

## ***First Wednesday — A Monthly Discussion of Employment Law Issues and Other Hot Topics for Management***

---



***By Jeffrey A. Snyder - Issue No. 21: April 7, 2004***

Jeff is a Shareholder of Thoits, Love, Hershberger & McLean, specializing in employment law and commercial litigation. He can be reached at (650) 327-4200 or [jsnyder@thoits.com](mailto:jsnyder@thoits.com).

### **Protecting Company Trade Secrets In An Age Of Employee Mobility**

Two realities shape today's workplace. First, employees are not likely to stay with their companies for the long term. With increased layoffs, rising merger and acquisition activity, and decreased loyalties, today's employee will likely change jobs and employers many times over his/her career. The second reality is that intellectual property ("IP"), including lists of customers and key contacts, is increasingly becoming a company's most valuable asset. Thus, a key risk management question is: What can be done to prevent an employee from taking the company's most strategic, valuable property when he or she moves on?

This issue must be dealt with systematically, upon hiring the employee and using company-wide security procedures, as described below.

#### **Confidentiality Agreements with "Anti-Solicitation" Features**

All new hires should be required to sign a legally enforceable confidentiality agreement. This agreement cannot take the form of a covenant-not-to-compete ("Non-compete"), or anything similar, since a company then runs the risk that a court will refuse to enforce the agreement. By statute in California, a Non-compete is void and unenforceable. There are two narrow exceptions: one relates to the sale of good will in

a business and the other to the sale of a partnership or limited liability company (“LLC”) interest. Since the exceptions don’t apply to most new-hire situations, many companies try to use “anti-solicitation” clauses, such as the following, to avoid the Non-compete bar:

“For a period of one year following the termination of employment, I will not call on, solicit or take away any of Company’s customers or potential customers with whom I have had any dealings as a result of my employment by Company.”

This clause, standing alone, is not good enough. A recent California Appellate panel (*Thompson v. Impaxx, Inc.*) ruled against the employer in a case of wrongful termination featuring this clause. In this case, the employee, Thompson, refused to sign an anti-solicitation agreement which included the above-quoted clause. The company fired him for that reason. He sued for wrongful termination based on the rule that termination of an employee for refusing to sign an unenforceable Non-compete can be a “wrongful termination” in violation of public policy. The court ruled in Thompson’s favor, allowing the case to proceed on his wrongful termination theory, a surprising result considering the clause did not directly prevent Thompson from working for a competitor.

Key to the court’s decision was the fact that the anti-solicitation clause was not tethered to the protection of the company’s trade secrets. This clause was definitely less restrictive and less anti-competitive than the broad, traditional Non-compete clauses specifically outlawed by statute. But the court held that it was nevertheless anti-competitive and void as an unlawful business restraint unless necessary to protect the company’s trade secrets. According to the court, “[I]n the absence of a protectable trade secret, the right to compete fairly outweighs the employer’s right to protect clients against competition from former employees.”

### **Importance of Trade Secret Descriptions and Protective Measures**

The agreement between the company and its employees must, therefore, describe the types of trade secrets the company intends to protect. But the company must do more than identify the trade secrets and confidential information being protected. Simply labeling information as a trade secret, or as “confidential information,”

does not establish that the information fits the description or is worthy of legal protection. The information must actually be a trade secret, which involves two legal elements.

First, the information must have 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. This might include a customer list or development process, technique, formula, etc. Second, the company must make reasonable efforts to maintain the secrecy of the information.

Much of trade secrets litigation focuses on the second prong of this test – the reasonable efforts to maintain secrecy. A court will consider such things as: building security and access restrictions, computer system security and related use of keys, access codes and passwords, document storage and retention policies, use of confidentiality agreements with employees and customers (Non-disclosure agreements, or NDAs), written security policies, etc., depending on the circumstances of the company and particular industry standards. Not only must the security precautions be in place, but they must be regularly observed, evaluated and updated periodically.

To summarize, a company should (1) implement all reasonable security measures if it intends to protect its trade secrets, beginning with a legally enforceable confidentiality/anti-solicitation agreement signed by all employees; (2) actually put the security measures into practice; and (3) observe and update the measures as needed.

### **Other Measures to Consider, Including Post-Termination**

Beyond having employees sign confidentiality agreements and maintaining the secrecy of the IP, other security measures should be considered. For example, a policy banning camera-equipped cell phones in the workplace is appropriate for any company developing sensitive technology. These popular and seemingly-innocuous phones can make it very easy for an employee to covertly snap photos of the company's most valuable IP assets.

When it is apparent that an employee will be leaving, the company should act quickly to cut off that employee's access to its computer systems and physical property.

All company property must be recovered. The employee could possibly have a laptop computer or PDA device which belongs to the company or stores company information – don't overlook these.

The company should also conduct an exit interview, and determine where the employee is going, why, with whom, how he was recruited and what exactly he will be doing. This interview gives the opportunity to remind the employee of continuing obligations not to disclose company trade secrets or violate any written agreements or company policies post-termination. Copies of any such agreements and policies should be given to the employee at this time. The person's new employer should be notified in writing, preferably by an attorney, to alert the new employer that your ex-employee had access to valuable trade secrets which should not be disclosed or used under any circumstances in the new employment.

Other post-termination steps might include the "hiring" of the employee as a consultant for a period of time after the employment, with the person essentially being paid (in installments) not to compete. If the employee competes, the payments stop. This type of arrangement can ultimately be ruled unenforceable in court, but presumably the payments will make it worthwhile for the employee to act appropriately and avoid the courts.

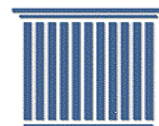
Finally, if all else fails, and the employee violates legal or contractual duties with respect to trade secrets, the company might sue for an immediate temporary restraining order and preliminary injunction, to prevent the disclosure and use of trade secrets. The issue of misappropriation of trade secrets needs to be acted upon immediately, not only for legal reasons, but for the obvious practical reason that dissemination could irreparably harm the company's business.

**First Wednesday Distribution List:**

- If you are not receiving this newsletter directly, please send me your e-mail address and I will add you to the First Wednesday Distribution List.
- If you would like this newsletter redirected to others within your organization, please send me their e-mail addresses.
- First Wednesday is a publication of general applicability and not specific to any set of facts. Thus, it should not be relied upon for any specific case or matter without further discussion. No attorney-client relationship is formed as a result of your reading or replying to this newsletter, which is not intended to provide legal advice on any specific matter, but rather to provide insight into current developments and issues.

Jeffrey A. Snyder  
Thoits, Love, Hershberger & McLean  
245 Lytton Avenue, Suite 300  
Palo Alto, California 94301-1426  
Telephone: (650) 327-4200  
Facsimile: (650) 325-5572  
E-mail: [jsnyder@thoits.com](mailto:jsnyder@thoits.com)

THOITS  
LOVE  
HERSHBERGER  
& McLEAN  
Attorneys at Law



A Professional Corporation