SEYFARTH SHAW LLP
ATTORNEYS

Trading Secrets

A Law Blog on Trade Secrets, Non-Competes, and Computer Fraud

2011 - Year in Review

Trading Secrets

Table of Contents

About Us ..... A

2012 Trade Secrets Webinar Series ..... B

Our Authors C

Trading Secrets Blog Index ..... D

Trading Secrets Blog Posts ..... E

Trading Secrets

Dear Clients and Friends,

2011 was a successful year for our Trading Secrets blog. Launched in 2007, the blog has continued to grow in both readership and postings. Content from Trading Secrets has appeared on newsfeeds such as Lexology and iTechLaw, IP.com's "Securing Innovation" Blog, and Kevin O'Keefe's "Real Lawyers Have Blogs," one of the leading sources of information and commentary on the use of blogs. We are pleased to provide you with this 2011 Year in Review which compiles our significant blog posts from 2011 and highlights our blog's authors. For a general overview, we direct you to our Top 10 2011 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2011 Trade Secrets Webinar Series - Year in Review blog entry which provide a summary of some of the key cases and legislative developments in 2011, as well as practical advice on maintaining trade secret protections.

As the specific blog entries that are contained in this Review demonstrate, our blog authors stay on top of the latest developments in this area of law and provide timely and entertaining posts on significant new cases, legal developments, and legislation. In 2012, 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 provide resource material (e.g. applicable statutes, significant cases and links, and webinars) on the blog.

In addition to our blog, Seyfarth's dedicated Trade Secrets, Computer Fraud, and Non-Competes group hosts a popular series of webinars, which address significant issues facing clients today in this important and ever changing area of law. In 2011, we hosted six webinars: *Trade Secrets in the Financial Services Industry*, *The Anatomy of a Trade Secret Audit*, *Georgia's New Non-Compete Statute*, *Managing and Protecting Trade Secrets in the Brave New World of Cloud Computing and Social Media*, *Choosing the Right IP Protection: Patent, Trade Secret or Both?*, *and Key Considerations Concerning Trade Secrets and Non-Competes in Business Transactions*. For those who missed any of the programs in 2011's webinar series, the webinars are available on compact disc upon request and CLE credit is available for attorneys licensed in Illinois, New York or California. If you are interested in receiving CLE credit for viewing recorded versions of the 2011 webinars, please e-mail CLE@seyfarth.com to request a username and password.

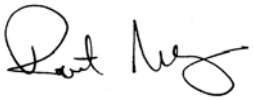
We kicked off the 2012 webinar series with a program entitled, "Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff," and had over 1000 registrants. More information on our upcoming 2012 webinars is available in program listing contained in this Review. Our highly successful blog and webinar series further demonstrate that Seyfarth Shaw's national Trade Secrets, Computer Fraud & Non-Competes Practice Group is one of the country's pre-eminent groups dedicated to trade secrets, restrictive covenants, computer fraud, and unfair competition matters.

Thank you for your continued support.

Michael Wexler

Chicago Partner and Practice Group Chair

Robert Milligan



Los Angeles Partner and Trading Secrets Editor

Trading Secrets

2012 Trade Secrets Webinar Series

Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff
January 26, 2012

Sarbanes-Oxley and Maintaining Trade Secrets and Confidential Information
March 2012

Trade Secret Practice: Specific Pleading and Identification Requirements
April 2012

Trade Secrets in the Financial Services Industry
May 2012

Trade Secrets and Non-US Based Companies
June 2012

Legislative Update: Georgia's Non-Compete Statute, Other Legislation Updates
July 2012

How To Conduct An Effective Entrance and Exit Interview To Protect Trade Secrets
September 2012

California Year in Review/Hot Topics
November 2012

Our Authors

Kate Perrelli is a partner in the firm's Boston office and Chair of Seyfarth's Litigation Department. She is a trial lawyer with over 20 years of experience representing regional, national, and international corporations in the financial services, transportation, manufacturing, technology, pharmaceutical, and staffing industries. Her commercial practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, unfair competition and complex commercial disputes, including dealer/franchise disputes, and contract disputes.

