EPSTEIN BECKER GREEN

Take 5: Views You Can Use - August 2012

August 22, 2012 | Publications

People

Peter (Pete) A. Steinmeyer
Member of the Firm
Trade Secrets & Employee Mobility
Chicago
312-499-1417
psteinmeyer@ebglaw.com

This issue of **Take 5** *was written by Peter Steinmeyer, a Member of the Firm and the Managing Shareholder of Epstein Becker Green's Chicago office. He is also the Co-Chair of the firm's Non-Competes, Unfair Competition and Trade Secrets Practice Group.*

Along with a most unexpected first-place run by the Chicago White Sox, summer 2012 brought a number of significant developments in the area of noncompetes and trade secrets. Here are five pieces of advice based on these recent developments.

1. Carefully review computer use policies as a result of the continuing judicial split on the federal Computer Fraud and Abuse Act.

Common scenario: An employee plans to resign from an employer and join a competitor. Prior to resigning, the employee uses his company computer to access confidential and proprietary information and then sends the information to his personal email account to use for the benefit of his new employer. The employer sues the former employee for misappropriation and other state law claims, and seeks federal jurisdiction by asserting a claim under the Computer Fraud and Abuse Act ("CFAA").

Dilemma: Does the CFAA protect the employer if the employee had permission to "access" the computer and company documents but not "use" them for an improper purpose, such as to benefit a new employer?

Just a few weeks ago, the U.S. Court of Appeals for the Fourth Circuit entered the fray over the scope of liability under the CFAA by adopting a narrow view of the statute. In *WEC Carolina Energy Solutions LLC v. Miller*, No. 11-1201 (4th Cir. July 26, 2012), a former employee of WEC Carolina Energy Solutions LLC ("WEC") allegedly downloaded confidential information while still employed by WEC but prior to his resignation to work for a competitor, and then used that information unlawfully to compete against WEC on behalf of his new employer. WEC claimed that the former employee's unauthorized "use" of its computers to gain access to proprietary information violated the CFAA's "without authorization" or "exceeds authorized access" provisions. The trial court dismissed the complaint for failing to state a claim under the CFAA, and the Fourth Circuit affirmed.

In affirming the dismissal, the Fourth Circuit adopted "a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and held that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which is authorized to access."

The Fourth Circuit joined the Ninth Circuit in its narrow reading of the CFAA, in contrast to the more expansive view held by certain other circuit courts of appeals, including the Seventh Circuit. Due to this split in the courts of appeals, this critical issue of liability under the CFAA will eventually end up before the Supreme Court of the United States.

In the meantime, employers should carefully review their computer use policies to determine whether such policies could be used effectively to limit unauthorized access and use.

2. Beware of state laws banning employers from requesting social media passwords from employees and applicants.

Following the lead of Maryland, Illinois recently became the second state to enact a law banning employers from requesting or requiring disclosure of employee or applicant passwords for social media accounts.

- Despite this limitation, the law does not prevent an employer from doing the following:
- Maintaining policies governing the use of the employer's electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use;
- Monitoring an employee's work email account or the usage of the employer's electronic equipment; and

Accessing information about employees and job applicants that is in the public domain and not password protected.

Other states have proposed similar legislation. Accordingly, this is an issue for employers to follow, particularly those with multistate operations.

3. Pay careful attention to how a corporate transaction may affect an employee's noncompete agreement.

Earlier this summer, the Ohio Supreme Court held that when a company that was the original party to a noncompete agreement merged into another company, unless the noncompete agreement contained a "successors and assigns" clause, the merger was a termination of employment, which triggered the running of the restrictive period in the noncompete.

Although the Ohio Supreme Court recently voted to reconsider this decision, the original decision illustrates the importance of including "successors and assigns" verbiage in a noncompete agreement. It also illustrates the attention that should be placed on the enforceability of a noncompete following a corporate transaction, and whether it may be prudent for an acquiring corporation to have its new employees sign fresh noncompete agreements.

4. Be careful when prosecuting trade secret misappropriation claims without objective evidence of actual misappropriation.

Starting and continuing the prosecution of a misappropriation of trade secrets action without objective evidence of actual misappropriation can result in the imposition of attorneys' fees against the plaintiff. On April 17, 2012, we wrote on the Trade Secrets & Noncompete Blog about this issue in connection with a malicious prosecution action that was filed against Latham & Watkins after the unsuccessful prosecution of a trade secrets action on behalf of a client.

On July 11, 2012, in *SASCO v. Rosendin Electric, Inc.*, 2012 WL 2826955 (Cal.App. 4 Dist.), the California Court of Appeal, Fourth Appellate District, provided more clarity on this issue and affirmed the trial court's order awarding defendants almost $485,000 in attorneys' fees and costs pursuant to California Civil Code § 3426.4 (the Uniform Trade Secrets Act).

As reflected in the *SASCO*decision, if an employer is presented with evidence that no misappropriation occurred and continues to prosecute the case and loses or dismisses the case, it may be faced with an attorney fee demand from the defendant.

5. Keep an eye out for federal trade secrets protection.

On July 17, 2012, the "Protecting American Trade Secrets and Innovation Act of 2012" was introduced in the U.S. Senate by Democratic Senator Herb Kohl of Wisconsin.

The proposed law would authorize federal judges to issue emergency orders, without prior notice to any other party, allowing the seizure of property used or intended to be used for trade secret misappropriation. It would also provide for other civil relief similar to that available in most states under their respective versions of the Uniform Trade Secrets Act.

Any complaint filed under the proposed law would have to include a "sworn representation" that the dispute involves a "substantial need for nationwide service of process" or a "misappropriation of trade secrets from the United States to another country."

Resources

2012-08-Take-5-Newsletter-Peter-SteinmeyerDownload