MAY 2009, VOL. 46, NO. 4

ILLINOIS STATE BAR ASSOCIATION

LABOR & EMPLOYMENT LAW

The newsletter of the ISBA's Section on Labor & Employment Law

Preventing the misappropriation of trade secrets through proactive policies and procedures

By Peter A. Steinmeyer[1]

In this high-technology era, where a company's most valuable assets are frequently its people and information and where the equivalent of thousands of pages of documents can be copied and moved with a few keystrokes, attorneys are increasingly being asked to stop the misappropriation of confidential information and trade secrets by employees and rival businesses. While there is no magic wand that will prevent a theft or stop a thief in his tracks, a company can substantially lower the risk of trade secret misappropriation through proactive policies and procedures.

What is a trade secret?

Under the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.* ("ITSA"), a "trade secret" is defined as:

> information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known 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 or confidentiality.

765 ILCS 1065/2(d).

In addition to ITSA's requirements, Illinois courts often consider the following common-law factors to determine if information constitutes a "trade secret": (i) the extent to which the information is known outside of the plaintiff's business; (ii) the extent to which the information is known by employees and others involved in the plaintiff's business; (iii) the extent of measures taken to guard the secrecy of the information; (iv) the value of the information to the plaintiff's business and to its competitors; (v) the effort and money expended in developing the information; and (vi) the ease or difficulty with which the information could be properly acquired or duplicated by others. *Liebert Corp. v. Mazur*, 357 Ill. App. 3d 265, 276-277, 827 N.E.2d 909, 921-922, 293 Ill. Dec. 28, 293 Ill.Dec. 28 (1st Dist. 2005).

A court's analysis of whether a company took "reasonable" steps to safeguard its trade secrets requires a "balancing of costs and benefits that will vary from case to case." *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179 (7th Cir. 1991). In one case decided by the Seventh Circuit, the Court held that a mere "oral confidentiality agreement" was sufficient under ITSA, even though it was "unwise in hindsight." *Learning Curve Toys, Inc. v. Playwood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003). In so ruling, the Seventh Circuit explained that, "as part of the reasonableness inquiry, the jury could have considered the size and sophistication of the parties, as well as the relevant industry." *Id.* at 726.

Examples of trade secrets include customer lists and data, pricing and discounting information, marketing or business strategies, financial plans or data, product formulas, blueprints, and training manuals.

Information that qualifies as a "trade secret" under ITSA is entitled to extra protections

Although information which does not meet the statutory definition of a "trade secret" is still legally protectible information (*i.e.*, employees are not free to steal it, and can be sued under a variety of common law theories if they do), ITSA makes it easier to obtain injunctive relief by expressly authorizing injunctive relief to prevent actual or threatened misappropriation of trade secrets. *See* 765 ILCS 1065/3. *See also, Illinois Bell Tel. Co. v. Lake County Grading*, 313 Ill. App. 3d 184, 189, 728 N.E.2d 1178, 1181, 245 Ill. Dec. 821 (2nd Dist. 2000) ("[W]here a statute expressly authorizes injunctive relief, a plaintiff need only show defendant's violation of the Act and that plaintiff has standing to pursue the cause. The general rules of equity requiring a showing of irreparable injury and a lack of an adequate remedy at law need not be shown." (internal citations omitted))

Moreover, under ITSA, "[i]f neither damages nor unjust enrichment caused by the misappropriation are proved by a preponderance of the evidence, the court may award damages caused by misappropriation measured in terms of a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret." 765 ILCS 1065/4. ITSA further provides for exemplary damages and attorney fee awards in cases of willful and malicious misappropriation. *See* 765 ILCS

1065/4 and 765 ILCS 1065/5.

What should an employer do to protect its trade secrets and other confidential information?

Given that not every situation requires a "Fort Knox" level of protection, what should a reasonable employer do to protect its trade secrets and other confidential information?

First, every employer should set forth a confidentiality policy in its employee handbook or elsewhere, and that policy should advise employees of their confidentiality obligations. It should define what is confidential (many employees legitimately may not know) and it should state that all confidential information or other company property, in whatever form (*i.e.*, paper or electronic), is to be returned at termination and never disclosed to a third party without proper authorization. Employees should be required to sign an acknowledgement of their receipt of the handbook or policy, and the acknowledgement should also set forth the employee's agreement to be bound by the policy.

Second, electronic documents, files and information should be stored on a password-protected computer system.

Third, to the extent possible, access to trade secrets and confidential information should be limited to those with a "need to know." Not everyone needs access to client lists, product formulas, marketing and business strategies, and the like. For example, although a salesperson may need data regarding his territory, he may not need access to data from other territories. Apportion knowledge and access on a "need to know" basis.

Fourth, with respect to persons with access to particularly sensitive information, a confidentiality agreement and/or a post-employment restrictive covenant should be considered. In that regard, under Illinois law, the need to prevent an employee from using the employer's trade secrets or other confidential information for his own benefit or that of a new employer is sufficient justification for a post-employment non-competition or non-solicitation agreement. *Arpac Corp. v. Murray et al.*, 226 Ill. App.3d 65, 72-73, 589 N.E.2d 640, 647 (Ill. App. 1 Dist. 1992).

Fifth, shredding confidential documents, rather than merely throwing them away, is always prudent, as is labeling certain documents such as customer lists "confidential."

Sixth, employers should conduct an exit interview with a departing employee and, at that interview, not only should the departing employee be reminded of his obligation to maintain the confidentiality of the employer's trade secrets and other confidential information, he should also be specifically asked to confirm that he has returned all of the employer's property and information in whatever form (*i.e.*, paper or electronic) in which it is maintained. Ideally, he would also be asked to sign a certification that he has done so. Not only does the act of signing such a certification reiterate the importance of the employee's confidentiality obligation, should that certification later prove false (*i.e.*, if it is later determined that the employee in fact misappropriated trade secrets), the false certification will be a critical piece of evidence in showing reasonableness by the employer and maliciousness by the former employee.

Seventh, if an employee is departing under suspicious circumstances, or if there is other reason to suspect possible misappropriation of trade secrets, records of the employee's computer activity in the days and weeks leading up to his termination should be preserved (*e.g.*, by preserving the employee's e-mails and making a forensic image of the employee's hard drive). Litigation over trade secret misappropriation frequently turns on evidence of unusual computer activity shortly before a departure.

Finally, employers should periodically inventory their trade secrets and also perform self-audits of all of their practices and procedures regarding trade secrets (*e.g.*, review their employee handbooks, confidentiality policies and procedures, non-disclosure agreements, and restrictive covenants) to ensure that they are appropriate under the circumstances and compliant with applicable laws.

Conclusion

Different employers have different needs with respect to the protection of their trade secrets and confidential information, and reasonable precautions for one employer might be completely unreasonable for another. However, regardless of the size or nature of the business, virtually every employer has trade secrets or other confidential information, and every employer can and should proactively take appropriate measures to protect those assets. Such proactive steps not only help to prevent trade secret misappropriation, they also increase the likelihood that a court will deem such information a trade secret entitled to the heightened protections of ITSA.

---

1. Peter A. Steinmeyer is a Member of the Chicago office of Epstein Becker & Green, P.C., where he concentrates on employment litigation and advice and counsel with respect to employment issues. He is Co-Chair of the Firm's Non-Competes, Unfair Competition and Trade Secrets Practice Group.

Reprinted with permission from the
Illinois State Bar Association's
Labor & Employment Law newsletter,
Vol. 46 #4, May 2009.

www.isba.org