SEYFARTH SHAW

Management Alert

Top Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2016

By Robert B. Milligan and Daniel Joshua Salinas

Continuing our annual tradition, we present the top developments/headlines for 2016 in trade secret, computer fraud, and non-compete law. Please join us for our first webinar of the New Year on February 2, 2017, at 12:00 p.m. Central, where we will discuss these new developments, their potential implications, and our predictions for 2017.

1. Defend Trade Secrets Act

One of the most significant developments of 2016 that will likely have a profound impact on trade secret cases in the coming years was the enactment of the Defend Trade Secrets Act ("DTSA"). The DTSA creates a new federal cause of action for trade secret misappropriation, albeit it does not render state law causes of action irrelevant or unimportant. The DTSA was passed after several years and many failed attempts. The bill was passed with overwhelming bipartisan, bicameral support, as well as backing from the business community.

The DTSA now allows trade secret owners to sue in federal court for trade secret misappropriation, and seek remedies previously unavailable. Employers should be aware that the DTSA contains a whistleblower immunity provision, which 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). This is significant for employers because it places an affirmative duty on them 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." Employers who do not comply with this requirement forfeit the ability to recoup exemplary damages or attorneys' fees under the DTSA in an action against an employee to whom no notice was ever provided.

At least one federal district court has rejected an employee's attempts to assert whistleblower immunity under the DTSA. In *Unum Group v. Loftus*, No. 4:16-CV-40154-TSH, 2016 WL 7115967 (D. Mass. Dec. 6, 2016), the federal district court for the district of Massachusetts denied a defendant employee's motion to dismiss and held that a defendant must present evidence to justify the whistleblower immunity.

We anticipate cases asserting claims under the DTSA will be a hot trend and closely followed in 2017. For further information about the DTSA, please see our webinar "New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive."

2. EU Trade Secrets Directive

On May 27, 2016, the European Council unanimously approved its Trade Secrets Directive, which marks a sea-change in protection of trade secrets throughout the European Union ("EU"). 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. Similar to the DTSA, the purpose of the EU's Trade Secrets Directive was to provide greater consistency in trade secrets protection throughout the EU. For further information about the EU's Trade Secrets Directive, please see our webinar "New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive."

3. Government Agencies Continue to Scrutinize the Scope of Non-Disclosure and Restrictive Covenant Agreements

Fresh off of signing the DTSA, the Obama White House released a report entitled "Non-Compete Reform: A Policymaker's Guide to State Policies," which relied heavily on Seyfarth Shaw's "50 State Desktop Reference: What Employers Need to Know About Non-Compete and Trade Secrets Law" and contained information on state policies related to the enforcement of non-compete agreements. Additionally, the White House issued a "Call to Action" that encouraged state legislators to adopt policies to reduce the misuse of non-compete agreements and recommended certain reforms to state law books. The Non-Compete Reform report analyzed the various states that have enacted statutes governing the enforcement of non-compete agreements and the ways in which those statutes address aspects of non-compete enforceability, including durational limitations; occupation-specific exemptions; wage thresholds; "garden leave;" enforcement doctrines; and prior notice requirements.

With those issues in mind, the Call to Action encourages state policymakers to pursue three "best-practice policy objectives": (1) ban non-competes for categories of workers, including workers under a certain wage threshold; workers in occupations that promote public health and safety; workers who are unlikely to possess trade secrets; or workers who may suffer adverse impacts from non-competes, such as workers terminated without cause; (2) improve transparency and fairness of non-competes by, for example, disallowing non-competes unless they are proposed before a job offer or significant promotion has been accepted; providing consideration over and above continued employment; or encouraging employers to better inform workers about the law in their state and the existence of non-competes in contracts and how they work; and (3) incentivize employers to write enforceable contracts and encourage the elimination of unenforceable provisions by, for example, promotion of the use of the "red pencil doctrine," which renders contracts with unenforceable provisions void in their entirety.

While some large employers have embraced the Call to Action, even reform-minded employers are likely to be wary of some of these proposals. Moreover, this initiative may die or be limited with the new Trump administration.

On October 20, 2016, the Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") jointly issued their "Antitrust Guidance for Human Resource Professionals." The Guidance explains how antitrust law applies to employee hiring and compensation practices. The agencies also issued a "quick reference card" that lists a number of "antitrust red flags for employment practices." In a nutshell, agreements (whether formal or informal) among employers to limit or fix the compensation paid to employees or to refrain from soliciting or hiring each other's employees are per se violations of the antitrust laws. Also, even if competitors don't explicitly agree to limit or suppress compensation, the mere exchange of compensation information among employers may violate the antitrust laws if it has the effect of suppressing compensation.

