SEYFARTH SHAW

Management Alert

Top Developments and Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2017 and What We Expect in 2018

By Robert B. Milligan and Daniel Joshua Salinas

Continuing our annual tradition, we present the top developments and headlines for 2017 and what we expect in 2018 in trade secret, computer fraud, and non-compete law.

1. Notable Defend Trade Secrets Act Developments

Just nearly two years after its enactment, the Defend Trade Secrets Act ("DTSA") continues to be one of the most significant and closely followed developments in trade secret law. The statute provides for a federal civil cause of action for trade secret theft, protections for whistleblowers, and new remedies (e.g., *ex parte* seizure of property), that were not previously available under state trade secret laws.

The *ex parte* seizure provision of the DTSA was one of the most controversial provisions of the statute during its drafting. The provision allows a trade secret holder to request, without notice to the alleged wrongdoer, that a district judge order federal law enforcement officials to seize property to prevent the propagation or dissemination of trade secrets. Opponents of the DTSA argued that the ex parte seizure provision would open the door to abuse by purported "trade secret litigation trolls" and increase litigation costs. The cases to date involving the seizure provision suggest that those early concerns may not materialize.

NOW AVAILABLE!

2017 Trading Secrets Year in Review

Seyfarth's Year in Review is a compilation of our significant trade secrets, non-competes, and computer fraud blog posts throughout 2017. To request a pdf, hard copy, or CD of the Review, click here.

2017 Year in Review Trade Secrets Webinar

To view the webinar recording and key takeaways, click here.

A rising development with the DTSA concerns its application to alleged misappropriation that occurs both before and after the statute's May 11, 2016, effective date. Federal district courts in multiple jurisdictions have allowed plaintiffs to proceed with DTSA claims, at least partially, when the plaintiffs can sufficiently allege that any wrongful misappropriation occurred after the date of the enactment of the DTSA. See, e.g., *IA Technologies, Inc. v. ASUS Computer International*, No. 14-CV-03586-BLF, 2017 WL 491172 (N.D. Cal. Feb. 7, 2017) (allowing plaintiff to amend complaint to add DTSA claim after discovery revealed alleged continued misappropriation); but *see Avago Techs. United States Inc. v. NanoPrecision Products*, No. 16-cv-03737, 2017 WL 412524 (N.D. Cal. Jan. 31, 2017) (dismissing DTSA claim because alleged trade secrets were disclosed before the DTSA came into effect).

While the language of the DTSA appears to bar or significantly limit the inevitable disclosure doctrine, some federal district courts have nonetheless used the doctrine as grounds for injunctions. See, e.g., *Fres-co Systems USA, Inc. v. Hawkins*, 2017 WL 2376568 (3rd Cir. June 1, 2017) ("Given the substantial overlap (if not identity) between Hawkins's work for Fres-co and

his intended work for Transcontinental—same role, same industry, and same geographic region—the District Court was well within its discretion to conclude Hawkins would likely use his confidential knowledge to Fres-co's detriment."); *Molon Motor and Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545 (N.D. Ill. May 11, 2017) ("allegations on the direct competition between the parties, as well as the allegations on the employment breadth and similarity of Desai's quality control work at the two companies, are enough to trigger the circumstantial inference that the trade secrets inevitably would be disclosed by Desai to Nidec.").

The DTSA's whistleblower immunity provision, which protects individuals from criminal or civil liability for disclosing a trade secret if certain conditions are met, continues to be largely untested.

We anticipate cases asserting claims under the DTSA will continue to be a hot trend and closely followed in 2018. For further information about the DTSA, please see our desktop reference: "The Defend Trade Secrets Act: What Employers Should Know Now."

2. Other Notable Trade Secret Cases

The *Waymo v. Uber* (N.D. Cal.) case was one of the most closely watched trade secret cases last year. The case involved a former Waymo employee who allegedly misappropriated trade secrets concerning self-driving car technology, which Waymo alleged was worth over $2 billion. The case involved disputes over a wide array of issues, such as trade secret preemption, the attorney-client privilege and Fifth Amendment, and the scope of injunctive relief (and non-competes) in California. The case reportedly settled mid-trial in February 2018, which gave Waymo/Google a .34 percent equity stake (approx. $245M) in Uber.

The Ninth Circuit in *U.S. v. Liew* held that it was not plain error for the district court not to instruct the jury that disclosure "'to even a single recipient who is not legally bound to maintain [a trade secret's] secrecy' destroys trade secret protection." As a result, the Ninth Circuit upheld criminal convictions under the (pre-Defend Trade Secrets Act) Economic Espionage Act ("EEA") for trade secret misappropriation despite a third-party competitor (who was not bound by any confidentiality obligations) acquiring the trade secret.

