SEYFARTH SHAW LLP
ATTORNEYS

Management Alert

2012 Trade Secrets Webinar Series - Year in Review

Throughout 2012, Seyfarth Shaw LLP's dedicated Trade Secrets, Computer Fraud & Non-Competes Practice Group hosted a series of CLE webinars that addressed significant issues facing clients today in this important and ever changing area of law. The series consisted of eight webinars:

1) Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff;
2) Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing;
3) Pleading, Providing and Protecting Trade Secrets in Litigation;
4) Protecting Your Trade Secrets in the Financial Services Industry;
5) When Trade Secrets Cross International Borders;
6) Trade Secrets and Non-Compete Legislative Update;
7) Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours; and
8) 2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law.

As a conclusion to this well-received 2012 webinar series, we compiled a list of key takeaway points for each of the webinars, which are listed below. For those clients who missed any of the programs in this year's webinar series, the webinars are available on CD upon request or you may click on the title below of each webinar for the online recording. CLE credit is available as discussed below. We are also pleased to announce that Seyfarth will continue its trade secrets webinar programming in 2013 and has several exciting topics lined up. We will release the 2013 trade secrets webinar series in the coming weeks.

Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff

The first webinar of the year, led by Seyfarth partners Gary Glaser and Scott Schaefers, addressed the issue of employees' privacy rights on their work computers; unauthorized use or disclosure of company intellectual property while using social media; and the Computer Fraud and Abuse Act (CFAA).

- To have the best chance of seeking remedies under the federal CFAA, only give employees access to company networks on a need-to-know basis. Require all employees with access to confidential company information to sign confidentiality and restricted access and use agreements. Have clear written policies in place that leave no doubt that any access and use of company information, for purposes other than company business, is strictly prohibited, and have employees acknowledge receiving copies of such policies. Send out periodic reminders of those policies, each of which should require acknowledgement of receipt by the employees.

- Do NOT attempt to access an employee's personal e-mails, files or Internet accounts without advice of counsel. Under both federal and many state laws, employees often have privacy rights in their personal information, even if they store it or access it on company computers.
- For social networking sites (e.g., LinkedIn), have clear written policies that spell out what company information may/may not be posted on such sites, and identify what information belongs to the company (e.g., contact lists, company photos or graphics, etc.), as well as a process for purging the company-owned information from their contact lists posted on social networking sites such as LinkedIn at the time the employee departs. An exit interview should also be conducted at the time any employee separates, and as part of that exit interview process, each exiting employee should be given a written reminder of their ongoing trade secret, confidentiality and social networking obligations. If an employee leaves the company without such clear written direction, the company risks waiving any proprietary interest in the information in his/her LinkedIn profile. Also consider using ownership agreements that specify that the company owns the particular social media accounts that the employee may work on and remember to obtain the password from the employee to the company owned social media account before the employee leaves.

Employee Theft of Trade Secrets or Confidential Information in The Name of Protected Whistleblowing

In our second webinar of the series, Seyfarth partner Robert Milligan answered the question, "Can employees steal trade secrets and confidential information to support their whistleblower claims?" This program covered recent decisions addressing the interplay between maintaining employer confidentiality and protection of trade secrets and protected activity under whistleblower statutes and "self-help" discovery, as well as the provisions in whistleblower bounty programs that preclude enforcement of confidentiality agreements in certain instances.

- A central goal of Sarbanes-Oxley is the accurate valuation and protection of a company's assets. But what does this mean for trade secrets, which have traditionally been thought of as an undefined intellectual property right? Sarbanes-Oxley has mandated duties of disclosure and internal controls that have transformed trade secrets into an asset that must be valued and reported.
- At a minimum, companies should create a trade-secret protection committee or have a corporate officer whose job it is to identify, value, and protect trade secrets. However, doing so requires an understanding of 1) what a trade secret is, 2) where one finds a trade secret, and 3) how to appropriately protect a trade secret. The key is to identify, inventory and value as well as institute internal controls to protect trade secrets. Seyfarth has extensive experience assisting companies with this process and offers an effective and well-received *trade secret audit program*.
- Section 922 of the Dodd-Frank Act prevents any person from interfering with a whistleblower's report, including by threatening to enforce confidentiality agreements. Whistleblower thieves may seek revenge by making confidential information public in addition to bringing it before the SEC. Companies must act swiftly to have genuine confidential or trade secret information removed from public mediums, such as the Internet, to attempt to preserve its secrecy. New whistleblower rules may decrease incentives to follow internal reporting procedures and instead provide a perverse incentive for sham employees to work for bounties rather than fulfill their employment obligations. Careful planning should be done to make good hiring decisions as well as employing effective performance management of existing hires to attempt to manage the risk of the retention of rogue and disloyal servants.
- Consider these strategies to protect trade secrets and confidential information when faced with a whistleblower thief:
    - ✔ Make sure you have a clear anti-retaliation policy and document investigation. Follow your corporate compliance programs and ethics policies and procedures.