In recent years, the National Labor Relations Board ("NLRB") has issued numerous decisions in which workplace rules were found to unlawfully restrict employees' Section 7 rights. Last year, the U.S. Court of Appeals for the D.C. Circuit denied Quicken Loans, Inc.'s petition for review of an NLRB decision finding that confidentiality and non-disparagement provisions in the company's Mortgage Banker Employment Agreement unreasonably burdened employees' rights under Section 7 of the NLRA.

4. New State Legislation Regarding Restrictive Covenants

Oregon has limited the duration of employee non-competes to two years effective January 1, 2016. Utah has enacted the Post-Employment Restrictions Amendments, which limits restrictive covenants to a one-year time period from termination. Any restrictive covenant that is entered into on or after May 10, 2016, for more than one year will be void. Notably, Utah's new law does not provide for a court to blue pencil an agreement (i.e., revise/modify to the extent it becomes enforceable), rather the agreement as a whole will be deemed void if it is determined to be unreasonable.

In what appears to have become an annual tradition, Massachusetts legislators have attempted to pass legislation regarding non-competes, to no avail. Two other states in New England, however, are able to claim accomplishments in that regard. Specifically, Connecticut and Rhode Island each enacted statutes last summer imposing significant restrictions on the use of non-compete provisions in any agreement that establishes employment or any other form of professional relationship with physicians. While Connecticut's law limits only the duration and geographic scope of physician non-competes, Rhode Island completely banned such provisions in almost all agreements entered into with physicians.

5. Noteworthy Trade Secret, Computer Fraud, and Non-Compete Cases

In *Golden Road Motor Inn, Inc. v. Islam*, 132 Nev. Adv. Op. 49 (2016), the Supreme Court of Nevada refused to adopt the "blue pencil" doctrine when it ruled that an unreasonable provision in a non-compete agreement rendered the entire agreement unenforceable. Accordingly, this means that employers conducting business in Nevada should ensure that non-compete agreements with their employees are reasonably necessary to protect the employers' interests. Specifically, the scope of activities prohibited, the time limits, and geographic limitations contained in the non-compete agreements should all be reasonable. If an agreement contains even one overbroad or unreasonable provision, the employer risks having the entire agreement invalidated and being left without any recourse against an employee who violates the agreement.

The Louisiana Court of Appeal affirmed a $600,000 judgment, plus attorneys' fees and costs, against an ex-employee who violated his non-compete when he assisted his son's start-up company compete with the ex-employee's former employer. See *Pattridge v. Starks*, No. 50,351-CA (Louisiana Court of Appeal, Feb. 24, 2016) (Endurall III).

A Massachusetts Superior Court judge struck down a skin care salon's attempt to make its non-compete agreement seem prettier than it actually was. In denying the plaintiff's motion for a preliminary injunction, the court stressed that employees' conventional job knowledge and skills, without more, would not constitute a legitimate business interest worth safeguarding. See *Elizabeth Grady Face First, Inc. v. Garabedian et al.*, No. 16-799-D (Mass. Super. Ct. March 25, 2016).

In a case involving alleged violations of the Kansas Uniform Trade Secrets Act ("KUTSA") and the Computer Fraud and Abuse Act ("CFAA"), a Kansas federal district court granted a defendant's motion for summary judgment, holding that (a) payments to forensic experts did not satisfy the KUTSA requirement of showing an "actual loss caused by misappropriation" (K.S.A. 60-3322(a)), and (b) defendant was authorized to access the company's shared files and, therefore, he did not violate the CFAA. See *Tank Connection, LLC v. Haight*, No. 6:13-cv-01392-JTM (D. Kan., Feb. 5, 2016) (Marten, C.J.).

The Tennessee Court of Appeals held that the employee's restrictive covenants were unenforceable when the employer had not provided the employee with any confidential information or specialized training. See *Davis v. Johnstone Group, Inc.*, No. W2015-01884-COA-R3-CV (Mar. 9, 2016).

Reversing a 2-1 decision of the North Carolina Court of Appeals, the state's Supreme Court held unanimously that an assets purchase-and-sale contract containing an unreasonable territorial non-competition restriction is unenforceable Further, a court in that state must strike, and may not modify, the unreasonable provision. See *Beverage Systems of the Carolinas, LLC v. Associated Beverage Repair, LLC*, No. 316A14 (N.C. Sup. Court, Mar. 18, 2016).

The Ohio Court of Appeal upheld a non-compete giving the former employer discretion to determine whether an ex-employee was working for a competitor. See *Saunier v. Stark Truss Co.*, Case No. 2015CA00202 (Ohio App., May 23, 2016).

In a clash between two major oil companies, the Texas Supreme Court ruled on May 20, 2016, that the recently enacted Texas Uniform Trade Secrets Act ("TUTSA") allows the trial court discretion to exclude a company representative from portions of a temporary injunction hearing involving trade secret information. The Court further held a party has no absolute constitutional due-process right to have a designated representative present at the hearing.

