LITIGATION MINUTE: PRACTICAL ADVICE FOR PROTECTING TRADE SECRETS

Date: 16 November 2020

U.S. Complex Commercial Litigation and Disputes Alert

By: Michael R. Creta

WHAT YOU NEED TO KNOW IN A MINUTE OR LESS

When people hear “intellectual property,” they often think first of patents, trademarks, and copyrights. Trade secrets are a fourth type of intellectual property that are critical to businesses because they broadly cover various forms of economically valuable information that may not otherwise qualify as a patent, trademark, or copyright. The trick to trade secrets, however, is that the legal protections available turn on the business protecting the information in the first instance. If the information is not adequately protected by the business itself, the law will not protect it either. Here are five tips for protecting trade secrets:

Develop Policies and Practices

Employee handbooks or other company policies should clearly restrict the use of trade secrets and protect against their dissemination, both internally and externally. By way of a few examples, companies can implement security restrictions for access to certain documents/information, check-in and check-out procedures for documents, and document retention and destruction policies. Importantly, while policies protecting information from transmission outside the company are helpful, more targeted restrictions on access even within the company go further towards demonstrating the existence of a true trade secret.

Train Employees

Company policies are a good starting point for trade secret protection, but a well-drafted policy offers little protection from careless or uninformed employees. It is difficult to provide sufficient detail in a policy such that employees will be able to spot—and properly handle—a trade secret. Because of this, employee training is a critical complement to written policies. Hold in-person or virtual sessions to explain what types of information are confidential, why it is necessary to protect such information, and what can and cannot be done with such information. It can also be useful to provide concrete examples of phishing or other scams that could lead to inadvertent disclosure. Make sure to classify the training as confidential if you are sharing example trade secrets!

Limit Access

As noted above, with trade secrets, less is more. Access to trade secrets should only be provided on a need-to-know basis and both physical and electronic security measures should be implemented to ensure that access stays that way. Such measures can include, among other things, locking cabinets, rooms, or offices, marking documents as “confidential,” limiting the use of portable electronic storage devices or personal email addresses, implementing firewalls, instituting the use of encryption measures, requiring logon passwords for company

©2005-2026 K&L Gates LLP. All Rights Reserved.

computers, and restricting file access rights to certain employees. Companies should also consider any additional vulnerabilities created by increased remote access to trade secrets in a post COVID-19 world.

Contractual Restrictions

Contractual restrictions—including confidentiality, non-competition, and non-solicitation provisions or agreements—provide another helpful tool for protecting trade secrets. Subject to varying state laws, these types of agreements may be an option for new hires, longstanding employees, suppliers, distributors, and various other business partners.

Establish Procedures for Outgoing Employees

A substantial degree of trade secret misappropriation occurs through departing employees taking their former employer's trade secrets with them when they walk out the door. Employers can reduce this risk by implementing various departure protocols, such as cutting off system and email access upon notice of departure (or, at the least, the day of separation), conducting exit interviews to confirm that the departing employee has not retained any confidential information, reminding the employee of any nondisclosure obligations (contractual or otherwise), demanding immediate return of all company devices, and determining where the employee intends to work in the future.

KEY CONTACTS



MICHAEL R. CRETA
PARTNER

BOSTON
+1.617.951.9101
MICHAEL.CRETA@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.