

Management Alert



2017 Trade Secrets Webinar Series Year in Review

Throughout 2017, 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 six webinars:

1. 2016 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Simple Measures for Protecting Intellectual Property and Trade Secrets
3. Protecting Confidential Information and Client Relationships in the Financial Services Industry
4. Protecting Your Trade Secrets in the Pharmaceutical Industry
5. Trade Secret Protection: What Every Employer Needs to Know
6. Protecting Trade Secrets in the Social Media Age

As a conclusion to this well-received 2017 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 DVD [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 2018, and we will release the 2018 trade secrets webinar series topics in the coming weeks.

2016 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, Michael Wexler, and Joshua Salinas, reviewed noteworthy cases and other legal developments from across the nation over the last year 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 2017.

- The DTSA can be a powerful tool to protect intellectual capital. However, in order to take full advantage of the DTSA, businesses should carefully check their agreements with employees, handbooks and equity awards to make sure they contain language mandated by the Defend Trade Secrets Act.
- 2016 was a record year for data and information security breaches. Organizations should alert and train employees on following company policies, 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.

- Several states enacted laws to limit the scope and duration of non-competes in 2016. There were also some significant decisions limiting their scope and enforceability in 2016 as well. Companies should have their non-disclosure and non-compete agreements reviewed to ensure that they comply with the latest state and federal laws, including the new Defend Trade Secrets Act.

Simple Measures for Protecting Intellectual Property and Trade Secrets

Every day, companies unknowingly give up intellectual property and trade secrets, which they could have otherwise protected with simple processes. Poor R&D policies may not capture patent rights on a company invention, or a faulty or simply outdated employment agreement may not protect a customer list used by an employee who leaves for a competitor. These pitfalls are easily avoidable by implementing measures on the front end and educating employees on the basics of intangible property and how to protect it.

In this webinar, Seyfarth attorneys Patrick Muffo and Kevin Mahoney provided a basic overview of what types of intellectual property and trade secrets are protectable, how to protect them, and helpful tips to ensure that a company is doing everything they can to avoid common issues associated with intangible property.

- Businesses routinely miss out on opportunities to protect their valuable intellectual property simply because they do not realize that their inventions or developments qualified as intellectual property in the first place. Particularly in light of changes in patent law that reward the first party to file for a patent—regardless of whether they invented something first or not—it is important to be proactive about applying for patent protection as early as possible. If a business believes that an invention may qualify for either a design or utility patent, it should take steps to start the patent application process as soon as possible.
- Copyright and trademark protection are also an important, and often overlooked, component of intellectual property protection. Trademarks are routinely granted for patterns, brands, logos, trade dress, and other identifying images which businesses may have thought were too generic to qualify for such protection. Copyrights are also becoming an increasingly important tool in protecting computer code.
- Trade secrets are also intellectual property, but are governed by an entirely different set of laws and are protected in different ways, often through litigation. Because the recently-enacted Defend Trade Secrets Act of 2016 requires the owner of trade secrets to have taken reasonable steps to protect that information, businesses should identify their processes for identifying what information qualifies as a trade secret and what steps they have taken to protect that information, including the implementation of employee confidentiality agreements. Confidentiality agreements drafted before 2016 need to be updated to include certain whistleblower language as a result of the passage of the Defend Trade Secrets Act.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

In Seyfarth's third installment of its 2017 Trade Secrets Webinar series, Seyfarth attorneys Scott Humphrey, Robyn Marsh, and Dawn Mertineit focused on trade secret and client relationship considerations in the banking and financial services industry, with a particular focus on a firm's relationship with its FINRA members. This webinar also included practical steps financial institutions can implement to protect trade secrets and client relationships; tips on what to do if your trade secrets are improperly removed or disclosed or if a former employee is violating his/her restrictive covenant agreements; how to prosecute a case against a former employee who is a FINRA member; and the impact of the Protocol for Broker Recruiting on trade secrets and client relationships.

- Remember that you can seek court injunctive relief (Temporary Restraining Order and, possibly, Preliminary Injunction) before proceeding in FINRA.
- The definition of a trade secret varies by company, but you must take adequate steps to protect them as a company, and the information cannot be publicly available or easily discovered, to merit enforcement under the law.
- Employers can take steps at all stages to protect their confidential information—don't forget to implement on-boarding and off-boarding procedures, as well as policies and procedures that will be in effect during an employee's tenure, to protect your information before a problem arises.

Protecting Your Trade Secrets in the Pharmaceutical Industry

Seyfarth's fourth installment, presented by Justin Beyer, Marcus Mintz, Dean Fanelli, and Thomas Haag, focused on how to define and protect trade secrets in the pharmaceutical industry, including a review of significant civil and criminal cases in the industry, a discussion on how federal and state trade secret statutes and decisions may impact the protection of trade secrets, and best practices for protecting trade secrets from invention through sale.