The *Liew* case is significant because it illustrates one of the DTSA's substantial changes to the EEA–the definition of a trade secret. Before the DTSA, trade secrets were defined under the EEA to include information that was subject to reasonable secrecy measures and "derive[d] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." This case also reminds businesses about the potential risks to trade secrets when selling business assets. Building facilities, electronic devices, and any other equipment sold should be vetted to ensure no valuable company information is inadvertently disclosed.

The Wisconsin Supreme Court in *North Highland Inc. v. Jefferson Machine & Tool Inc.*, 2017 WI 75 (July 6, 2017) affirmed the high summary judgment bar to trade secret misappropriation claims. There, the Court found that the plaintiff had failed to present sufficient evidence of misappropriation or conspiracy to proceed beyond the summary judgment stage. This case puts parties in Wisconsin on notice as to the importance of finding some direct evidence of misappropriation in defeating a motion for summary judgment.

The decision in *Zenimax Media, Inc. v. Oculus VR, LLC*, No. 3:14-CV-1849 (N.D. Texas 2017) illustrates that nondisclosure agreements remain important and can be a powerful alternative when trade secret claims are not successfully. The jury in that case found no liability on the plaintiff's trade secret claim but awarded the plaintiff $200 million in damages for the breach of a nondisclosure agreement. The jury was charged with determining, "[w]hat sum of money would fairly and reasonably compensate ZeniMax and ID Software for their injuries that resulted from Oculus's failure to comply with the Non-Disclosure Agreement?"

For a 50 state survey of non-compete laws, please see our recently updated: "50 State Desktop Reference: What Businesses Need To Know About Non-Compete and Trade Secrets Laws."

3. Notable Restrictive Covenant and Forum Selection Clause Cases

The Wisconsin Supreme Court heightened the scrutiny for employee non-solicitation agreements in the state. *Manitowoc Company, Inc. v. Lanning*, 2018 WL 472928 (Jan. 19, 2018). The case involved an engineer who had been with the plaintiff employer for over 25 years until he left to become a director of engineering with a competitor. The former employee had a non-solicitation of employees covenant with his former employer, which provided: "for a period of two years … (either directly or indirectly) solicit, induce or encourage any employee(s) to terminate their employment with Manitowoc or to accept employment with any competitor, supplier or customer of Manitowoc…." The Court found the covenant was an unreasonable restraint of trade and, thus, unenforceable. The Court reasoned that the former employee did not have specialized knowledge about all of employer's 13,000 world-wide employees and he did not have a relationship with every employee.

Illinois federal district courts continue to reject the controversial *Fifield v. Premier Dealer Service*, 993 N.E.2d 938 (Il. App (1st) 2013) decision by the Illinois Appellate Court. The court in *Fifield* held that a restrictive covenant executed by an at-will employee is unenforceable, for lack of adequate consideration, unless the employment relationship lasts at least two years beyond the date of execution. The federal district court for the Northern District of Illinois in *Stericycle, Inc. v. Simota*, Case No. 16 C 4782 (Oct. 20, 2017) rejected *Fifield*'s two-year bright line test and instead held that the enforcement of a non-compete supported by continued employment requires an individualized, case-by-case assessment. The court reasoned that the Illinois Supreme Court would likely reject the "bright line" test. The federal district court for the Southern District of Illinois in *Apex Physical Therapy v. Ball et al.*, Case No. 3:17-cv-119 (Nov. 3, 2017) refused to dismiss claims against two former employees for breach of their restrictive covenants finding the Illinois Supreme Court would most likely reject the arbitrary two year bright-line rule in favor a fact-specific, totality-of-the-circumstances approach to the question of whether there was adequate consideration for the restrictive covenant agreement.

Effective January 1, 2017, California's enacted Labor Code Section 925 restrains the ability of employers to require employees to litigate or arbitrate employer disputes outside of California or under the laws of another state, subject to certain exceptions. The statute applies to any agreement that is a condition of employment. Few courts have yet to address the statute because it applies only to agreements entered into, modified, or extended on or after January 1, 2017. One court found the statute inapplicable because the former employee did not agree to the forum selection clause at issue while he was a resident of California. See *Mechanix Wear, Inc. v. Performance Fabrics, Inc.*, No. 2:16-cv-09152-ODW (SS), 2017 WL 417193 (C.D. Cal., Jan. 31, 2017).

Nonetheless, federal district courts continue to uphold valid and enforceable forum selection clauses regardless whether the agreement at issue involves non-competition or other restrictive covenants, even over objections that the forum selection clause purportedly violates any applicable state policies against non-competes. See, e.g., *Mostipak v. Badger Daylighting Corp.*, No. 217CV00247MCECKD, 2017 WL 4310677 (E.D. Cal. Sept. 28, 2017).

4. New State Legislation Regarding Restrictive Covenants

Oregon enacted new legislation in 2017 that renders non-competition and non-solicitation covenants void and legally unenforceable for home care workers. West Virginia enacted new legislation that limits non-competes for physicians to one year durations and with geographical restrictions of 30 road miles from the physician's primary place of practice. West Virginia's new law provides exemptions for physicians who are shareholders, owners, partners, members, or directors of a health care practice.