- Be careful in all communications with the whistleblower. Do not make him or her feel threatened. Try to find an employee that the whistleblower thief trusts to get back company documents.
- Consider engaging a third-party neutral to maintain confidential documents and information if the whistleblower has not yet gone to the SEC.
- Consider amnesty negotiations. Remind the whistleblower of the serious legal consequences of stealing trade secret and confidential information.
- Offer to study the problem internally and report to the SEC.
- Move swiftly to attempt to obtain the removal of any confidential or trade secret documents from the Internet by working with Internet service providers to obtain the immediate takedown and involve the court as needed.

Pleading, Proving and Protecting Trade Secrets in Litigation

The third installment in the 2012 Trade Secrets Webinar Series was presented by trade secrets practice leader Michael Wexler. Many courts require that claims for trade secret misappropriation be pled specifically as to the nature of the trade secret or suffer the consequences of challenges to the pleadings. The challenge is to plead with reasonable particularity without actually disclosing the secrets in a public document. From a defense stand point, the identity of the trade secret is paramount to prepare defenses, determine the value of the secrets, and determine if they were actually misappropriated. This webinar covered the ethical, technical and practical aspects of initial pleadings that are fundamental to the filing and defending of trade secret claims.

- In any trade secrets litigation in which you represent the plaintiff, you must have a frank discussion with your client prior to the inception of the litigation concerning its duties to identify the alleged misappropriated trade secrets with specificity and the resulting discovery disclosure that will be required in the litigation. Simply put, the client needs to know that counsel for the defendant(s) (at a minimum) will be provided access to the allegedly purloined trade secret as well as others. Depending upon the state and occasionally the individual judge, the defendants may also be able to obtain access to the stolen trade secrets subject to a protective order so that they can defend themselves against the claim. A plaintiff must be mindful that their secrets may be further disclosed to a competitor during trade secret litigation subject to non-disclosure obligations and that plaintiff must vigorously defend and protect the confidentiality of said information throughout the litigation.
- A majority of states either by statute or case law require that a plaintiff disclose their trade secrets with specificity as part of the discovery process. Failure by the plaintiff to provide sufficient specificity regarding the stolen trade secret in discovery may result in a defendant obtaining summary judgment on the claim. Some states require the plaintiff to provide a specific trade secret disclosure document before discovery commences. See California Code of Civil Procedure section 2019.210.
- Protective orders in trade secret litigation must be carefully tailored to protect confidential information disclosed in discovery and limit the disclosure of such information to those who need to know for purposes of the litigation. A protective order should have appropriate measures concerning how documents containing confidential information will be provided to the court, witnesses, and experts. Careful consideration should also be made on whose burden it is to justify the protection level assigned to particular documents.
- Plaintiffs should use contention interrogatories to flesh out any allegations made by the defendant(s) that particular alleged trade secrets are in the public domain. Written discovery should probe the basis of such allegations, including when and where such disclosure occurred.

Protecting Your Trade Secrets in the Financial Services Industry

The fourth webinar in the series, presented by partners Scott Humphrey and James McNairy, focused on trade secret considerations in the banking and finance industry, including prosecuting claims against former employees who are FINRA members.

- When seeking injunctive relief in a trade secrets dispute involving parties that are subject to FINRA regulation, be sure to first consult FINRA (NASD) Rule 13804 governing injunctive relief—while the moving party may first seek injunctive relief from a court of competent jurisdiction, the party must also make specified filings with FINRA.
- When litigating a trade secret dispute before FINRA, keep in mind that the FINRA process is often less formal than in court, and the arbitration panel may include persons who are not lawyers. Thus, it behooves both parties to keep their legal arguments concise and, where complex trading algorithms or other complex trade secrets are at issue, the trade secret should be described as simply as possible.
- When the FINRA trade secret dispute arises out of facts involving broker recruitment, the parties should be aware of the 2004 "Protocol for Broker Recruiting," which currently has well over 400 signatories and allows brokers to take to their new employer certain account information. Other limitations within the protocol should also be carefully considered before filing suit.