Mike Wexler is a partner in the firm's Chicago office and Chair of the national Trade Secrets, Computer Fraud, and Non-Competes Practice Group. His practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, unfair competition, complex commercial disputes, intellectual property infringement, and white collar criminal defense in both federal and state courts. A former state prosecutor, Mr. Wexler's extensive investigatory experience and considerable jury trial practice enables him to advise clients with regard to potential disputes and represent clients through and including a determination of their rights at trial.

Robert Milligan is the editor of the blog and a partner in Seyfarth Shaw LLP's Los Angeles office in the Commercial Litigation and Labor and Employment Departments. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation and other intellectual property theft, real estate litigation, insurance bad faith, invasion of privacy, products liability, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower cases, bankruptcy and other business torts. Mr. Milligan has represented clients in state and federal courts in complex commercial litigation and employment litigation. His experience includes trials, binding arbitrations and administrative hearings, mediations, as well as appellate proceedings.

Paul Freehling is a partner with the Chicago office of Seyfarth Shaw LLP. With more than 40 years of professional experience, Mr. Freehling has tried cases in both state and federal courts and before arbitration tribunals, and he has argued before three U.S. Circuit Courts of Appeal as well as the Illinois Appellate Court. In addition to his practice in a wide variety of complex litigated matters, Mr. Freehling has significant experience in alternative dispute resolution both as a neutral and as an advocate. He has been appointed to the Roster of Distinguished Neutrals by the CPR Institute for Dispute Resolution, the premier organization for alternative methods of dispute resolution.

Joshua Salinas is an attorney in the Los Angeles office of Seyfarth Shaw LLP, practicing in the areas of trade secrets, restrictive covenants, computer fraud, and commercial litigation. Joshua's experience includes the prosecution and defense of trade secret misappropriation and unfair competition claims.

Scott Humphrey is a partner in Seyfarth Shaw LLP's Trade Secrets, Restrictive Covenants and Corporate Espionage Group. He serves on the Group's National Steering Committee and has successfully prosecuted and defended trade secrets and restrictive covenant cases throughout the United States. In doing so, Scott has successfully obtained and defeated temporary restraining orders,

preliminary injunctions and permanent injunctions involving trade secret and restrictive covenant matters for clients in the technology, securities and financial services, transportation, electronics, software, insurance, healthcare, consumer products, and manufacturing industries. Scott has also written and reviewed restrictive covenant agreements for both Fortune 100 and small privately held corporations.

David Monachino is a partner in the Commercial Litigation, Labor, Employment, Trade Secrets, Product Liability, and Business Torts groups in the New York office of Seyfarth Shaw LLP. His civil litigation practice covers the full spectrum of litigation services, including litigation management, motion practice, jury trials, and appeals before federal and state courts and administrative agencies, in employment discrimination, restrictive covenants, trade-secret theft, corporate espionage, unfair competition, class action, privacy rights, and complex commercial and real estate litigation.

Scott Schaefers is a partner in Seyfarth Shaw's Chicago office, where he specializes in commercial litigation, antitrust and trade regulation, and trade secrets and restrictive covenants. He has significant experience in representing commercial and non-for-profit clients in a wide range of litigation matters.

Eddy Salcedo is an experienced first-chair trial lawyer and is currently in the New York office of Seyfarth Shaw LLP. He has successfully represented a wide range of clients in trade secret, enforcement of non-competition agreements, partnership disputes, and trademark infringement litigations. He has also served as trial counsel for parties in construction and real estate development disputes, contract disputes, and general commercial and civil litigation. His experience includes state and federal bench and jury trials, appeals and arbitrations. He has appeared as counsel of record in the Appellate Division and the Court of Appeals of New York (New York's highest state court), and the U.S. Court of Appeals for the Second Circuit. Mr. Salcedo is a native Spanish speaker.

