NCHRA NORTHERN CALIFORNIA HUMAN RESOURCES ASSOCIATION

HR West®

A MAGAZINE FOR CALIFORNIA HR PROFESSIONALS

RUTAN

RUTAN & TUCKER, LLP

Keeping Company Secrets:

Protecting Your Proprietary Information Under California Law

A. The Challenge Of Controlling Confidential Information

Your company's director of product development, top salesperson, or chief financial officer has just decided to accept a position with your biggest competitor. He just gave his four-week notice – leaving plenty of time to download the company's customer lists, financial statements, and new product information before starting his new job. Much of this information is already loaded onto his company-owned laptop, but one early-morning trip to the office enables him to download the remaining data he wants to take to with him. For most small- and medium-sized businesses, the security systems in place are insufficient to prevent this sort of theft, making such actions almost inevitable. The good news is that with a few relatively inexpensive precautions, the company may be able to significantly limit the damage this employee can cause with the improperly obtained information.

The crux of the problem is that once an employee becomes an *ex*-employee, the company's leverage over him is limited, and it becomes difficult to dissuade him from his course of action. At that point, the employer's best recourse is often trade secret laws, which can provide powerful protection for properly protected proprietary information. However, in order for these trade secret laws to be effective, the company must have taken certain steps to protect the information it considers to be a trade secret. The purpose of this article is to explain, in general terms, what type of information may constitute a trade secret, and second, to detail steps that can be taken to protect that information.

B. Defining What Constitutes A Trade Secret In California

Everyone agrees on the technical definition of a trade secret. The problem is that few agree on how to apply that definition to real life. Trade secrets in California are governed by the appropriately-named Uniform Trade Secrets Act ("UTSA"), which defines a "trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique, or process that (1) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[1]

In light of this broad definition, a variety of types of information have been found to constitute trade secrets, including:

- customer lists;
- employee lists;
- internal documents showing employee compensation or areas of expertise;
- research results, methods, procedures, or other expertise, including research regarding *unsuccessful* processes or procedures, whether or not subject to patent protection;
- strategic business information regarding pricing, material costs, and suppliers;
- financial, marketing, distribution, and manufacturing plans; and
- computer software and databases.

[1] CAL. CIV. CODE § 3426.1(d).

Of course, as the UTSA definition makes clear, whether certain information constitutes a trade secret requires a close look at the facts. Determining whether information "derives independent economic value" such that the possessor of the information has a competitive advantage over those who do not is a specific inquiry, and requires consideration of the particulars of the business and its industry.

For example, it is public knowledge that certain cookie companies sell to Disneyland. That information is not a trade secret, since anyone can walk through Disneyland and learn what brand of cookies are sold there. However, the name of the cookie company's specific contact at Disney, her deal points, and her purchasing history is not public information. There are probably a number of companies that would like to learn this individual's name and bargaining history. This information is clearly valuable to competing cookie companies and would almost certainly be considered a trade secret. Determining the precise point where the information ceases to be "public knowledge" and becomes a trade secret involves delving into gray areas beyond the scope of this article.

C. Protecting Your Trade Secrets

Merely labeling information as a "trade secret" does not entitle it to protection. A trade secret must actually be kept "secret" to be entitled to protection under the law, since widespread public disclosure of confidential information will obliterate its trade secret status. For example, courts have noted that dissemination of information via the Internet can destroy a trade secret.[2] Even inadvertent publication of a company's customers, pricing, projects, or other sensitive data on a website can result in a trade secret losing its protected status. Trade secret protection can also terminate when information is disclosed to third parties, including the friends or relatives of company executives. In short, if a business hopes to have a court protect stolen information as trade secrets, the business must treat the information as secret as well.

Whether a company has taken sufficient steps to protect the information at issue is an inherently fact-specific inquiry, and there are numerous methods a company can use to protect the sanctity of its trade secrets. In general, companies should tailor their protective measures to the particulars of their business model and their specific industry as a whole. That being said, the following are examples of measures that can be implemented to bolster the company's claim its proprietary information is entitled to trade secret treatment.

➢ *Decide What You Want To Protect*

The first step to protecting a business's trade secrets is to identify what information actually constitutes a trade secret. Management should determine the types and categories of information that it deems proprietary, and should mark relevant documents as "CONFIDENTIAL" and "TRADE SECRET." This decision must be carefully deliberated, as a court may determine that the information that is not marked confidential is not a trade secret. At the same time, however, marking *everything* as confidential may lead a court to view the designation as overbroad, and to disregard it entirely. Labeling documents in this manner communicates to employees that the company considers the documents trade secrets, and that they should not remove or share the information with others. Companies should also revisit the list periodically to ensure that it remains updated and accurate. While this is a necessary first step, it is by no means sufficient, since simply marking documents as "CONFIDENTIAL" or "TRADE SECRET" will usually not be sufficient to afford protection.

---

[2] *DVD Copy Control Assn., Inc. v. Bunner*, 116 Cal. App. 4th 241, 251 (2004).

