Alert
Employment & Discrimination

GREEN·SEIFTER
ATTORNEYS, PLLC

Protecting Your Assets:

Practical Advice for Avoiding Employee Theft of Proprietary Information

Green & Seifter, Attorneys, PLLC September 13, 2010

Employee theft of conf dential and proprietary information is pervasive. In studies reported by the Washington Post and Bloomberg Business Week, almost 60% of ex-employees admitted to taking company data. Two-thirds of the admitted thieves acknowledged that they did so in order to assist them in their new jobs. Unsurprisingly, the theft not only occurs in the traditional form of stealing paper documents and hard f les, but occurs by copying electronic f les. The surveys also ref ect an increasing attitude by employees that they are "entitled" to this information, and they feel no remorse for their actions.

The cost of this thievery can be staggering for many businesses. The stolen data is often information that has been developed over years, at signif cant cost and expense. Moreover, the information itself is often central to the company's market share and success, and provides the company an advantage over its competitors. Conf dential and proprietary information does not simply include formulas and patents, but may include such things as client and customer lists, marketing and business development strategies, and customer rates and contracts.

When proprietary information is removed by an employee and shared with a competitor (or used by the employee in a new competing enterprise), employers generally have two options: (1) accept the loss and the resulting damage to their business; or (2) f ght to preserve the information as conf dential, which usually involves incurring signif cant legal expenses. There are, however, several steps that employers may pursue to protect their conf dential and proprietary information prior to facing this choice.

Step One. Employers must take the time to identify their company's conf dential and proprietary information and develop the appropriate technology and security protocols to protect such information from unintended dissemination or theft. Such steps may include: (i) physically restricting access to servers, routers and other network technology to those whose job responsibilities require access; (ii) installing surveillance equipment; (iii) keeping company equipment under inventory and control; (iv) encrypting data for limited access by approved personnel; (v) locking f le cabinets and off ces where sensitive information may be stored; (vi) designating documents as trade secret or conf dential; and (vii) shredding documents containing conf dential information before discarding them into the trash.

Step Two. Prepare and implement updated policies and agreements with employees having access to conf dential and proprietary information, such as:

(a) Conf dentiality Agreements. Such agreements require employees to acknowledge that they will have exposure to certain company conf dential and proprietary information during the course of their employment, and prohibits the employee from any unauthorized use or disclosure of this information. These agreements further require employees to return any conf dential or proprietary information upon separation from employment.

(b) Non-Solicitation Agreements. Such agreements generally prohibit departing employees from soliciting the company's customers and clients. These agreements also limit the employee's right to solicit company employees to leave the company. Non-solicitation agreements, like non-compete agreements, must be reasonable in their scope and duration to protect the company's conf dential information.

(c) Non-Compete Agreements. Such agreements generally prohibit departing employees from entering into competing enterprises with their former employer. These agreements also contain acknowledgments by the employee about the company's proprietary information and detail employee's obligations upon re-employment.

Continued on back page...

(d) Inventions Agreement. Such agreements generally contain the employee's assignment to the employer of any interest the employee may claim in intellectual property created by the employee while employed by company.

(e) General Employment Policies. Such policies, typically included in a company's personnel manual, may address a number of important issues, such as protocol for use of company equipment, storing of company data, reproduction and use of company data, and each employee's responsibilities in maintaining proprietary company data.

Given that most states, including New York, have a policy bias against restricting an individual's right and freedom of employment, it is important that the agreements discussed above be drafted to tailor the company's specif c needs. General agreements limiting solicitation and competition, often found f oating around the internet and used by many companies, are frequently invalid because of their failure to comply with evolving state law requirements and because they impose unreasonable restrictions on the employees' rights. Extreme caution is advised when relying upon such standardized documents. If properly tailored to protect a company's legitimate business interest, such agreements can and will be enforced by the courts.

Step Three. Ensure the implementation of appropriate security policies. From the date of hire through the date of termination, HR and technology practices and policies must be followed to ensure that the data remains conf dential and will subsequently be protected by the court in the event of an unlawful theft. Employees should be educated not simply on the company's policies and be required to sign the appropriate acknowledgments and agreements, but training classes should be provided on protocols for maintaining company data as proprietary. Such meetings, can train employees on how to handle and store the company's proprietary information, and can also serve to reinforce the company's policies and practices. Employees can often be an employer's f rst line of defense in minimizing unintended leaks or theft of the conf dential data.

Step Four. At the time of an employee's separation from employment, much can be done to protect a company's interests. Too often, employers simply rush the exit of a terminated employee, rather than take the opportunity to conduct some important reviews. For example, companies should analyze their technology systems to discover whether a departing employee has attempted to copy or remove conf dential data. A review of an employee's activity in the weeks or months prior to their departure may reveal inappropriate activity. Access to computer systems should be revoked to not only avoid theft, but sabotage. During an exit interview, employees can be provided with copies of their signed agreements and company policies and be required to return any company property in their possession. Companies should use a checklist to ensure that nothing is missed, and request that employees sign documents acknowledging that they have returned all company property.

In conclusion, employee theft is no doubt a real cause for concern by companies whose conf dential and proprietary information is valued. To avoid the theft of this information, employers have concrete options for protecting their assets. By adopting and implementing appropriate policies and agreements, employers can minimize their risk of employee theft of proprietary data.

If Green & Seifter, Attorneys, PLLC, can provide you with additional insight and information regarding protecting your company's proprietary information, please contact **John L. Valentino.** John Valentino is a Managing Member of **Green & Seifter, Attorneys, PLLC, (www.gslaw.com)**and concentrates his practice in the areas of Business Transactions and Employment Law. He can be reached at **jvalentino@gslaw.com or (315)701-6308**.

John L. Valentino
Green & Seifter, Attorneys, PLLC
110 West Fayette Street
One Lincoln Center, Suite 900
Syracuse, NY 13202
(315) 701-6308 or
jvalentino@gslaw.com