SEYFARTH SHAW

Management Alert

2018 Trade Secrets and Non-Competes Webinar Series Year in Review

Throughout 2018, 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 seven webinars:

1. 2017 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Protecting Confidential Information and Client Relationships in the Financial Services Industry
3. The Anatomy of a Trade Secret Audit
4. Protecting Trade Secrets from Cyber and Other Threats
5. 2018 Massachusetts Non-Compete and Trade Secrets Reform
6. Protecting Trade Secrets Abroad and Enforcing Rights Abroad and in the U.S.
7. Criminal Trade Secret Theft: What You Need to Know

As a conclusion to this well-received 2018 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, recordings of the webinars are available on the blog, or you may click on the title of each available webinar below for the online recording. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your company for CLE credit. Seyfarth will continue its trade secrets webinar programming in 2019, and we will release the 2019 trade secrets webinar series topics in the coming weeks.

2017 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 2018.

- While the Defend Trade Secrets Act provides for an *ex parte* seizure order, courts have been very unwilling to provide such relief except in extraordinary circumstances.
- In light of recent state laws and appellate court decisions at both the federal and state level in 2017, choice of venue and choice of law provisions must be carefully considered and strategically implemented.

- The ABA's May 4, 2017, Ethics Opinion encourages lawyers to have an open exchange of communication with their clients about the securities measures their firms are taking to safeguard the clients' confidential information.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

Seyfarth attorneys Scott Humphrey, Erik Weibust, and Marcus Mintz 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. In addition, the panel covered what to do if 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, but your company must take adequate steps to protect them, 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 onboarding 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.

The Anatomy of a Trade Secret Audit

Seyfarth attorneys Kate Perrelli, Dawn Mertineit, Justin Beyer, and Andrew Stark focused on trade secret audits, with an emphasis on the importance of a proactive, systematic approach to assessing and protecting trade secret portfolios.

- Recent government and news media attention on trade secret theft serves as a firm reminder of the risk of trade secrets being stolen and the importance of protecting them. Trade secret theft costs U.S. companies hundreds of billions of dollars per year, and even the largest and most sophisticated companies are victims.
- It is critical to identify and understand your company's trade secrets to ensure that you have adequate protections from theft in place.
- Have a well-communicated plan for the audit to ensure buy-in from appropriate stakeholders and set expectations.
- An equally important, but sometimes overlooked, component of the trade secret audit is reviewing and analyzing a company's internal technology. Any plan to prevent misappropriation should include analyzing company technology, upgrading it when feasible, or customizing it to prevent someone from stealing information.

Protecting Trade Secrets from Cyber and Other Threats

Seyfarth attorneys Robert Milligan and Scott Atkinson, along with Center for Responsible Enterprise and Trade CEO Pamela Passman, focused on identifying the greatest threats to trade secrets, implementing an effective trade secret protection program, and enacting effective risk reduction processes across an organization.

- Building a culture of trade secret protection is essential for protecting against cyber threats. Simply having policies is not enough; companies need to follow up with training, acknowledgements/record keeping, and engaged leaders who lead by example.
- One key part of an effective trade secret protection plan is having an effective onboarding and off-boarding process, including exit interviews. Exit interviews should be conducted, and employees should be reminded of their continuing

confidentiality and other obligations to the company. Don't forget to ask for any passwords to any company-owned mobile devices.

- As companies build internal capabilities to protect trade secrets and ensure robust cybersecurity, those capabilities should be required of key supply chain partners or vendors that have access to trade secrets and should be measured and monitored to ensure they are effective.

2018 Massachusetts Non-Compete and Trade Secrets Reform

What Companies with Massachusetts Employees Need to Know

Seyfarth attorneys Kate Perrelli, Erik Weibust, and Dawn Mertineit focused on Massachusetts non-compete and trade secrets reform. At long last, Massachusetts Governor Charlie Baker signed a Non-Compete Reform Bill into law on August 10. The presenters focused on what businesses should understand about the impacts of the changes, what to expect next, and how to safeguard assets and maintain an advantage over competitors.

- Non-competes must be limited to one year, but can be extended to two if the employee breaches his or her fiduciary duty or steals company property.
- Must be in writing and signed by both parties; at least 10 days notice must be provided to employees/candidates; and the right to counsel must be explicit in the agreement.
- Garden leave is not required. "Other mutually agreed-upon consideration" is adequate. But what that means, and whether the court will even assess the adequacy of consideration, is left to the courts to determine.
- Continued employment is no longer sufficient consideration. Something more, that is "fair and reasonable" must be provided. Again, what that means is left to the courts to determine.
- Choice of law and venue requirements are likely unenforceable in other states and in federal court. Nevertheless, comply with the law in case an employee files a declaratory judgment action in Massachusetts.
- **Bottom line:** Be clear in your agreements. All the law really does is establish what must, may, and may not be included in private agreements.

Protecting Trade Secrets Abroad and Enforcing Rights Abroad and in the U.S.

Seyfarth attorneys Daniel Hart, Marjorie Culver, Alex Meier, and Paul Yovanic Jr. focused on protecting trade secrets internationally and enforcing rights abroad and in the United States. The panel covered how to identify the greatest threats to trade secrets, tips and best practices for protecting trade secrets abroad, and enforcement mechanisms and remedies.

- Companies don't want to be in a position where they are relying exclusively on trade secrets law to protect proprietary information. When possible, execute a confidentiality agreement. This will not only protect a wider range of information, but also often helps with securing pre-discovery injunctive relief.
- In order to adequately protect trade secrets abroad, companies should inform employees of the important nature of secret information, take steps to secure secret information and limit access only to necessary employees, and avoid liability without culpability by revising employment agreements and informing new hires of the prohibited conduct.
- Restrictive covenants abroad are easier to enforce when agreements are narrowly tailored for duration, geographic scope, and nature and when penalties are reasonable.
- For international misappropriation, consider whether you want to pursue relief in the foreign jurisdiction or in the United States. The Defend Trade Secrets Act and, in some instances, Section 337 actions before the International Trade Commission rules offer powerful alternatives to proceedings in other jurisdictions.

Criminal Trade Secret Theft: What You Need to Know

Seyfarth attorneys Andrew Boutros and John Schleppenbach focused on criminal liability for trade secret theft, including four key statutes, key elements for criminal prosecution, civil RICO under the Defend Trade Secrets Act, and best practices for avoiding misappropriation and for handling misappropriation when it occurs.

- 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, intellectual capital owners have a powerful new tool to protect trade secrets, but intellectual capital owners must also be prepared to defend against claims brought under the DTSA. 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 that 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 Defend Trade Secrets Act 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.

2019 Trade Secret Webinar Series

Beginning in January 2019, we will begin another series of trade secret webinars. The first webinar of 2019 will be "2018 National Year in Review: What You Need to Know About the Recent Cases and 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, or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (www.seyfarth.com/tradesecrets). Subscribe to our Trading Secrets Blog for timely legal and news updates at www.tradesecretslaw.com.