Daniel Hart is an associate in the Atlanta office of Seyfarth Shaw LLP. Mr. Hart also regularly advises employers on the enforceability of restrictive covenants in employment agreements and has represented employers in litigation involving breach of restrictive covenants and misappropriation of trade secrets.

Scott Humphrey is a partner in Seyfarth Shaw's Chicago office. He is a member of the Trade Secrets, Computer Fraud & Non-Competes Practice Group, and currently serves on the group's National Steering Committee. As a member of the Trade Secrets Group, Mr. Humphrey has successfully obtained and defeated temporary restraining orders, preliminary injunctions and permanent injunctions in jurisdictions throughout the United States and for clients involved in technology, securities and financial services, pharmaceuticals, transportation, electronics, health care, media talent, business consulting, insurance and consumer products.

Marcus Mintz is an associate in the Litigation Department of Seyfarth Shaw LLP. His practice includes litigation of trade secrets cases, franchise and dealer disputes, fraud cases, shareholder disputes, commercial real estate litigation, and general litigation within the employee/employer context, including suits for breach of restrictive covenants and theft of proprietary business information.

Trading Secrets

Bob Stevens is a partner in the Labor and Employment and Trade Secrets, Computer Fraud and Non-Competes Groups of Seyfarth Shaw LLP. He has over 15 years of experience representing public and privately held companies throughout the United States in employment related litigation. He concentrates his practice on litigation and counseling matters involving employment discrimination, restrictive covenant, trade secret, and wage and hour issues.

Erik Weibust is a senior associate in the Litigation Department of Seyfarth Shaw LLP, and is a member of the Securities and Financial Litigation and Trade Secrets, Computer Fraud & Non-Competes practice groups. He is also an active member of the firm's national Sarbanes-Oxley Whistleblower Team.

Gary Glaser is a partner in the New York office practicing in the area of labor and employment law and litigation. In addition to his litigation practice, Mr. Glaser also counsels and represents clients in litigation involving corporate espionage / noncompete / restrictive covenant / trade secrets issues; wage and hour issues; employment agreements; human resources policies and procedures; management training regarding sexual harassment and other EEO and labor law issues.

Molly Joyce is a partner in the Chicago office of Seyfarth Shaw LLP. She practices in the area of commercial litigation, with particular experience in cases involving claims of breach of contract, fraud, breach of fiduciary duty, unfair competition, trade secret misappropriation, product liability, negligence and antitrust violations.

Ryan Malloy is an associate in the Commercial Litigation and Construction Practice Groups of Seyfarth Shaw LLP. He handles complex commercial litigation matters, including the defense and litigation of partnership disputes, banking and finance matters, breach of contract suits, and tort claims.

James McNairy is a partner in the Sacramento office of Seyfarth Shaw LLP. He is a member of the Litigation department and his practice focuses on commercial, trade secret, and employment litigation. Mr. McNairy prosecutes and defends trade secret misappropriation claims, including obtaining associated expedited discovery and relief.

Jason Stiehl is a partner in the Litigation Department of Seyfarth Shaw LLP. Mr. Stiehl represents clients in complex commercial disputes involving trade secrets and restrictive covenants, unfair competition, corporate espionage, contract, and intellectual property claims in both state and federal court. He also has extensive nationwide class action experience, including involvement in multi-district litigation.

Rebecca Woods' practice is two-fold, focusing on counseling and litigation. She counsels clients who have business disputes on how to avoid, or how to prepare for, litigation. She combines her knowledge of clients' businesses and business goals with her expertise in litigation strategies and potential outcomes to provide clients the information they need to decide the best next steps.

