revise your agreements or policies.

Similarly, companies should stay current when it comes to technological protections. A technology that is sufficiently protective now may be obsolete in a year or two (or less). Information technology personnel should monitor products and ensure that the company is using the most cutting-edge technology possible.

Finally, companies should make regular trade secret protection review a policy. For example, conduct a review at least once a year (or more frequently, depending on the needs of a particular case). That will ensure the constant and never-ending improvement necessary to properly protect what may be your most valuable assets.

## About the Author:

*Jordan Grotzinger is co-chair of Greenberg Traurig's Los Angeles litigation practice and a business trial lawyer. Contact him at* **grotzingerj@gtlaw.com**.

***Jordan D. Grotzinger***

grotzingerj@gtlaw.com