A Texas Court of Appeals held on August 22, 2016, that a former employer was entitled to $2.8 million in attorneys' fees against a former employee who used the employer's information to compete against it. The Court reached this ruling despite the fact that the jury found no evidence that the employer sustained any damages or that the employee misappropriated trade secrets.

In *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, Case No. 4:13-CV-4021 (7th Cir., Jan. 21, 2016), the Seventh Circuit Court of Appeals affirmed a district court's conclusion that a plaintiff had produced no evidence refuting the defendant's contention that it honestly believed it was engaging in lawful business practices rather than intentionally deceiving or defrauding the plaintiff. Even though the plaintiff's technology did not expressly permit third parties to access the digitized records and use the information without printing copies, thereby avoiding payment of fees to plaintiff, such access and use were not prohibited.

A divided Ninth Circuit panel affirmed the conviction of a former employee under the CFAA, holding that "[u]nequivocal revocation of computer access closes both the front door and the back door" to protected computers, and that using a password shared by an authorized system user to circumvent the revocation of the former employee's access is a crime. See *United States v. Nosal*, ("Nosal II") Nos. 14-10037, 14-10275 (9th Cir. July 5, 2016).

The Ninth Circuit in *Facebook v. Power Ventures*, Case No. 13-17154 (9th Cir. Jul. 12, 2016), held that defendant Power Ventures did not violate the CFAA when it made copies and extracted data from the social media website despite receiving a cease and desist letter. The court noted that Power's users "arguably gave Power permission to use Facebook's computers to disseminate messages" (further stating that "Power reasonably could have thought that consent from *Facebook users* to share the [Power promotion] was permission for Power to access *Facebook's* computers") (emphasis in original). Importantly, the court found that "[b]ecause Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA."

6. Forum Selection Clauses

California enacted a new law (Labor Code § 925) that restrains the ability of employers to require employees to litigate or arbitrate employment disputes (1) outside of California or (2) under the laws of another state. The only exception is where the employee was individually represented by a lawyer in negotiating an employment contract. For companies with headquarters outside of California and employees who work and reside in California, this assault on the freedom of contract is not welcome news.

We also continued to see federal district courts enforcing forum selection clauses in restrictive covenant agreements. For example, a Massachusetts federal district court last fall transferred an employee's declaratory judgment action to the Eastern District of Michigan pursuant to a forum-selection clause in a non-compete agreement over the employee's argument that he had signed the agreement under duress because he was not told he would need to sign it until he had already spent the money and traveled all the way from India to the United States.

7. Security Breaches and Data Theft Remain Prevalent

2016 was a record year for data and information security breaches, one of the most notably being WikiLeaks' release of emails purportedly taken from the Democratic National Committee's email server. According to a report from the Identity

Theft Resource Center, U.S. companies and government agencies saw a **40% increase** in data breaches from 2015 and suffered over a thousand data breaches. Social engineering has become 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. For technical considerations and best practices and policies of attorneys when in the possession of client data, please view our webinar, "A Big Target—Cybersecurity for Attorneys and Law Firms."

8. The ITC's Extraterritorial Authority in Trade Secret Disputes

In a case involving the misappropriation of U.S. trade secrets in China, the U.S. Supreme Court was asked to decide whether Section 337 of the Tariff Act does, in fact, authorize the U.S. International Trade Commission ("ITC") to investigate misappropriation that occurred entirely outside the United States. See *Sino Legend (Zhangjiangang) Chemical Co. Ltd. v. ITC*. The crux of Sino Legend's argument was that for a statute to apply abroad, there must be express congressional intent. Not surprisingly, Sino Legend argued that such intent was missing from Section 337 of the Tariff Act. In *Tianrui Group Co. Ltd. v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011), the Federal Circuit held that such intent was manifest in the express inclusion of "the importation of articles … into the United States" which evidenced that Congress had more than domestic concerns in mind. On January 9, 2017, the Supreme Court denied Sino Legend's petition for certiorari, thereby keeping the ITC's doors open to trade secret holders seeking to remedy misappropriation occurring abroad. For valuable insight on protecting trade secrets and confidential information in China and other Asian countries, including the effective use of non-compete and non-disclosure agreements, please check out our recent webinar titled, "Trade Secret and Non-Compete Considerations in Asia."

We thank everyone who followed us this year and we really appreciate all of your support. We will continue to provide up-to-the-minute information on the latest legal trends and cases in the U.S. and across the world, as well as important thought leadership and resource links and materials.

Robert Milligan is a partner in Seyfarth's Los Angeles Office and co-chair of the Trade Secrets, Computer Fraud & Non-Compete Practice Group. D. Joshua Salinas is an attorney in Seyfarth's Los Angeles Office. If you have any questions, please contact Robert Milligan at rmilligan@seyfarth.com or D. Joshua Salinas at jsalinas@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.