Trading Secrets

2011 Year-End Blog Review

Trade Secrets

- Top 10 2011 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law
  January 17, 2012 by Robert Milligan and Joshua Salinas
- Does A Trade Secret Plaintiff Have To Disclose Its Trade Secrets Prior To The Commencement Of Discovery In California Federal Court?
  January 13, 2012 by Joshua Salinas
- California Federal Court Holds That Trade Secret Misappropriation Defendant Need Not Respond To Plaintiff's Discovery Requests Until Provided With Identification Of Information Claimed To Have Been Stolen
  January 12, 2012 by Paul Freehling
- After Ohio Jury Finds Trade Secret Misappropriation But Awards Zero Damages, Trial Judge Enters Injunction Order But Sets Royalty Payment As Alternative
  January 10, 2012 by Paul Freehling
- US Companies Have Options Against Chinese Companies For Trade Secret Misappropriation
  January 9, 2012 by Eddy Salcedo
- At Long Last, New Jersey Passes Trade Secrets Act
  January 9, 2012 by David Monachino
- What Does It Take to Plead a Claim for Trade Secret Misappropriation Claim Under the Uniform Trade Secrets Act?
  December 23, 2011 by David Monachino
- 2011 Trade Secrets Webinar Series - Year in Review
  December 20, 2011 by Robert Milligan
- Use Of Even A Small Amount Of Commercially Valuable Confidential Information Obtained From Someone Without Authority To Convey It Constitutes Actionable Trade Secret Misappropriation According To Eighth Circuit
  December 19, 2011 by Paul Freehling
- Colorado Magistrate Judge Outlines Stringent Pleading Requirements Which Must Be Satisfied Before Plaintiffs Alleging Trade Secret Misappropriation Can Compel Responses To Discovery Requests; Judge Also Encourages Filing Pleadings Under Seal
  December 8, 2011 by Paul Freehling
- Massachusetts Judge Finds Statutory Trade Secrets Misappropriation, Despite Contrary Jury Verdict in Parallel Common Law Action, and Awards Plaintiff Draconian Injunctive Relief and Millions of Dollars in Damages, Fees and Costs
  November 30, 2011 by Paul Freehling
- Social Media and Trade Secrets Collide: Whose Twitter Is It, Anyway?
  November 18, 2011 by Gary Glaser

Trading Secrets

- At Long Last, New Jersey Is Poised To Pass The "New Jersey Trade Secrets Act"
  November 16, 2011 by David Monachino
- Failure to Specifically Identify Trade Secrets in a Complaint Does Not Bar a Complaint in New Jersey Federal Court
  October 27, 2011 by David Monachino
- Plaintiff Receives Million Plus Attorneys' Fees Award In Trade Secret Dispute Despite Small Damages Award
  October 24, 2011 by Paul Freehling
- Employers' Obligation to Defend and Indemnify Rogue Employees In California?
  October 14, 2011 by Robert Milligan and Joshua Salinas
- New Federal Trade Secret Bill Introduced
  October 7, 2011 by Robert Milligan
- Trade Secrets Along the Time-Space (Internet) Continuum or "Lost in Translation"
  September 6, 2011 by Jason Stiehl
- "Internet Communications" Alone Insufficient To Invoke Florida Long-Arm Statute Against Lindsay Lohan In Trade Secrets Misappropriation Suit
  July 21, 2011 by Eddy Salcedo
- California Federal Court Recently Invokes "Trade Secret" Exception to California's Anti-Noncompete Statute To Effectively Blue Pencil Noncompete Agreement
  July 14, 2011 by Scott Schaefers
- Wiener v. Wiener: A Wiener Controversy Of A Different (Trade Secrets) Sort
  June 27, 2011 by James McNairy
- Affidavits Not Enough to Obtain Injunctive Relief in Alleged Raiding Case
  July 26, 2011 by Marcus Mintz
- Award of Damages for Misappropriation Does Not Preclude Also Awarding Injunctive Relief
  June 22, 2011 by Paul Freehling
- Colorado Statute of Limitations For Misappropriation Of A Trade Secret Begins To Run Upon Knowledge That It, Or Even A Related Trade Secret, Has Been Misappropriated
  June 19, 2011 by Paul Freehling
- Electronic "Redactions" Not Always Effective: Greater Caution In Dealing With Sensitive Materials In Trade Secret Cases Necessary
  June 6, 2011 by Eddy Salcedo
- Delaware Court Enjoins Use of Ex-Employers Trade Secrets
  April 16, 2011 by Paul Freehling
- Michigan Court Orders Corporation to Reveal Facts Regarding Potential Misappropriation
  April 1, 2011 by Paul Freehling
- Court Of Federal Claims Details How To Compute Damages For Misappropriation Of An Asset That Has No Readily Ascertainable Market Value
  March 8, 2011 by Paul Freehling
- Emails Sent By Employee To Attorney From Company Computer May Not Be Privileged
  February 28, 2011 by Seyfarth Shaw LLP

