Maschoff Brennan
INTELLECTUAL PROPERTY AND COMPLEX LITIGATION

PROTECTING YOUR IDEAS AND YOUR BUSINESS
949.202.1900 | MABR.COM
IRVINE | LOS ANGELES | SALT LAKE CITY | PARK CITY

Keeping Your Trade Secrets Secret

By Erynn L. Embree

Virtually all companies possess trade secrets critical to the success of the business; however, without undertaking proper care, business owners may find that some of their most precious assets may not be adequately protected, or are at risk of ending up in the wrong hands. Affirmative steps must be taken for a business to protect its trade secrets, including from disclosure and use by current employees, or former employees seeking to compete by starting their own business or working for a competitor.

Trade secrets encompass a wide range of information – whether it is financial, business, scientific, or technical – and regardless of how the information is stored. Trade secrets can include designs or blueprints, pricing information, or computer technology, for example. Customer information, business plans, and even marketing materials may qualify as trade secrets.

Trade secrets receive protection under both the federal Defend Trade Secrets Act and state statutes. To qualify for trade secret protection, a trade secret owner must engage in "reasonable efforts" to maintain secrecy. What is "reasonable," however, is not explicitly defined. Courts apply a standard of reasonableness based on a number of factors that vary by circumstance, including the degree of sophistication of the company seeking protection, the overall size of the company, and the nature of the trade secret. Your local mom and pop shop will likely not be held to the same standard that would be applied to a Fortune 500 company.

Notwithstanding that no one size fits all, there are certain reasonable steps that every company should consider implementing, depending on individual circumstances and the type of trade secrets at issue:

a. Restricting access: Limit access to trade secret information on a "need-to-know basis," including by limiting access to servers or documents and password-protecting files. Hard-copy information should be locked or have restricted access, with proper disposal.

b. Non-disclosure and confidentiality agreements: Require employees, independent contractors, and any prospective or actual business partners or vendors to sign non-disclosure or confidentiality agreements prior to any information transfer. These agreements should have specific provisions that describe or expressly refer to the trade secret materials and identify the terms on which they can be used, disclosed, and retained.

c. Company policies: Advise employees of the existence of your trade secrets; prepare a protocol for how trade secret materials should be handled, including procedures for marking documents, specifying to whom a trade secret is restricted, and under what circumstances, if any, a trade secret may be disclosed to others (e.g., certain individuals and only after an NDA has been signed).

d. Employee handbook: Include instructions on the treatment of trade secrets.

e. Institute reminders: Remind employees and contractors regularly of their obligations to protect your company's trade secrets.

f. Secure employee workspaces: Confirm that employees implement company safeguards in both home and office workspaces, including password protection and automatic log-out functions after inactivity; multi-factor authentication; up-to-date anti-virus protection; and limited or disabled USB or other external ports to prevent unauthorized removal of documents.

g. Secure business networks & devices: Protect digital information with a firewall or VPN and implement two-factor authentication.

A company should consider consulting an attorney to ensure its non-disclosure agreements are compliant with the law, which is constantly changing. For example, an NDA that prevents an employee from acting as a whistleblower may be rendered unenforceable under certain circumstances.

In addition to protecting your trade secrets from others, businesses should also be mindful of protecting themselves from inadvertently obtaining others' trade secrets. A new hire can unwittingly infect your company's system with stolen information, particularly if they are a former employee of a competitor, putting your business at risk. The following are only a few of the steps a company should consider to prevent unwanted disclosures:

a. Non-disclosure obligations: Verify whether your new hire is under any non-disclosure or non-compete obligations and help them to understand and comply with their lawful obligations.

b. Confirm return of prior company information. Ask your new hire to confirm in writing their return and non-retention of their prior employer's confidential information and documents.

c. Separate industry knowledge from competitor information: Make clear to a new hire that they are not to bring with them or use information obtained from a competitor and that they are being asked only to use their general skills or knowledge of your industry. Have the employee sign an acknowledgment of this policy.

d. Secure employee workspaces: Limit or disable USB and other external ports to prevent unwanted information from being introduced into your systems.

Working with legal counsel to identify your company's trade secrets and to assess what reasonable measures should be undertaken is one way to ensure that your company's assets are protected, whether on a day-to-day basis or in the courtroom.

Erynn Embree is an associate in the Orange County office of Maschoff Brennan. She focuses on a variety of intellectual property and complex litigation matters, including patent and trademark infringement and breach of contract actions.