SEYFARTH SHAW LLP
ATTORNEYS

Management Alert

Top 10 2011 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law

We have compiled a list of the top 2011 developments/headlines in trade secret, computer fraud, and non-compete law. While large jury verdicts and criminal prosecutions garnered a significant amount of attention, there were also a number of significant state and federal court decisions that have altered the landscape of trade secret, computer fraud, and non-compete law in various jurisdictions. For example, in *Illinois*, the state supreme court broadened the discretion and increased the flexibility of trial courts in determining the reasonableness of non-competes. Also, in *Texas*, the state supreme court made it easier to enforce non-competes by opening the door for other consideration (apart from access to trade secrets) to serve as consideration for a non-compete. On the federal front, the *Ninth Circuit* in *United States v. Nosal* found that an employee may be liable under the Computer Fraud and Abuse Act ("CFAA") for violations of an employer's computer use policies (the court has since *granted en banc review* and heard oral arguments in December 2011) and there remains a circuit split on the applicability of the CFAA in the workplace.

There have also been significant legislative efforts to modify trade secret, computer fraud, and non-compete law in various jurisdictions. For instance, in *Georgia*, the Restrictive Covenant Act illustrates the state's fundamental change in public policy toward enforcement of restrictive covenant agreements, including non-competes and non-solicits. In *New Jersey*, the state recently adopted its own version of the Uniform Trade Secrets Act. In *Massachusetts*, a non-compete reform bill has undergone significant review, comment, and revision regarding standing, attorneys' fees, and consideration for non-compete agreements. On the federal front, the *Patent Reform Act* was passed and there have also been efforts to modify the CFAA.

In 2012, we expect to see more cases involving the intersection between cloud computing/social networking and trade secrets. With the proliferation of electronic information used to conduct business and as more data is housed remotely and outside company servers, courts have begun addressing the extent to which companies retain ownership of such information and can sue for the misuse of such information.

We also expect to see more cases addressing trade secret preemption and the protection (or lack thereof) of confidential information. Some courts have also continued to insist on greater specificity in pleadings on trade secret claims and the strict identification of alleged trade secrets in discovery by plaintiffs to frame the issues in dispute. Disputes concerning the enforcement of forum selection and choice of law provisions in non-compete disputes will also remain prevalent. Lastly, we also expect to see more cases involving the interplay between employee confidentiality obligations and employees' rights under the *Sarbanes-Oxley Act*.

Below is our listing of top developments/headlines in trade secret, computer fraud, and non-compete law for this past year in no particular order:

1. Significant State Supreme Court Decisions

Several significant state supreme court decisions have addressed the construction of enforceable non-compete provisions. The *Virginia Supreme Court* required employers to demonstrate that the non-compete is no broader than necessary to

protect the employer's "legitimate business interests" and does not "unduly burden" the ex-employee's right to earn a living. The *Texas Supreme Court* continued the state's movement toward non-compete enforceability and for the first time approved of something other than providing an employee confidential business information as appropriate consideration for a non-compete agreement (i.e. stock options). The *Illinois Supreme Court* also made non-compete enforceability easier by granting Illinois trial courts significant discretion to consider "the totality of the facts and circumstances of the individual case" when assessing whether a "legitimate business interest exists." The *Idaho Supreme Court* found that a two-year non-compete agreement executed in connection with the sale of a business was enforceable under California law and could be narrowed within a scope that was reasonably necessary to protect the goodwill of the sold business. The *Montana Supreme Court* ruled that an employer will not be permitted to enforce a non-compete provision in an employment agreement where the employer was solely responsible for ending the employment relationship. The *Oklahoma Supreme Court* recently held that non-compete agreements are reviewable by a court, even if the agreement contains an arbitration clause and there is no claim as to the validity or enforceability of the arbitration clause, and further held that provisions that are contrary to Oklahoma's statutory limitations on non-competes may result in the court invalidating the entire non-compete.

2. Expanded Role Of The International Trade Commission in Preventing Foreign Trade Secret Theft

The Federal Circuit's decision in *TianRui Group Co. v. International Trade Commission* confirmed that the *ITC has jurisdiction to address trade secret claims*, even when the alleged wrongful conduct occurs in a foreign country. The court found that the ITC has jurisdiction through section 337 of the Tariff Act, which prohibits "[u]nfair methods of competition and unfair acts in the importation of articles … into the United States…." U.S. companies now have a meaningful remedy to address concerns about the extraterritorial protection of trade secrets.