- Jury Must Decide Whether A Manufacturing Process That Is Disclosed In An Expired Patent And Is Not Concealed From Visitors To The Plant Constitutes A Trade Secret
  February 21, 2011 by Paul Freehling
- New Article On Trade Secret Litigation In State Courts Released
  February 15, 2011 by Robert Milligan
- Fitness Companies Spar Over Unauthorized Access Of Departing Employee's Personal E-mail Accounts
  January 25, 2011 by Robert Milligan and Josh Salinas

Computer Fraud and Abuse Act

- Employers May Have Sweat Equity In Their Executives LinkedIn Accounts, But Employees Score Win In War Over The Applicability Of The Federal Computer Fraud And Abuse Act In The Workplace
  January 5, 2012 by Scott Schaefers
- Key Computer Fraud and Abuse Act Case Heard By Ninth Circuit En Banc Panel: Can Rogue Employees Be Held Liable For Data Theft Under The Computer Fraud and Abuse Act?
  December 16, 2011 by Robert Milligan
- Department of Justice Takes Pro-Employer Stance On Amendments To Computer Fraud And Abuse Act: Employers Should Continue To Be Able To Hold Employees Liable For Violations Of Computer Usage Policies Under The Act"
  November 22, 2011 by Robert Milligan and Joshua Salinas
- Dead Again? Use of Computer Fraud and Abuse Act By Employers To Combat Employee Data Theft Limited By Ninth Circuit's Latest Ruling
  October 29, 2011 by Robert Milligan
- Liability Under Computer Fraud and Abuse Act For Violating Computer Use Policies Gains Momentum In Ninth Circuit
  October 6, 2011 by Robert Milligan and Joshua Salinas
- Ex-Employee Violated Duty Of Loyalty, Breached Non-Compete, And Committed Computer Fraud Act Violation, But New Employer Not Liable For Misappropriation Of Non-Trade Secret "Confidential Information"
  September 11, 2011 by Paul Freehling
- New York Federal Court Dismisses Computer Fraud and Abuse Act Claims For Defendant's Alleged Use Of "Supercookies" And "History Sniffing"
  September 4, 2011 by Robert Milligan and Joshua Salinas
- Outside Counsel Fees May Be a Qualified Loss to Meet the CFAA's $5000 Jurisdictional Requirement
  May 15, 2011 by David Monachino
- The Federal Computer Fraud and Abuse Act is Back in Play for Employer Suits Against Dishonest Employees in the Ninth Circuit
  May 2, 2011 by Scott Schaefers and Robert Milligan