When Trade Secrets Cross International Borders

Our fifth webinar in the 2012 series was presented by Robert Milligan, Marjorie Culver and Matthew Werber and provided a high-level discussion of recent non-compete and trade secret issues that impact foreign companies conducting business in the United States and companies operating internationally. This program provided an overview of the key considerations that foreign companies should appreciate in order to effectively navigate trade secret and non-compete law in the U.S. and highlighting the issues facing U.S. trade secret owners attempting to address the theft of stolen trade secrets abroad. This webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these jurisdictions to ensure they are adequately protecting their trade secrets.

- In many U.S. states, initial employment and continued employment can be sufficient consideration for non-compete, non-solicitation and non-disclosure agreements, whereas in several European countries, the employer must pay for any post-termination non-compete. In contrast to the law in some foreign countries, employers can still enforce the non-compete even if the employer terminates the employment relationship in some U.S. states. Injunctive relief is typically the top litigation goal in most U.S. trade secret/non-compete matters. There are significant differences in U.S. states concerning the interpretation of the Uniform Trade Secrets Act (which has been adopted in 46 U.S. States). For example, there are significant differences regarding the application of the inevitable disclosure doctrine, trade secret preemption and recoverable damages.
- Cross-border considerations: employers must be vigilant and think critically about the most likely venue that a non-compete/trade secret battle will occur should an employee later leave the company as forum and choice of law can be outcome determinative. Employers should carefully select employees for cross-border coverage, taking into consideration where the work will likely be performed, where the employee will likely reside, what jurisdiction/choice of law is most favorable, and the likely chance of successful enforcement. The employer should draft to the highest standard based upon the likely locale of any dispute concerning the non-compete.
- Trade secret holders seeking to remedy misappropriation occurring abroad should consider the United States International Trade Commission (ITC) as a potential forum for seeking relief. In *TianRui Group Co., Ltd. v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011), the Federal Circuit ruled that the ITC can exercise its jurisdiction over acts of misappropriation occurring entirely in China so long as the dispute concerns products being imported into the United States.

Trade Secrets and Non-Compete Legislative Update

The sixth webinar of the year, led by Robert Stevens, Erik Weibust, and Daniel Hart, focused on new and pending legislative changes to non-compete and trade secrets statutes, including a review of Georgia's Revised Restrictive Covenant Act one year after its enactment, recent and pending legislative changes to non-compete statutes in New Hampshire and Massachusetts, adoption of the New Jersey Uniform Trade Secrets Act, and pending legislative changes to trade secrets statutes in Idaho and at the federal level.

- To the extent that they have not already done so, employers operating in Georgia should have their non-compete agreements evaluated by counsel to ensure that they are taking full advantage of the change in Georgia public policy toward enforcement of restrictive covenant agreements, which permits courts to blue pencil overbroad agreements and which only applies to agreements signed after May 11, 2011.
- Employers operating in New Hampshire should ensure compliance with the new statutory requirement of disclosing non-compete and non-piracy agreements to employees prior to making an offer of employment or an offer of change in job classification, while employers operating in Massachusetts should stay abreast of proposed legislation that, if enacted, could make enforcement of restrictive covenants more difficult in Massachusetts. Please see *our chart* that summarizes the various iterations of the proposed legislation.
- In light of New Jersey's adoption of the Uniform Trade Secrets Act and proposed legislation in Idaho and at the federal level, trade secrets law is slowly moving toward greater uniformity. In light of the continually developing statutory landscape, employers operating anywhere in the United States should continue to ensure that they have taken reasonable measures to protect their trade secrets, by, among other steps, limiting access to trade secrets to employees with a need for such access, providing password protections on documents, encrypting data, limiting the ability of employees to remotely print highly sensitive documents, and enacting vigorous restrictive covenant agreements in jurisdictions where such agreements are permitted.

Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours

The seventh webinar in our series, presented by Michael Wexler, Robert Milligan and Joshua Salinas, discussed best practices when dealing with newly hired or departing employees and the incumbent trade secret, non-competition and information protection issues.

- During the job interview of a competitor's employee, remember to 1) discuss general skills and talents, not the former employer's customers or trade secrets; 2) control the interview and put the employee at ease; 3) make clear that the employee should not, under any circumstances, use or bring any of his employer's information or solicit any former co-workers; 4) focus on making the transition as smooth as possible for the former employer; and 5) check if the employee has any existing agreements with former employers before making an offer.
- Key agreements/provisions/policies that companies should have with their employees: 1) non-disclosure and trade secret protection agreements; 2) non-solicitation of employee agreements/provisions; as permitted by law 3) agreements/provisions relating to former employer's trade secrets (don't use or disclose and do not bring to premises); 4) computer use and access provisions/agreements; 5) social media ownership agreements and policies; and 6) invention assignment agreements.

