SEYFARTH SHAW

Management Alert

2016 Trade Secrets Webinar Series Year in Review

Throughout 2016, Seyfarth Shaw'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 11 webinars:

1. 2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Data Security and Trade Secret Protection for Lawyers
3. New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive
4. Protecting Confidential Information and Client Relationships in the Financial Services Industry
5. Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?
6. The Defend Trade Secrets Act: What Employers Should Know Now
7. Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements
8. International Non-Compete Law Update
9. The Intersection of Trade Secrets Violations and the Criminal Law
10. Trade Secret Audits: You Can't Protect What You Don't Know You Have
11. Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches

As a conclusion to this well-received 2016 webinar series, we compiled a list of key takeaway points for each program, which are listed below. For those clients who missed any of the programs in this year's series, the webinars are available on CD upon request, or you may click on the title of each webinar for the online recording. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your groups for CLE credit. Seyfarth will continue its trade secrets webinar programming in 2017, and we will release the 2017 trade secrets webinar series topics in the coming weeks.

2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law

The first webinar of the year, led by Robert Milligan, Jesse Coleman, and Joshua Salinas, reviewed noteworthy cases and other legal developments from across the nation in the areas of trade secret and data theft, non-compete enforceability, computer fraud, and the interplay between restrictive covenant agreements and social media activity, and provided

predictions for what to watch for in 2016.

- Data breach is a question of when and not if. Companies should ensure they have implemented sufficient information security policies and a data breach response plan. There are limitations in the law and challenges in international misappropriation cases. The best strategy is to try to prevent breach and misappropriation through effective policies, procedures, and agreements, employee training, technology solutions, and continual assessment and improvement.

- Courts continue to struggle with issues regarding adequacy of consideration for restrictive covenants. Employers who have asked existing employees to sign non-competes or are considering doing the same should evaluate whether consideration was or will be provided for the non-compete to ensure enforcement under applicable law.

- While the circuit court split continues to widen regarding the interpretation of unauthorized access under the Computer Fraud and Abuse Act, the recent decision in *U.S. v. Christensen* (9th Cir. 2015) may provide employers with a civil cause of action in California against employees who misuse company data without permission.

Data Security & Trade Secret Protection for Lawyers

In recent years, the prevalence of data and information security breaches at major corporations have become increasingly more commonplace. While general awareness may be increasing, many companies are still neglecting to address serious information security issues.

In the second installment, Seyfarth attorneys Richard D. Lutkus and James S. Yu were joined by Joseph Martinez, Chief Technology Officer and Vice President of Forensics at Innovative Discovery. This program covered considerations that attorneys should take into account when in possession of any client data. Coverage included both technical considerations, best practices and policies, as well as practical advice to steer clear of ethical violations.

- Whether corporate or outside counsel, there are basic steps that can dramatically increase the security of your or your client's data. Management of data will continue to be a necessity for any entity. Proper policies, protocols, and training should be developed and put into place to protect data in transit and at rest. Use of encryption and access control are both key to proper protection of data.

- Social engineering is the number one cause of data breaches, leaks, and information theft. Organizations should alert and train employees on following policy, spotting potential social engineering attacks, and having a clear method to escalate potential security risks. Employee awareness, coupled with technological changes towards better security will reduce risk and exposure to liability.

- Lawyers have an ethical duty to ensure that reasonable steps are taken to protect their client's and employer's data. Significant statistics have shown that many law firms and practitioners are behind the curve in terms of information security preparedness. Hackers have recently focused their targets on the lax security practices of law firms to obtain client data or inside information.

New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive

In Seyfarth's third installment of its 2016 Trade Secrets Webinar series, Seyfarth attorneys Robert Milligan, Justin Beyer, and Daniel Hart provided attendees with a thorough discussion of the fundamentals as well as updates of the Defend Trade Secrets Act (DTSA) and the proposed EU Trade Secrets Directive. The panel gave insight into the limitations and new benefits of the Act and the proposed Directive.

- With the passage of the Defend Trade Secrets Act, there is now a federal cause of action for trade secrets disapproval. Some of the key provisions in the Act include a three year statue of limitations, the availability of attorneys' fees, exemplary damages, as well as increased criminal penalties for a violation of the Economic Espionage Act. It also includes

portions of the DTSA as predicate offenses for the RICO Act.