3. Continuing Developments in Legislation

New Jersey, one of the four remaining states that had not adopted some or all of the provisions of the Uniform Trade Secrets Act (UTSA), *recently passed the state's own version of the UTSA*. New Jersey's Trade Secrets Act was *recently signed into law* on January 9, 2012.

Senators Kohl (D-WI) and Coons (D-DE) also *introduced a federal bill* in October 2011 that would create a new federal private right of action for trade secret owners.

Georgia passed the *Restrictive Covenant Act*. The Act has three significant implications: (1) it creates statutory presumptions that restraints two years or less in duration are reasonable in time and restraints more than two years are unreasonable; (2) it eases the drafting requirements for specific restrictive covenants; and (3) it permits Georgia courts to "blue pencil" (i.e. partially enforce) restrictive covenants that otherwise would be overbroad and, therefore, completely unenforceable under existing Georgia case law. At least *one Georgia court has interpreted* the new Act as providing courts discretion to re-write restrictive covenants to make them enforceable, rather than merely providing the authority to remove overbroad covenants.

The Massachusetts legislature *heard testimony* in September 2011 regarding a non-compete bill that aims to modify the common law pertaining to non-compete agreements and to simultaneously afford greater procedural protections to those affected by the contractual restrictions on mobility in employment. Changes include the elimination of a threshold that confined the use of non-compete agreements to employees earning over $75,000 per year in favor of a requirement that courts more broadly consider the economic impact on an affected employee before deciding whether to enforce a non-compete agreement. Bill 2293 also provides for mandatory attorneys' fees to employees. However, an employer can avoid paying fees if the court determines that it took "objectively reasonable efforts to draft the rejected or reformed restriction so that it would be presumptively reasonable." Finally, the new bill would permit the signing of mid-employment non-compete agreements so long as "fair and reasonable" consideration is provided to the affected employee To date, the Massachusetts legislature has yet to approve the proposed *bill*.

There have also been efforts to amend the CFAA. Proposed amendments to the CFAA that would restrict the definition of

"exceeds authorized access" have recently been the subject of debate. U.S. Senator Patrick Leahy (D-VT) *proposed a bill* that excluded violations of computer use policies and terms of service agreements from "exceed[ing] authorized access" in violation of the statute. The Department of Justice has taken a *pro-employer stance* and objected to CFAA changes, while emphasizing the importance of holding employees liable for violations of computer use policies to protect our nation's economic security.

Additionally, the American Invents Act of 2011 was signed into law. The *America Invents Act of 2011* changes the U.S. Patent system to a "first-to-file" format. More importantly, it allows companies to defend against alleged patent infringement when they practice information they elect to keep as trade secrets, but are sued for infringement because another inventor filed for a patent first. Companies can keep information related to their inventions a trade secret and retain these "prior use rights" as long as they have "commercially" practiced their invention.

4. Significant Jury Trials Verdicts and Criminal Sentences

In 2011 we saw several significant trade secret jury trial decisions. The second jury in the contentious *Barbie vs. Bratz* case *awarded more than $80 million in damages*, plus attorneys' fees and treble damages to MGA for Mattel's alleged trade secret misappropriation; *a reversal of the case's first jury trial* that resulted in a large jury verdict in favor of Mattel. *Mattel is appealing the decision* and we expect to see more litigation in this case in 2012.

The jury in *Pacesetter Inc. v. Nervicon Co. awarded more than $2.3 billion in damages* (later pared down to $947 million by the trial court judge) to St. Jude Medical for a former employee's theft of confidential technical information about the company's medical devices. Additionally, the jury in *DuPont v. Kolon awarded more than $919 million in damages* for a former employee's theft of information regarding DuPont's anti-ballistic Kevlar fiber.