- Private Information Stored On Electronic Devices Subject To Search By Law Enforcement If Arrested In California
  March 16, 2011 by Robert Milligan and Joshua Salinas
- Computer Fraud and Abuse Act Remains Viable Claim For Employers To Assert Against Employees Who Steal Company Data
  March 2, 2011 by Robert Milligan and Joshua Salinas
- District Court Holds That Computer Forensic Investigation Costs Satisfy "Loss" Requirement of Computer Fraud and Abuse Act
  February 9, 2011 by Robert Milligan and Joshua Salinas
- The Eleventh Circuit Splits with the Ninth Circuit in Interpreting the Computer Fraud and Abuse Act
  January 7, 2011 by Paul Freehling and Scott Schaefers

Non-Compete & Restrictive Covenants

- Oklahoma Supreme Court Nixes Overly Broad Non-Compete Agreement
  December 30, 2011 by Rebecca Woods
- Montana Supreme Court Holds That Employer May Not Enforce Non-Compete Agreement Where Employee Was Terminated Without Cause
  December 22, 2011 by Paul Freehling
- Can The Seller Of A Business Who Also Becomes Employed By Purchaser Be Held To Non-Compete Agreement Under California Law? The Idaho Supreme Court Says Yes
  December 14, 2011 by Molly Joyce
- Illinois Supreme Court Affirms Legitimate Business Interest Test For Restrictive Covenants And Provides Some Guidance On How To Analyze A Legitimate Business Interest
  December 1, 2011 by Scott Humphrey
- Virginia Employers Should Update Their Non-Compete Agreements In Light of New Virginia Supreme Court Ruling
  November 22, 2011 by Guest Author for TradeSecretsLaw.com
- Virginia Supreme Court Clarifies Obligations Of Employer Seeking To Enforce Non-Compete
  November 14, 2011 by Marcus Mintz
- Because Arizona's "Fundamental Policy" Regarding Non-Compete Clauses Is So Different From That Of The State Of Washington, Arizona Federal Court Refuses To Enforce Clause's Provision Calling For Applicability Of Washington State Law
  November 12, 2011 by Paul Freehling
- A Pennsylvania District Court Finds That A Non-Compete Agreement Is Not Subject To Automatic Stay in Bankruptcy
  November 8, 2011 by David Monachino
- Massachusetts Legislature Hears Testimony on Non-Compete Bill
  November 1, 2011 by Kate Perrelli, Erik Weibust, and Ryan Malloy
- Controlling The Forum: Nebraska Federal Court Transfers Non-Compete Declaratory Relief Action To Minnesota Federal Court
  November 1, 2011 by Paul Freehling

Trading Secrets

- Georgia Court Blue Pencils / Rewrites Overbroad Restrictive Covenant
  October 20, 2011 by Bob Stevens and Daniel Hart
- Federal Court Reverses Prior Decision on Retroactive Impact of New Georgia Restrictive Covenant Act
  August 14, 2011 by Dan Hart
- California Appellate Court Rules that Five-Year Employee Noncompete Agreement of Unlimited Geographic Reach is Enforceable as a Sanction Against Reticent Defendant
  July 20, 2011 by Scott Schaefers
- Does the New Georgia Restrictive Covenant Act Have a Retroactive Impact?
  July 18, 2011 by Bob Stevens
- The Unemployment Rate, Mismatched Skills, and ... Non-competes?
  July 5, 2011 by Michael Elkon
- Texas Supreme Court Allows Stock Options as Consideration for Non-Compete Agreements
  June 30, 2011 by Robert Milligan
- What Georgia's Restrictive Covenant Act Means - and Doesn't Mean - for Employers
  May 16, 2011 by Dan Hart
- Iowa - Sophisticated Employees Bound by Reasonable Restrictive Covenants; Plaintiff to Post $2 Million Bond
  May 11, 2011 by Paul Freehling
- Georgia Governor Signs New Restrictive Covenant Act
  May 11, 2011 by Seyfarth Shaw LLP
- "Under Pressure" Not Enough To Make Agreement Unenforceable
  May 6, 2011 by Eddy Salcedo
- Indiana Court Upholds A Covenant Not To Solicit Recent Customers, But Prohibitions Against Contact or Accepting Referrals With Such Customers Are Stricken
  May 4, 2011 by Paul Freehling
- Georgia House of Representatives Passes "Fix" to Restrictive Covenant Act
  February 25, 2011 by Michael Elkon
- Injunctive Relief and a Substantial Monetary Judgment Awarded to National CPA Firm Against Former Employees Who Breached Non-Compete Agreements
  February 14, 2011 by Paul Freehling
- Massachusetts Legislature Considers Revised Non-Compete Bill
  February 4, 2011 by Erik Weibust
- Illinois House of Representatives Revisits Non-Compete Statute
  February 6, 2011 by Scott Humphrey
- Georgia Legislature to Consider Re-enacting Restrictive Covenant Act
  January 7, 2011 by Seyfarth Shaw LLP