- Trade secret laws cover any information which is confidential, kept confidential, and from which the owner derives economic benefit. In order to maintain such protections, owners must be vigilant and proactive about maintaining the secrecy of their trade secret information. One of the ways in which employers should do so is to update their employment agreements to comply with the immunity notice provisions of the Defend Trade Secrets Act, without which the employer may lose the ability to recover attorney's fees or double damage awards.
- In the pharmaceutical and biotechnology space, companies should also take active steps to develop internal guidelines and protocols for the identification and protections of information that may be the subject of trade secret protection, whether that information is related to research and development, strategic business plans, or future opportunities and trends. These steps include, but are not limited to: (i) advising all employees of the confidential and proprietary nature of their work; (ii) limiting access to proprietary and confidential information to only those employees requiring such information; (iii) actively monitoring how information is distributed both internally and externally; and (iv) regularly updating employees of the necessity to maintain confidentiality of all information.
- Trade secrets are particularly valuable with respect to the development of biologics. Given long clinical development timelines, composition patents covering reference biologics may be about to expire or will have already expired, at time of marketing approval. Confidential and proprietary details relating to reference protein drug production, isolation, storage and delivery; as well as its post-transnational modifications, are at least as important to know as the identity of the reference protein's amino acid sequence, when creating a biosimilar. Thus these trade secrets represent potentially enormous barriers to market entry for third party developers of biosimilar versions. They should, therefore, be kept in the strictest confidence.
- If a company does, however, find itself in a situation in which it fears that an employee has or may misappropriate its trade secret information, it should take certain immediate steps, including: (a) reminding the employee of his/her obligations; (b) forensically imaging and reviewing the employee's email communications, downloading history, and/or internet activity; (c) cutting off the employee's access to company confidential information, as soon as notice is provided that the employee is taking a position with a competitor; and (d) if necessary, filing suit to recover and protect the secrecy of the trade secrets. Once trade secrets are disclosed in public, whether properly or improperly, it becomes exceedingly difficult to prove the ongoing secrecy of the information and even harder to put the secret back in its box.

Trade Secret Protection: What Every Employer Needs to Know

In Seyfarth's fifth installment, attorneys Robert Milligan and Daniel Joshua Salinas were joined by Jim Vaughn, one of

California's leading forensics experts. The panel focused on how to help employers navigate the tricky trade secrets waters and provided best practices for trade secret protection.

- Employers should review their non-disclosure and non-compete agreements to determine whether they have accurately defined the scope of categories of their confidential information, as well included the whistleblower immunity language required under the Defend Trade Secrets Act. Additionally, they should ensure their agreement complies with recent changes in non-compete law, including legislative changes in Nevada, Oregon, Idaho, and Alabama.
- Employers should consider how they treat employee-owned devices for work, as well as corporate-issued mobile devices. Getting access to those devices may prove to be challenging upon an employee's departure. Having technology and a policy in place to allow the employer to gain access to their data is critical.
- Effectively protecting trade secrets includes not only creating an internal culture of confidentiality with employees but also limiting information made available to vendors and subcontractors and having appropriate trade secret protection agreements with third parties.

Protecting Trade Secrets in the Social Media Age

There is no denying that social media has transformed the way companies conduct business, but social media and related issues in the workplace can be a headache for employers. In light of the rapid evolution of social media, companies today face significant legal challenges on a variety of issues, ranging from employee privacy and protected activity to data practices, identity theft, cybersecurity, and protection of intellectual property. Request a copy of our 2017–2018 Social Media Privacy Legislation Desktop Reference [here](#).

In Seyfarth's sixth installment, attorneys Justin Beyer, Dawn Mertineit, and Ryan Behndelman discussed the relationship between trade secrets and social media, including the interplay between social media privacy laws and workplace investigations and how developing internal company policy and/or contracts can protect company assets; how to define, understand, and protect trade secrets in social media; how courts are interpreting ownership of social media accounts and whether social media sites constitute property; how to prevent trade secret misappropriation or distribution through social media channels; and the interplay between protection of company information and ownership of company accounts in the social media age.

- By allowing social media in the workplace, companies are exposed to multiple risks, including the theft of confidential information and potential embarrassment to the company. It is imperative that companies craft a social media policy that will not only protect the company, but will also work within the company's individual structure.
- In defining an employee's obligations as it relates to social media usage, companies should make sure they have policies in place (as well as a provision in any employment agreements) regarding the ownership of company social media accounts. Having clear, written policies and agreements can eliminate or reduce the need for costly and time-consuming litigation to determine who owns company-related social media presences.
- Finally, due to the concern about employer involvement in an employee's social media presence, employers should be mindful to abide by direction provided by state legislation as well as the National Labor Relation Board's interpretation of what constitutes improper interference in speech activities. Because of this, it is important to craft any social media policy with a view toward protecting company assets and reputation, without being perceived to infringe on the speech or privacy rights of employees.

2018 Trade Secret Webinar Series

Beginning in January 2018, we will begin another series of trade secret webinars. The first webinar of 2018 will be "2017 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, Robert Milligan at rmilligan@seyfarth.com, 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.

www.seyfarth.com

Attorney Advertising. This Management Alert is a periodical publication of Seyfarth Shaw LLP and should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. Any tax information or written tax advice contained herein (including any attachments) is not intended to be and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on the taxpayer. (The foregoing legend has been affixed pursuant to U.S. Treasury Regulations governing tax practice.)

Seyfarth Shaw LLP Management Alert | December 13, 2017

©2017 Seyfarth Shaw LLP. All rights reserved. “Seyfarth Shaw” refers to Seyfarth Shaw LLP (an Illinois limited liability partnership). Prior results do not guarantee a similar outcome.