The *TCW Group, Inc. v. Gundlach* case, followed with great interest in the financial community ended in split jury verdicts, after each party had sought hundreds of million of dollars in damages against the other. The jury found the former investment chief liable for alleged trade secret misappropriation and breach of his fiduciary duty but did not award any damages on the fiduciary duty claim. Instead, the jury assigned the determination *of damages for trade secret theft to the judge*. The jury awarded the former investment chief $66.7 million for back pay after his termination. The parties *recently settled* the litigation pursuant to a confidential settlement, prior to the court's ruling on the amount of damages to award on the trade secret claim.

Regarding criminal prosecution, an *ex-Goldman Sachs programmer* was sentenced to more than 8 years in prison for the theft of confidential information regarding the company's trading system. Additionally, an *ex-Dow AgroSciences scientist* was sentenced to more than 7 years in prison for the theft of secret information about organic insecticides.

5. Emerging Areas in Social Media and Cloud Computing

The explosion of cloud computing and the ubiquity of social media has increased the risks and vulnerabilities in protecting valuable company data and prized trade secrets. Companies utilizing cloud-computing services must employ *effective measures to protect and secure* their intellectual property. Issues have also arisen regarding the ownership of employee created social media content and passwords. For example, the current *PhoneDog v. Noah Kravitz* case in the Northern District of California involves a dispute regarding the ownership of an *employee's Twitter account*, specifically the account's follower list and password. The outcome of this case will be closely monitored by employers, especially in light of the 2010 case *Sasqua Group v. Courtney*. In that case, a New York district court found that an allegedly misappropriated customer list was not a trade secret because the information could be easily located through Google and LinkedIn searches.

A New Jersey district court in *Syncsort Incorporated v. Innovative Routines, International, Inc.*, 2011 U.S. Dist. LEXIS 92321, (D.N.J. August 18, 2011), however, found that *posting information on the internet* might not necessarily void that information's trade secret status. The takeaway is that prior methods to maintain confidentiality may no longer be viable with the heightened connectivity of social media and cloud computing. More recently, *a Pennsylvania federal court* held that an employer may claim ownership of its former executive's LinkedIn connections where the employer required the executive to

open and maintain an account, the executive advertised her and her employer's credentials and services on the account, and where the employer had significant involvement in the creation, maintenance, operation, and monitoring of the account.

6. Applicability of the Computer Fraud and Abuse Act In The Workplace

On April 28, 2011, the Ninth Circuit Court of Appeals *held* in an important decision upholding legal protections for employer data that employees may be held liable under the federal Computer Fraud and Abuse Act (18 U.S.C. 1030 et seq.) in cases where employees steal or remove electronic files or data in violation of their employers' written computer-use restrictions. The Ninth Circuit found that a former employee "exceeds authorized access" to data on his employer's computer system under the CFAA where the employee takes actions on the computer that are prohibited by his employer's written policies and procedures concerning acceptable use (e.g. prohibitions against copying or e-mailing files to compete or help a third party compete with the employer).

Subsequently in October 2011, the Ninth Circuit Court of Appeals *ordered* that *U.S. v. Nosal* be reheard by en banc panel and that the "three-judge panel opinion [in *U.S. v. Nosal*, 642 F.3d 781 (9th Cir. 2011)] shall not be cited as precedent by or to any court of the Ninth Circuit." Accordingly, the ability of employers to sue employees who violate computer usage policies by stealing company data under the CFAA in the Ninth Circuit is again in question. This comes after the three-judge panel *Nosal* opinion was beginning to gain *momentum* in district courts in the Ninth Circuit. *Oral argument* occurred in December and a decision should be issued with the coming months.

Should the Ninth Circuit reverse the decision, the U.S. Supreme Court may take up the decision as a reversal would cement the conflict between the Ninth Circuit and other circuits, such as the Fifth and Eight Circuits. The U.S. Supreme Court's decision to take up the case may also be impacted by whether Congress passes amendments to the Computer Fraud and Abuse Act which would curtail the ability of the government and companies to sue for violation of usage policies, including violations of social media sites terms of service.

