LJN LAW JOURNAL NEWSLETTERS

Employment Law Strategist®

An ALM Publication

Volume 18, Number 4 • August 2010

# Employers Beware

## *A Storm of Trade Secret Theft Is Brewing!*

**By Rick Bergstrom and Mark Temple**

The modern employee is increasingly mobile. According to an article published in *Forbes Magazine* in 2007, 85% of American workers are expected to be employed by a new company within the coming 12 months. Moreover, in these difficult economic times, many companies are taking advantage of the opportunity to poach top talent from their competitors. According to an article published in *The Wall Street Journal* in February 2010, 70% of companies surveyed were very — or somewhat — concerned about losing top talent due to cutbacks made during the recession. Employee mobility, coupled with the exceeding ease with which confidential and proprietary trade secret information can be stored and transported, create the perfect platform for trade secret theft by departing employees. Indeed, in a recent survey conducted by the Ponemon Institute, 59% of the individuals surveyed confirmed that they kept company information after leaving their former employer. This occurred despite the fact that 79% of the individuals surveyed conceded that they were not permitted to take a company's sensitive information.

Trade secrets, such as methods of manufacturing, targeted areas of growth, and customer sales data are often the "crown jewels" of a business. They have the potential to allow companies to gain a competitive edge in the marketplace and must be adequately protected. Further, given the risks and realities of employee theft of trade secrets, businesses should implement specific practices and procedures designed to protect their confidential information, lest they risk protracted and costly litigation. In addition, the risks and likelihood of hiring "contaminated employees" (*i.e.*, individuals who have stolen trade secrets from their former employers) are equally great, and companies that do not take appropriate proactive precautions in the hiring process can unintentionally find themselves embroiled in time consuming and expensive litigation.

The significant monetary risks at issue were recently graphically illustrated in a $38 million settlement agreement resulting from protracted litigation between Thermax and Purolite involving claims based on the alleged theft of trade secrets. Companies simply cannot afford to ignore this issue any longer.

### Data Transferability

The transferability of massive amounts of data has never been easier. CDs, DVDs, USB mass storage devices and e-storage are but a few quick and easy methods for the transfer of electronically stored information. These devices are easily accessible, often provided to employees by their employers, and can be purchased at any office supply store for less than the cost of a cup of Starbucks coffee. Thus, the transfer of data via these means can easily be completed secretly and quietly, below the radar of an undiscerning employer.

#### *Not Just a Hypothetical Problem*

In January 2009, the Ponemon Institute conducted a study entitled "Data Loss Risks During Downsizing: As Employees Exit So Does Data." The survey population consisted of 945 individuals who were either terminated, or had resigned their latest employment in the preceding 12 months. What all 945 members of

---

**Rick Bergstrom** is a labor and employment partner in the San Diego office of Jones Day. He can be reached at 858-314-1118 or rjbergstrom@jonesday.com. **Mark Temple** is a labor and employment partner in the firm's Houston office. He can be reached at 832-239-3741 or mdtemple@jonesday.com. The authors would like to thank **Liat Yamini**, a Labor & Employment Associate in Jones Day's Los Angeles office, for her substantial work on this article.

the study had in common was that they all received laptops and access to proprietary information at their previous employment.

Again, 59% of those surveyed confirmed they kept company information after leaving their former employer. The most common kinds of files that were kept were e-mail communications (62%), hard copy files (62%) and software programs or tools (32%). Of course, at many companies, e-mail messages and their attachments frequently contain much of the company's most valuable confidential information.

The most common methods of transfer were the taking of hard copy files, and CD-, DVD- and memory stick- uploads. In addition, 38% of the survey group transferred the stolen files by sending them to an external e-mail account. Surprisingly, 13% of participants actually claimed that they were permitted to keep the laptop provided by their former employers after termination of the employment relationship. Any hope that this type of information is taken but never used, was also shattered by the survey results. 68% of the respondents surveyed who had obtained new jobs, either already had, or were planning on using the confidential and proprietary information in their new employment. Adding insult to injury, 67% of these same individuals used their former employer's confidential, sensitive information in securing new jobs.

## Sound Protection Program: 'The Key Ps'

To combat these problems, companies should develop their own trade secret protection program that includes the following elements: 1) pinpointing their trade secrets; 2) implementing paper protections for trade secrets; 3) implementing physical protections for trade secrets; and 4) post-departure processes for protection of trade secrets.

***Pinpoint***

A "trade secret" is information that: 1) has independent economic value; 2) is not generally known to the public or to persons who can receive economic value from its disclosure or use; and 3) is subjected to a reasonable degree of secrecy by the company, both internally and externally. The first step in protecting trade secret information is pinpointing what the company wants to protect. Employers must identify where the information is stored (work, home, third parties), how it is stored (hard copy, electronic, server, laptop), who has access to it (employees, consultants, manufacturers, potential investors, attorneys) and possible disclosures (business dealings, litigation, marketing materials, Internet, articles, seminars). Once identified, employers should consider the various methods for safeguarding the trade secret information.

