LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, OCTOBER 9, 2019

TOP TRADE SECRETS LAWYERS

Developing a trade secret protection program to reduce risk and increase court enforcement

By Mark Terman

Companies rely on trade secrets for competitive advantage. Theft of those assets hurts them by empowering competitors who have not invested the intellectual and financial capital needed to create them. Trade secret theft can also demoralize company sales, R&D and other employees who helped create the trade secrets only to have a former employee or business partner, now a competitor, seek to profit from their labor.

Protection programs can deter and limit trade secret misappropriation. If needed, the program can also put the company in a better position to seek an injunction to stop a competitor's use, and require return, of company trade secrets and to seek damages. Development of a trade secret protection program should consider the following.

Identify the Trade Secrets

California's enactment of the Uniform Trade Secrets Act, Cal. Civ. Code Sections 3426 to 3426.11, and the federal Defend Trade Secrets Act, 18 U.S.C. Section 1836, et. seq., share common essential elements to define "trade secret" as information that (a) derives economic value from not being known outside the company; and (b) is the subject of reasonable efforts to maintain its secrecy. A good starting place to evaluate proprietary information is to answer three questions.

First, what information, if taken and used by a competitor, could seriously damage the business or give the competitor an unearned windfall by not having to develop the information on its own? The more narrowly a company defines its trade secrets, the more likely a court will be persuaded. Some courts are skeptical of claims of trade secrets that look so all-encompassing and overbroad that the volume distracts from protection of the "real" trade secrets the company cares about most. Do not overlook "negative information," such as the results of lengthy and expensive research proving that a certain process will not work, which could be of high value to a competitor.

Second, in reality, is the information generally available to others, common industry practice, or outdated? If it is relatively easy to recreate, or reverse engineer, it is probably not a trade secret.

Third, if it is a trade secret, how much time and money will the company spend (or spent already) to develop the information? Developing this economic value record and updating it periodically can reduce the kind of "scrambling" to assemble the information that sometimes occurs when there is immediate urgency to seek a court order. This record may appear to be an unnecessary burden; but, it could also have interim import by helping enhance company value for financing, investors, M&A, insurance or other business purposes.

Maintain Secrecy

As a baseline for reasonable efforts to maintain secrecy, all personnel who may access trade secrets must sign a confidentiality agreement that prohibits their unauthorized use or disclosure. Require this as a condition of initial hire and include obligations to return of all company property upon end of employment. It should also require the new employee to certify that she or he has not used or disclosed any trade secrets of their prior employer to the company, and will not do so. Consider having HR or counsel meet with the new employee upon hire seeking to assure that they have not taken any trade secrets from the competitor who previously employed them.

Update employee handbooks by including confidentiality and social media policies, and limiting employees' expectation of privacy in their use of the company's computers, phones and work areas. Use pre-hire background checks to identify applicants whom the company lawfully should not even hire.

Identify and limit electronic and physical trade secret access to employees or work groups who need to know the information to do their jobs well. These "need to know" barriers tend to be the most practical and effective measures to protect information. Methods to consider include, labeling "trade secrets" as such (or "confidential"), implementing layers of computer password-protected access warning screens reminding employees of their confidentiality obligations, adding time-out functions on inactive computers, restricting ability to print or copy files, inserting codes into sensitive files that restrict access and permit tracking of their use, formatting hard drives before

computer disposal, installing physical barriers such as locks on doors and drawers, requiring identity and access badges, and shredding paper trash.

Include in the program lawful monitoring of networks, workstations and laptops to detect and make a record of attempted downloads; file transfers and use of trade secrets. Consider whether smartphones and cameras must be checked in upon workplace entry, and returned upon daily exit.

Issue company-owned, use-monitored computers and smartphones if financially feasible, and consider prohibiting or limiting their personal use. Enable access to the device to search in-person or by remote and, if the device is lost, the employee is suspected of wrongdoing, or leaves the company, information on the devices can be wiped-out remotely.

The prevalence of companies who permit use of employee-owned devices for business purposes raises employee privacy and other legal issues that can be anticipated with policies and agreements. For example, prohibit use of non-approved apps to convey company information, implement security measures on devices, and obtain written employee consent as a condition of employee access to the company's systems and information. This consent should include that the company can access the device, and can remote-wipe all information on the device, under certain business-reason circumstances. Consider a requirement for "sandboxing" software that segregates business information on the devices from personal information.

Protection programs can deter and limit trade secret misappropriation. If needed, the program can also put the company in a better position to seek an injunction to stop a competitor's use, and require return, of company trade secrets and to seek damages.

Do not overlook non-employees in the program. Execute NDAs with business partners and other outsiders who may come into contact with company trade secrets such as M&A parties, independent contractors, recycling and other vendors, IT and other consultants, bankers, and in appropriate situations, customers. Scrub presentations of company personnel to outsiders. Narrow company tours and other on-site events to avoid access to trade secrets.

Exit Procedures

Conduct interviews of exiting employees. Ask them where they are going. Remind them of their ongoing confidentiality obligations. Obtain return of all company property, including electronic storage devices. Deactivate and remote purge all devices not returned. Review places where trade secrets may have been stored off site and arrange for their return or purging. Obtain a signed certificate that all company property, including trade secrets, have been returned and any backups purged. An exiting employee's refusal to cooperate, or delay in doing so, is often a red flag. Even if they do not sign, provide an extra copy of the confidentiality agreement with a letter stating the expectation that they will abide by it and that they should show it to their next employer.

Promptly Investigate and Take Action

When a theft is suspected, involve counsel and investigate promptly. When a key employee leaves, do the same. Sources for examination include computer hard drives, smartphone memory, data and contacts, building and garage access logs, and expense reports. Include forensic experts trained to preserve evidence integrity. When investigation reveals that trade secrets were taken and the company's business is at risk, take legal and other lawful protective action. Not taking action may give an argument to the next violator that the company does not itself believe it has trade secrets to protect. ■

Mark Terman *is the national vice-chair of the Labor & Employment Practice Group at Drinker Biddle & Reath LLP.*