7. Forum Selection and Choice of Law Provisions

Courts around the country continue to split as to the circumstances under which the parties' choice of law and forum selection provisions set forth in non-compete agreements will be honored. The determination of what law to apply and the proper forum for the suit can often be dispositive in non-compete litigation. A *Nebraska federal district court* transferred a non-compete enforcement case to Minnesota because the court decided that the plaintiff's choice of forum was insufficient to prevent transfer from Nebraska even though only one of the several agreements at the subject of the action contained the forum selection and choice of law provisions. Additionally, an *Arizona federal district court* recently refused to enjoin violations of a non-compete agreement with a Washington choice law provision because of Arizona's greater interest in the case and the state's "fundamental policy."

8. Protection for Whistleblowers Under The Sarbanes-Oxley Act For Disclosure Of Company Confidential Information?

The U.S. Department of Labor's Administrative Review Board issued a ruling in *Vannoy v. Celanese Corp.*, which *further expands the scope of the whistleblower protection provision* in Section 806 of the Sarbanes-Oxley Act (SOX). In particular, the ruling presents the risk that a whistleblower's violation of confidentiality rules and misconduct that could harm employers may still qualify as protected activity in certain circumstances. Thus, this may provide employees with a license to take company data and allow them to attempt to immunize themselves from the consequences for their wrongful acts. *The ARB ruled that a whistleblower's misappropriation of confidential information in violation of a confidentiality agreement– which could irreparably harm the company and damage many other employees – might still qualify as protected activity.*

The ARB directed the ALJ to conduct an evidentiary hearing to determine whether the information the complainant misappropriated was the kind of "original information" Congress intended to protect and whether the method of transfer

of information was protected lawful conduct within the scope of SOX. In this regard, the ARB indicated that while Complainant's conduct may have violated company policy, no charges were brought in connection with his conduct. However, the ARB did not otherwise define "lawful conduct" in this context.

9. Trade Secret Preemption and Protection of Confidential Information

Defendants in trade secret cases will often seek to invoke trade secret preemption to attempt to dismiss common law claims that are based on the same or similar facts as the claim for trade secret misappropriation in the early stages of the litigation. The problem with the premature dismissal of claims is that if the finder of fact does not find that the information misappropriated rises to the level of a trade secret, the plaintiff can be precluded from obtaining any relief on the common law claims to protect confidential information or based upon facts that separately actionable. This effectively may cut off a plaintiff's right to pursue common law claims, such as tortious interference with contract or conversion, that are well established legal claims. A California federal district court in *Amron International Diving Supply, Inc. v. Hydrolinx Diving Communication*, 2011 U.S. Dist. LEXIS 122420 (S.D. Cal Oct. 21, 2011) recently refused to apply trade secret preemption until it was first determined whether the allegedly misappropriated information constituted a trade secret. We expect to see more trade secret preemption decisions in California and the rest of the country in 2012 as courts continue to grapple with this knotty issue.

10. Stricter Pleading Requirements and Pre-Discovery Identification Of Trade Secrets

Some courts across the nation have insisted on stricter pleading of trade secret claims as well as the disclosure of the alleged misappropriated trade secret by plaintiffs before discovery is permitted. For instance, a *Colorado federal court* held that before the plaintiffs may compel discovery, they must file a complaint that "describe(s) the *actual* equipment, methods, software or other information" they claim as trade secrets. Plaintiffs' "*general allegations and generic references* to products or information are insufficient to satisfy the reasonable particularity standard." Other *courts* have been more forgiving in the level of detail required to be pled in the complaint. Another recent *case* required the disclosure of the alleged misappropriated trade secrets with particularity in *federal court* before the defendant would be required to respond to plaintiff's discovery. We expect to see more cases addressing these significant issues in 2012.

Please continue following our blog, *www.tradesecretslaw.com*, this year. We plan to increase the frequency of our postings by including more authors (including special guest authors (e.g. law professors, clients, and forensic experts), enhancing the visual effectiveness of posts (e.g. more pictures, charts, and video), as well as providing resource material (e.g. applicable statutes, significant cases and links, and webinars). Thank you for your continued support of the blog.

By: *Robert Milligan* and Joshua Salinas

Robert Milligan is a partner in Seyfarth's Los Angeles office and Joshua Salinas is a law clerk in Seyfarth's Los Angeles office. If you would like further information, please contact your Seyfarth attorney, Robert Milligan at rmilligan@seyfarth.com or Joshua Salinas at jsalinas@seyfarth.com.