On June 3, 2017, Nevada amended Revised Statute 613, which governs non-competition agreements. The new law adds requirements to the enforceability and validity of non-competition agreements, and importantly, now allows courts to "blue-pencil" non-competition agreements, overturning Nevada Supreme Court's recent decision in *Golden Road Motor Inn, Inc. v. Islam*. The new law also provides certain limitations on the scope of customer non-solicitation covenants. The new law further provides that a non-competition agreement is only enforceable during the time in which the employer is paying the employee's salary, benefits, or equivalent compensation if an employee is terminated because of a reduction in force, reorganization, or similar restructuring.

Pennsylvania and New Jersey both introduced bills that would dramatically limit businesses' powers to sign workers to non-competes. These proposed bills are longshots to pass but could be models for other states to follow or for defendants to argue against non-competes.

5. Vermont's New Social Media Legislation

Vermont joined the growing number of states that have enacted social media privacy laws regulating the use of social media by employers and educational institutions. The bill was signed by Governor Phil Scott on May 17, 2017, and went into effect on January 1, 2018.

For applicants and employees, Vermont's new social media law prohibits the required or requested (i) turnover of employee personal account login; (ii) access of account in employer's presence; (iii) divulging of social media content to employer; or (iv) change of privacy settings. An employer may not require an employee or applicant to add anyone to a contacts list. Retaliation against an employee who exercises these rights is also prohibited.

Vermont's new social media law does allow, however, social media access when required for compliance with legal and regulatory obligations or investigating alleged unauthorized transfer or disclosure of proprietary information, unlawful harassment, threats of violence, or discrimination. Law enforcement agencies are also permitted to request or require access for screening or fitness determinations and investigations. Employers may request or require turnover of login information for an employer-issued device.

There are no remedies mentioned under Vermont's social media law. One notable aspect of the law is that any agreement by an employee to waive his or her rights under the statute is invalid.

Given the increasing pervasiveness of social media in the workforce, employers need to stay informed of the varied and ever-evolving legal requirements governing employee use of social media. To provide a starting point for that analysis, we have updated our convenient, one-stop Desktop Reference surveying existing social media privacy laws: "Social Media Privacy Legislation: What Employers Need to Know Desktop Reference."

6. The U.S. Supreme Court Declines Review of Two Notable 9th Circuit CFAA Cases

One of the significant developments in 2017 regarding computer fraud law involved things that didn't happen. Specifically, the U.S. Supreme Court declined to review two closely watched computer hacking cases, *Nosal v. U.S.*, 828 F.3d 865 (9th Cir. 2016) and *Power Ventures, Inc. v. Facebook, Inc.*, 844 F.3d 1058 (9th Cir. 2016).

In *Nosal*, the 9th Circuit Court of Appeals held that an employee whose computer access credentials were affirmatively revoked by his employer acted "without authorization" in violation of the Computer Fraud and Abuse Act ("CFAA") when he and/or his former employee co-conspirators used the login credentials of a current employee to gain access to the employer's computer systems.

In *Power Ventures*, the 9th Circuit found that Power Ventures (a third-party platform that aggregated information from users' various social media accounts) violated the CFAA when it continued to access and scrape data from Facebook's servers "after receiving written notification from Facebook" and circumventing certain network barriers implemented by Facebook.

These cases had the potential to have a significant influence on scope and interpretation of what constitutes authorized access under the CFAA. Indeed, the Supreme Court has yet to weigh in on the over 30-year old computer fraud statute. By declining to review *Nosal*, the Supreme Court leaves a growing circuit split involving the scope and applicability of the CFAA to former employees that access and/or misuse computer data without permission.

7. ABA Encourages Encryption of Emails When Transmitting Confidential Client Information

The American Bar Association issued an Ethics Opinion in the Spring of 2017 stressing that lawyers must make reasonable efforts to prevent inadvertent or unauthorized access to confidential information relating to the representation of their clients. The ABA recognized that in the age of constant cybersecurity threats, law firms are targets for hackers for two reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

In examining the applicable Model Rules to explain what factors constitute reasonable efforts when using technology to communicate with clients, the Opinion specifically mentions trade secrets lawyers, noting that they handle client matters involving proprietary information that "may present a higher risk of data theft." Trade secrets lawyers must, on a case-by-case basis, analyze how they communicate electronically about client matters and "particularly strong protective measures, like encryption, are warranted in some circumstances."

The Opinion makes clear that lawyers must have an open exchange of communication with their clients about the security measures their firms are taking to safeguard the clients' confidential information. They must recognize that the determination of whether they are making reasonable efforts in enhancing their cybersecurity is a fact-based analysis to be made on a case-by-case basis and may not be uniformly employed.

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