- The exit interview process with departing employees is key. Employers should:
    - ✔ Prepare for the interview, identify the trade secret and confidential information the employee accessed/used, consider having in-house counsel or HR and employee's manager present
    - ✔ Question the departing employee in detail.
    - ✔ Ask the employee why he/she is leaving.
    - ✔ Ask the employee what his/her new position will be.
    - ✔ Check the employee's computer activities and work activities in advance of the meeting.
    - ✔ Ensure that all Company property, hardware, and devices have been returned, including e-mail and cloud data, and social media accounts; consider using an inventory list.
    - ✔ Ensure that arrangements are made to have all company data removed from any personal devices, accounts, storage areas.
    - ✔ Disable access to company computer networks.
    - ✔ Make sure you obtain user names and passwords for all company social media accounts.
    - ✔ Inform the employee of his continuing obligations under agreements with the Company.
    - ✔ Consider letter to new employer and employee with reminder of continuing obligations.
    - ✔ Consider having departing employee's emails preserved and electronic devices forensically imaged.
    - ✔ Consider using an exit interview certification.

2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law

In Seyfarth's final installment of its 2012 Trade Secret Webinar series, Seyfarth attorneys James McNairy, Joshua Salinas and Jessica Mendelson reviewed noteworthy California cases and other legal developments in the increasingly hot areas of trade secret protection, the preemptive effect of the California Uniform Trade Secrets Act, California's hostility to non-competition and non-solicitation agreements, the continued erosion of the Computer Fraud and Abuse Act as a tool for California employers to curb data theft, and social media's influence on how organizations identify and protect confidential information.

- Clearly define company social media policies before problems arise. Avoid restricting employees' abilities to discuss the terms and conditions of their employment, wages, and other activities protected under Section 7 of the National Labor Relations Act. Employers who make use of social media accounts should consider using contracts to state clearly that the employer owns the accounts, which are to be used only for authorized purposes, but that do not overreach into areas that violate employee rights to privacy.
- Companies should ensure their computer and network policies cover "access," not merely "use," to comply with the Ninth Circuit's narrow interpretation of the CFAA. Access should be defined clearly to delineate functionally what computer resources and information employees permissibly may and may not access, with data repositories containing sensitive information requiring enhanced access restrictions.
- To fall under California Business and Professions Code section 16601's "sale of business" exception, non-competition covenants executed pursuant to the sale of a business should be incorporated into the terms of the purchase agreements and reflect a clear purpose to protect business goodwill.

- Because preemption under California's Uniform Trade Secrets act is increasingly invoked by defendants as a basis to dismiss claims related to the taking of trade secret information, it is imperative that potential plaintiffs carefully plead non-trade secret claims as distinct from the trade secret allegations within the complaint. Failure to do so can cause related claims to be preempted and, if the trade secret claim itself is faulty, significantly reduce the number of at issue claims.
- Create a culture of confidentiality within your company so that at every turn employees are aware of the importance of protecting confidential, proprietary, and trade secret information and the steps required of all employees to protect the company's information assets. Doing so may enable your organization to invoke the trade secrets exception to California Business and Professions Code section 16600, which may help protect company information assets and moderate high employee mobility in California.

2013 Trade Secrets Webinar Series

Beginning in January 2013, we will begin another series of trade secret webinars. The first webinar of 2013 will be a national year in review on the most important cases and developments throughout the country concerning trade secrets, non-competes, and computer fraud. To receive an invitation to this webinar or any of our future webinars, please sign up for our Trade Secrets, Computer Fraud & Non-Competes mailing list by clicking *here*.

For attorneys licensed in Illinois, New York or California, who are interested in receiving CLE credit for viewing recorded versions of the 2012 webinars, please e-mail *CLE@seyfarth.com* to request a username and password. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are also happy to discuss with you presenting similar presentations to your groups for CLE credit.

If you have any questions, please contact *Michael Wexler* at *mwexler@seyfarth.com*/(312) 460-5559, *Robert Milligan* at *rmilligan@seyfarth.com*/(310) 201-1579, the Seyfarth Shaw attorney with whom you work or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (*www.seyfarth.com/tradesecrets*). You may also access our blog, Trading Secrets, at *www.tradesecretslaw.com*.