- The Act also contains language requiring that an employer include information relating to whistleblower immunity for employers to obtain exemplary damages. This only underscores an important point to anyone maintaining employment agreements which contain restrictive covenants: it is imperative for employers to monitor applicable state and federal law to best preserve and maintain their rights and employment agreements.

- The European Commission's directive on trade secret protection will mark a sea-change in protection of trade secrets throughout the European Union. Each of the EU's 28 member states will have a period of 24 months to enact national laws that provide at least the minimum levels of protections afforded to trade secrets by the directive. Look for greater consistency in trade secrets protection throughout the European Union in the years ahead.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

Seyfarth's fourth installment, presented by Scott Humphrey, Marcus Mintz, and Kristine Argentine, focused on trade secret and client relationship considerations in the banking and finance industry, with a particular focus on a firm's relationship with its FINRA members.

- Enforcement of restrictive covenants and confidentiality obligations for FINRA and non-FINRA members are different. Although FINRA allows a former employer to initially file an injunction action before both the Court and FINRA, FINRA—not the Court—will ultimately decide whether to enter a permanent injunction and/or whether the former employer is entitled to damages as a result of the former employee's illegal conduct.

- Address restrictive covenant enforcement and trade secret protection before a crisis situation arises. An early understanding of the viability of your company's restrictive covenants and the steps your company has taken to ensure that its confidential information remains confidential will allow your company to successfully and swiftly evaluate its legal options when a crisis arises.

- Understand the Protocol for Broker Recruiting's impact on your restrictive covenant and confidentially requirements. The Protocol significantly limits the use of restrictive covenants and allows departing brokers to take client and account information with them to their new firm.

Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?

Seyfarth's fifth installment, attorneys Jim McNairy and Marc Jacobs conveyed strategies and best practices to help in-house counsel and HR professionals ensure that company and internal clients are protected.

- The National Labor Relations Act applies to all private sector workplaces—not just unionized facilities. Among other things, the Act protects an employee's right to engage in protected concerted activities, which in general are group action (usually by two or more employees) acting together in a lawful manner, for a common, legal, work-related purpose (e.g., wages, hours and other terms and conditions of employment). Limits on these rights and retaliation against an employee for engaging in protected concerted activity violates the Act. The National Labor Relations Board is aggressively protecting employees' rights to engage in protected concerted activity. As part of this effort, the NLRB will find unlawful workplace rules, policies, practices and agreements that explicitly restrict Section 7 activities (such as a rule requiring employees to keep their wage rate confidential) or that employees would reasonably believe restricts their Section 7 rights (e.g., a confidentiality agreement or policy that generally includes in the definition of confidential information "personnel information").

- In the 2015 *Browning-Ferris Industries* decision, the NLRB substantially broadened the definition of "joint employer." Under this new expanded definition, an entity can be found to be a joint employer if it has the authority, even if

unexercised, to control essential terms and condition of employment. As a result, if one entity has agreements with other entities to provide labor or services, that entity may be a joint employer of the other entities' employees based on the level of control it has over the terms and conditions of employment of the other entities/ employees. One indicia of that control would be requirements for hiring or employment, such as requirements to sign agreements or adopt policies for the protection of confidential information and similar restrictions.

- As a result, and also because of the signing of the federal Defend Trade Secrets Act, now is a critical time for all employers to review their policies, practices, procedures and agreements (1) regarding the protection of confidential information; and (2) with third-party service and labor providers. In reviewing confidential information policies and agreements, the focus should be on narrow tailoring using specifics and examples to protect information that lawfully may be protected in a lawful manner. For agreements with parties, the review should include an analysis of the factors that may show joint employer status so that you can balance the risk of a joint employer finding with the needs to protect your organization.

The Defend Trade Secrets Act: What Employers Should Know Now

In Seyfarth's sixth installment, attorneys Robert Milligan, Daniel Hart, and Amy Abeloff described the key features of the Defend Trade Secrets Act ("DTSA") and compared its key provisions to the state Uniform Trade Secrets Act ("UTSA") adopted in many states. They also provided practical tips and strategies concerning the pursuit and defense of trade secret cases in light of the DTSA, and provide some predictions concerning the future of trade secret litigation.

- The DTSA was passed after many failed attempts at creating trade secret legislation allowing for a federal cause of action for misappropriation. The bill was passed with overwhelming bipartisan, bicameral support, as well as backing from many big name businesses. The DTSA now allows trade secret owners to sue in federal court for trade secret misappropriation, and seek remedies heretofore unavailable.

