



Building a Case for Trade Secret Misappropriation

A former U.S. Attorney General once said: “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 yet.” At some point, many businesses must consider bringing a case for the misappropriation of trade secrets.

For example, consider the scenario where an employee takes home a laptop or tablet containing company data and refuses to return it after employment with the company is terminated. Or where a company hires a software developer to create proprietary software and the developer sells the same code to a competitor in violation of the parties’ agreement. These sorts of things happen all the time. Below, we discuss the requirements for bringing legal action for trade secret misappropriation and the potential remedies in such cases.

Trade Secret Defined

To prevail in court, a plaintiff must first demonstrate that the information at issue is a trade secret. This generally means that the information has economic value because it is not known by others and the owner has taken reasonable measures to maintain its secrecy. When determining economic value, courts often consider the resources and effort that was involved in developing the trade secret and in maintaining its secrecy.

Some examples of information that might constitute trade secrets include the following:

- Customer information
- Budgets, cost, and margin information
- Financial information prior to public release
- Business plans
- Market studies and research
- Internal market analysis and forecasts
- Client or customer lists
- Business processes
- Training manuals and materials
- Engineering notebooks
- Manufacturing processes and formulas
- Plans, designs, and patterns for specialized equipment
- Failed designs
- Software algorithms
- Pending, unpublished patent applications

Preventing and Detecting Trade Secret Misappropriation

A plaintiff also must show that it has taken reasonable steps to protect its trade secret from disclosure. For example, the secret formula for Coca-Cola is famously kept secured inside a vault. Common measures include physical security, digital and network security, and legal protections. Some examples include the following:

- Labeling documents as confidential
- Using password protection or encryption for sensitive information stored electronically
- Monitoring locations where sensitive information is stored
- Controlling who has access to sensitive information
- Limiting the number of hard copies of sensitive information in circulation
- Using locking file cabinets
- Restricting the use of portable electronic storage devices within the company
- Limiting public access to physical areas of the company where sensitive information is stored
- Using key cards to monitor and restrict employee access to physical locations
- Training employees on the handling and retention of sensitive information
- Employing strict confidentiality agreements with outside vendors and consultants
- Requiring employees to sign confidentiality agreements and/or non-compete agreements

Remedies for Trade Secret Misappropriation


Courts have an array of remedies at their disposal to address trade secret misappropriation. At the beginning of a case, a court may issue a preliminary injunction to prevent further use or disclosure of the plaintiff's trade secrets while the case is pending. In some cases, a court may issue a "gag" order to prevent further disclosure of trade secrets. In rare instances, a court may order the seizure of property to prevent dissemination of trade secrets.

Courts may also award money damages to compensate a plaintiff for its lost profits, to disgorge a defendant of its profits, or to impose a "reasonable royalty" for the defendant's use of the trade secret. Further, in cases of "willful and malicious" acts of trade secret misappropriation, courts may award punitive damages and attorneys' fees.

Additionally, in cases involving the violation of a nondisclosure or non-compete agreement, a breach of contract claim may be included alongside a trade secret claim. Where available, a contract claim can make it easier for a plaintiff to prove its case and obtain a full range of remedies.

Finally, there may be criminal penalties for parties that misappropriate trade secrets under state and federal trade secret laws as well as laws such as the Economic Espionage Act and the Computer Fraud and Abuse Act.

Conclusion

When it comes to trade secrets, an ounce of prevention is worth a pound of cure. However, once trade secrets are compromised, pursuing legal action may be necessary to protect valuable assets. If you are concerned about securing your company's trade secrets, or if you suspect your trade secrets may have been compromised or misappropriated, please reach out to us. 

DISCLAIMER: This paper provides background information of potential interest to facilitate and inform a reader's specific inquiry to be made with legal advisers of their choosing. It does not constitute legal advice. This paper is neither a guide nor an explanation of all relevant issues under consideration. Moreover, the law is ever evolving; observations made today may be inapplicable tomorrow. Fishman Stewart PLLC assumes no responsibility for any use of, or reliance on, this paper.