***Paper Protections***

Among the paper protections that companies should consider implementing are the following: non-disclosure agreements, confidentiality agreements, third-party agreements, document control and labeling processes, and visitor sign-in acknowledgements to protect their trade secrets. Additionally, employers should implement policies pertaining to confidential and personal information, technology use and security, and blogging and social networking. A thorough entrance interview and continuing education programs are also valuable tools in creating a culture that values and protects the company's confidential information.

***Restrictive Covenants As Paper Protections***

Employers may be tempted to use restrictive covenants, such as non-competition and non-solicitation provisions, as a means for protecting their trade secrets. While restrictive covenants may serve as a good defensive strategy, the range of enforceable restrictions varies state to state depending on the facts and circumstances involved. As a result, restrictive covenants must be narrowly tailored and crafted based on the particular circumstances of the employer and the state law that may be applicable.

For instance, California has a general bar against non-competition provisions, with limited exceptions. California Business & Professions Code § 16600 provides that every contract by which anyone is restrained from engaging in a lawful profession, trade or business is to that extent void. California courts have reasoned that the interests of employees in their own mobility and betterment are paramount to competing business interests. *See, e.g., Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244, 255 (1968).

Further, three recent California cases suggest that companies should narrowly tailor any non-solicitation of customer provision to protect only confidential information. In *Edwards v. Arthur Anderson LLP*, 44 Cal. 4th 937 (2008), the California Supreme Court recently found that a non-solicitation of customers provision not tied to the use of company confidential information was void under Business & Professions Code § 16600 based on the facts of the case. Similarly, in *The Retirement Group v. Galante*, 176 Cal. App. 4th 1226 (2009) and *Dowell v.*

*Biosense Webster, Inc.*, 179 Cal. App. 4th 564 (2009), two California Courts of Appeal determined under the facts of those cases that § 16600 voided a court order and agreement prohibiting solicitation of customers where the limitation was not tied to the use of the company's confidential information.

***Physical Protections***

Companies also must ensure that their physical infrastructure is protected. Companies should consider using shredders for important documents, and hiring information technology security professionals to implement document management systems. Additionally, employers should restrict employee access to areas (electronic and physical) in which trade secrets are kept, and as an added layer of protection, restrict the use of personal electronic devices in those areas. Companies can also place strategic typos in documents or source code, or "dummy names" on customer lists, to assist in identifying a security breach.

***Post-Departure***

A thorough exit interview may be useful specifically to audit the documents that are going to be removed by the employee and any information taken. Based on the company's assessment of the risks in light of the employee's position, their access to confidential information, and their plans for subsequent employment, companies should consider having their information technology specialists create a mirror image of the former employee's desk top and laptop computers, and user profile. Most importantly, companies should immediately terminate a departing employee's access to all internal networks. In the Ponemon Institute's study discussed earlier, at least 24% of the survey respondents had access to their employers' networks after departure from the company, and 35% of those maintained access to network files for one week or more. This simply cannot be permitted to occur given the valuable assets that are at stake.

## Trade Secret Theft Is a Double-Edged Sword

The danger of stolen trade secrets cuts two ways. Not only must companies protect their trade secrets from theft by departing employees, but also, companies should take proactive steps to not hire "contaminated employees" — those employees who have stolen trade secrets from their former employers.

Lawsuits based on "misappropriation" of trade secrets have resulted in a variety of severe penalties for the hiring company. Judges have issued injunctive relief to prevent companies from ever using stolen trade secret information, and have ordered damages in the tens of millions of dollars for actual losses and unjust enrichment. Indeed, the California Uniform Trade Secrets Act authorizes the award of punitive damages in a sum of up to twice the amount of actual damages where the misappropriation is found to have been willful and malicious.

## Limiting Liability in Hiring

In an effort to shield against hiring "contaminated employees," companies should generally run a criminal background check on prospective employees. Additionally, companies should require a newly hired employee to acknowledge, in writing, that he or she: 1) will not bring or use a former employer's sensitive information; 2) has not been asked to do so; 3) can perform the new job without the use of the former employer's information; and 4) has not and will not solicit former co-workers. This statement can be contained in an offer letter, proprietary information agreement, and/or a stand-alone acknowledgment. Further, when warranted, companies should consider obtaining a reimbursement (indemnity) agreement from new employees for litigation costs incurred by the company should it be determined that the individual engaged in unauthorized wrongful acts with regard to a former employer's trade secrets.

## Conclusion

In a marketplace of increased employee mobility and easy transfer of massive amounts of data, employers must protect themselves against trade secret theft by departing employees, and must shield their enterprises against individuals contaminated by stolen trade secret information. This may not be an easy task in California, where employee mobility and betterment is highly regarded by courts, and trade secret theft can be accomplished secretly, quietly and quickly. Nonetheless, companies should institute calculated protection programs and policies to prevent the spread of their companies' sensitive information, if they hope to maintain their competitive edge and minimize the risk of costly litigation.