- The DTSA contains an immunity provision that protects individuals from criminal or civil liability for disclosing a trade secret if such disclosure is made in confidence to a government official or attorney, indirectly or directly. The provision applies to those reporting violations of law or who file lawsuits alleging employer retaliation for reporting a suspected violation of law, subject to certain specifications (i.e., trade secret information to be used in a retaliation case must be filed under seal). The DTSA places an affirmative duty on employers to give employees notice of this provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information," and will only be in compliance with this requirement if the employer cross-references a policy given to relevant employees describing the reporting policy for suspected violations of law. Employers that do not comply with this requirement forfeit the ability to recoup exemplary damages or attorney fees in an action brought under the DTSA against an employee to whom no notice was ever provided.

- Though the passage of the DTSA creates a new federal cause of action for trade secret misappropriation, the passage does not render state law and causes of action irrelevant or unimportant. The UTSA is still an available cause of action in 48 states, and state law on misappropriation still plays a vital role in drafting non-disclosure and non-competition agreements. Though the DTSA can place certain limitations on employees via employment agreements and employers may be able to seek injunctive relief against former employees in the event of misappropriation, such restrictions must comport with relevant state law.

Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements

In the seventh installment of Seyfarth's webinar series, attorneys John Skelton, James Yu, and Dawn Mertineit focused on the importance of state-specific non-compete laws and legislation and recent Federal and State efforts to regulate the use of non-compete agreements; enforcement considerations for the Franchisee when on-boarding and terminating employees; and lessons learned from recent decision regarding enforcing non-compete provisions upon termination and non-renewal.

- As reflected by the May 5, 2016, White House report (Non-Compete Agreements: Analysis of the Usage, Potential Issues, and State Responses), state and federal non-compete legislative proposals and recent enforcement action by the Illinois Attorney General challenging the use of non-compete agreements for lower level employees, Franchisors and Franchisees need to anticipate more regulation and scrutiny.

- With respect to their own employees, Franchisors and Franchisees need to develop and implement on-Boarding, termination and other procedures designed to ensure that both departing and prospective employees understand their ongoing obligations with respect to the company's confidential and proprietary information and trade secrets and that such information is protected throughout the employment relationship.

- The enforceability of non-compete provisions are most often litigated in the context of a request for a preliminary injunction and several recent decisions confirm that to enforce a non-compete against a departing franchisee the franchisor (1) should be able to show harm to actual competition; (2) needs to act promptly and that enforcement delays likely means that any alleged harm is not irreparable; and (3) should develop and implement a post-termination plan beyond simply sending a notice of termination as the franchisor will need to present evidence of actual harm.

International Non-Compete Law Update

In this installment in Seyfarth's 2016 Trade Secrets Webinar Series, International attorney Dominic Hodson focused on non-compete considerations from an international perspective. Dominic discussed general principals and recent international developments in non-compete issues around the globe. Companies who compete in the global economy should keep in mind these key points:

- Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. However, there are some common requirements and issues regarding enforceability based on the region, particularly in common law jurisdictions such as the UK, Canada (excluding Quebec), Australia/New Zealand, and Singapore/Hong Kong. A restrictive covenant is void unless it is **reasonable** to protect a legitimate interest of the employer; simply wanting to stop competition post-termination is not a legitimate interest.

- Outside of common law countries, there is no uniformity in rules, and every country must be taken separately. There are often detailed statutory rules that the clause must fulfill, but nevertheless there are repeating themes: There must be reasonableness to the non-compete agreement, and you must require proportionality between the clause and the interest sought to be protected.

- With respect to non-common law countries, liquidated damaged are often allowed. Civil law countries tend to be much more forgiving of liquidated damages and don't have the same rules regarding "penalty clauses."

The Intersection of Trade Secrets Violations and the Criminal Law

In this webinar, attorneys Andrew Boutros, Katherine Perrelli, and Michael Wexler focused on criminal liability for trade secret misappropriation. Trade secret misappropriation is increasingly garnering the attention of federal law enforcement authorities. This reality creates different dynamics and risks depending on whether the company at issue is being accused of wrongdoing or is the victim of such conduct.