➢ *Limit Access To Sensitive Information With Physical And Digital Security Measures*

Employers should also take steps to limit access to trade secret information. For example, proprietary information should be shared with employees only on a "need to know" basis. In this age of technology, digital security measures will be paramount. Sensitive documents and files should be password-protected or locked to ensure that they are not accessed by unauthorized employees. Companies should also ensure that their websites do not disclose information that is intended to be trade secret, and that their employees are not blogging about the information online. Finally, employers should ensure that their policies provide management unfettered access, at any time, to all company-owned computers that are utilized by employees.

For more tangible items, to the extent it is practicable, proprietary information should be kept in locked files, or in rooms that only certain individuals are permitted to access. Unauthorized employees or visitors should not be permitted into areas where confidential information is kept or developed. Video surveillance can be useful for limiting and monitoring access to sensitive areas.

Some employers use log books to track employees' access to confidential information. Others protect sensitive documents by printing them on specially-colored paper that makes them more identifiable, and can also make effective photocopying, scanning, or faxing difficult. Document destruction procedures can also be implemented, in order to ensure that proprietary information cannot be gleaned from company trash bins.

➢ *Utilize Company Contracts And Policy Documents To Bolster Protection Of Sensitive Information*

Employers should require all employees, and especially those who will be given access to trade secrets, to sign confidentiality and nondisclosure agreements. Such agreements serve two purposes: (i) they communicate the employer's policy regarding trade secrets to the employee, and (ii) they may give the employer additional remedies and options in the event litigation arises from the theft of secrets. These agreements can protect the company's proprietary information even beyond the term of employment, and should be implemented as early in the employment relationship as possible. Employers should incorporate similar language into their handbooks.

To the extent that a company's customers or contact lists constitute trade secrets, employers should also consider implementing non-solicitation agreements that will limit departing employees' ability to siphon off customers once they arrive at a new employer. These agreements must be carefully drafted, as it is extremely difficult in California to prevent an employee from going to work for a competitor. Furthermore, documents that can be construed to do more than is necessary to protect a company's proprietary information will likely be found invalid by a court.

➢ *Take Special Precautions In Dealing With Departing Employees*

When employees leave the company, special precautions should be taken to protect the business's proprietary information. In this regard, an exit interview – where an appropriate member of management meets with the departing employee – is a crucial step. This interview serves to reinforce the company's confidentiality policies and collect any relevant access cards, keys, and identification that would allow the individual access to sensitive areas, as well as any other company property in his or her possession. Steps should also be taken to ensure that the employee has deleted any digital information that might have existed on his or her personal computers and data storage devices. During the interview, an acknowledgement form can be used to make sure that the employee has returned all company property, and that he or she understands the non-disclosure obligations. Even if the company believes the employee is improperly removing

proprietary information, this step will serve to reinforce to a judge or jury the notion that the company did everything within its power to protect its trade secrets.

If an employer learns that a former employee has joined a competitor, and has grounds to believe that its trade secrets might be compromised, it should react immediately. Any delay can be interpreted as a lack of interest in protecting the trade secrets, and might be used to defeat the company's attempts to protect its information. For example, if a company waits three months after becoming aware of the theft before seeking to protect its confidential information, there is a strong possibility the lengthy delay will lead a court to conclude that the information is not truly proprietary.

After learning of a potential problem, the company should first seek to informally protect its interests by sending a letter to both the ex-employee and his or her new employer, advising both of the individual's non-disclosure obligations. Such correspondence puts the new employer "on notice" that the former company is serious about protecting its trade secrets, and that can be useful in the event that litigation results from the use of the first employer's trade secrets. Such post-employment letters should be undertaken only with the assistance of qualified legal counsel in order to avoid being construed as inappropriately threatening litigation, making defamatory statements, or unlawfully interfering with the individual's right to pursue employment.

D. Finding A Solution That Works For Your Business

For a majority of small and medium size companies, the cost of a comprehensive security system that thoroughly prevents the theft of trade secret information is prohibitive. However, by properly identifying and taking steps to protect proprietary information, companies can go a long way towards recovering and/or controlling the dissemination of the trade secret information that has been improperly taken. As indicated above, this area of the law is complex. We strongly suggest you consult with your attorney at every phase of the process to ensure that your efforts made to protect your business's information are lawful and enforceable.

Jeffrey Wertheimer is a Partner in the Employment and Labor Department of Rutan & Tucker, LLP, where he draws on more than two decades of litigation and counseling experience to protect business and employer interests. Mr. Wertheimer has successfully defended clients in a variety of employment matters, including class action and multi-plaintiff wage and hour, harassment, disability discrimination, retaliation, wrongful termination, and breach of contract claims. Mr. Wertheimer may be contacted at jwertheimer@rutan.com.

Brandon Sylvia is an Associate in the Employment and Labor Department of Rutan & Tucker, LLP. Mr. Sylvia's practice involves representing employers in employment-related litigation, including wage-and-hour class action disputes, trade secret litigation, business contract disputes, and retaliation, harassment, and discrimination claims. In addition to litigation, Mr. Sylvia counsels employers regarding human resource issues, and assists employers in developing and implementing personnel policies and handbooks. Mr. Sylvia may be contacted at bsylvia@rutan.com.