- The theft of trade secrets is not only a civil violation—it is also a criminal act subject to serious fines and imprisonment. In an ever-increasing technological age where a company's crown jewels can be downloaded onto a thumb drive, victims and corporate violators must be mindful of the growing role that law enforcement plays in this active area. And, in doing so, working with experienced counsel is critical to interfacing with law enforcement (especially depending on which side of the "v." you are on), while still maintaining control of the civil litigation.

- With the advent of the Defend Trade Secrets Act (DTSA), intellectual capital owners have a powerful new tool to both

protect assets with as well potentially defend against. As such, processes must be in place to carefully screen new employees as well as provide vigilance over exiting employees so that one can guard against theft and be prepared to address purported theft brought to ones doorstep with a new hire. Finally, it is important to review and update agreements with the latest in suggested and required language to maximize protections, which is best accomplished through annual reviews of local and federal statutes with one's counsel.

- "Protect your own home" by putting tools in place before a trade secret misappropriation occurs. This includes taking a look at your employment agreements to make sure they are updated to comply with the DTSA and that they have been signed. In addition, make sure you have agreements in place with third parties (e.g., clients, vendors, contractors, suppliers) to protect your proprietary information. Finally, secure your network and facilities by distributing materials on a need-to-know basis: Don't let your entire workforce have access.

Trade Secret Audits: You Can't Protect What You Don't Know You Have

In Seyfarth's tenth installment, attorneys Robert Milligan, Eric Barton, and Scott Atkinson focused on trade secret audits. It is not uncommon for companies to find themselves in situations where important assets are overlooked or taken for granted. Yet, those same assets can be lost or compromised in a moment through what is often benign neglect. Experience has shown that companies gain tremendous value by taking a proactive, systematic approach to assessing and protecting their trade secret portfolios through a trade secret audit.

- As part of any trade secret audit, confidentiality agreements should be updated to include the new immunity language required by the Defend Trade Secrets Act (DTSA) to preserve the company's right to exemplary damages and attorney's fees under the DTSA.
- A trade secret audit, and the resulting protection plan, should have three primary goals:

  (1) Ensure that a company's trade secrets are adequately identified and protected from disclosure;

  (2) Ensure that a company has taken adequate steps to protect itself in litigation if a trade secret is misappropriated; and

  (3) Limit the risk of exposure to other companies' claims of trade secret misappropriation.

- As part of a trade secret audit, onboarding and off-boarding procedures are evaluated to ensure that the intellectual property rights of third parties and the company are respected.

Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches

In Seyfarth's final installment in the 2016 Trade Secrets Webinar Series, James McNairy and Justin Beyer, joined by computer forensics expert Jim Vaughn of iDiscovery Solutions, focused on best practices for assembling the evidence most often needed to prosecute a claim for misappropriation of trade secrets.

- The first step in prosecuting trade secret misappropriation starts with identifying your trade secret information, maintaining its confidentiality, and putting in place safeguards such as robust confidentiality agreements, computer use and access policies, and exit interviews that are tailored to flag any exfiltration of data by high risk employees or business partners with whom your company is parting ways. Diligence on the front end will better alert your organization of potential data theft and enable it to secure the data, should it be misappropriated.
- As part of your investigation of potential trade secret misappropriation, remember to conduct a complete audit of devices

and sources of data storage and transmission to ensure nothing is overlooked. While doing so, it is critical to maintain the forensic integrity of the devices and data to allow the best chance of admitting the information into evidence in any litigation.

- Efficiently organizing the right team to prosecute trade secret theft is critical. The "team" most often includes human resources professionals (to authenticate key agreements, policies, dates of employment etc.), a senior manager or executive (who can validate the existence of the trade secret, its value, the measures taken to maintain secrecy etc.), senior managers who worked with the suspected misappropriators (who can attest to access, use, and possession of the at issue information), in-house IT professionals (who can lay the foundation for devices, data, and access rights of the suspected misappropriators), and an independent computer forensics expert (who can objectively present the facts concerning data accessed, by whom, through what means, and explain any technical nuance to "connect the technical dots" of the bad actor(s) conduct).

2017 Trade Secret Webinar Series

Beginning in January 2017, we will begin another series of trade secret webinars. The first webinar of 2017 will be "2016 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law." 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.

Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your groups for CLE credit.

Michael Wexler is Chair and Robert Milligan is Co-Chair of the Trade Secrets, Computer Fraud & Non-Compete Practice Group. 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.