Trading Secrets

2011 Year-End Blog Review

Trade Secrets

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

January 17, 2012 by Robert Milligan and Joshua Salinas

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) 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 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 are 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 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.

Does A Trade Secret Plaintiff Have To Disclose Its Trade Secrets Prior To The Commencement Of Discovery In California Federal Court?

January 13, 2012 by Joshua Salinas

As a follow-up to yesterday's blog entry about a new California trade secret designation decision, another important issue that trade secret litigators face is whether the pre-discovery trade secret identification requirements of California Code of Civil Procedure section 2019.210 apply in California federal court. There is a split in authorities but recent cases suggest that California federal courts will require at a minimum an identification of trade secrets by the plaintiff as part of a trade secret plaintiff's Rule 26 disclosure or during the infancy of discovery.

In *Jardin v. DATAllegro*, No. 10-CV-2552-IEG (WVG), 2011 WL 3299395 (S.D. Cal. July 29, 1011), the Honorable Magistrate Judge William Gallo "wholeheartedly" agreed that section 2019.210 did not apply in federal district court. Yet despite refusing to directly apply the statute, Judge Gallo's pre-discovery trade secret identification order mirrored the procedures and policies provided in section 2019.2010. *Jardin* epitomizes the growing trend in which federal district courts will require parties to identify trade secrets with particularity before commencing discovery, without explicitly applying section 2019.210.

Section 2019.210 requires a plaintiff to identify allegedly misappropriated trade secrets before commencing discovery. The requisite pre-discovery identification helps serve four purposes: (1) promotes well-investigated claims, (2) avoid abuses of the discovery process, (3) frames the appropriate scope of discovery, and (4) enables the formation of complete and well-reasoned defenses. *Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F. Supp. 2d 980, 985 (S.D. Cal. 1999).

Jardin involved a dispute over the inventorship of U.S. Patent Number 7,818,349 ("Ultra-shared-nothing parallel database"). Plaintiff Jardin had previously filed a related suit two years earlier against Defendant DATAllegro regarding the infringement of a different patent. Consequently, discovery in the prior case allegedly provided Jardin with access to DATAllegro's confidential information. Additionally, a protective order entered in the previous case limited the use of the produced protected information. DATAllegro brought this issue to Judge Gallo, concerned that Jardin would improperly use confidential information from the prior case.

Judge Gallo found DATAllegro's confidentiality concerns legitimate. Despite his explicit rejection of section 2019.210, Judge Gallo ordered that no discovery would take place until Jardin identified the allegedly misappropriated information. In fact, Judge Gallo's orders and underlying policy considerations mirrored section 2019.210.

Jardin objected to Judge Gallo's order.

The Honorable Chief Judge Irma Gonzales upheld Judge Gallo's order, finding nothing erroneous in his refusal to apply section 2019.210. Judge Gonzales noted that the Ninth Circuit has not decided whether section 2019.210 applies in federal court and California district courts continue to reach conflicting conclusions. However, she stated that Federal Rule of Civil Procedure 26 provides district courts with broad discretion to control discovery. Thus, Judge Gallo could properly fashion his order after section 2019.210 without necessarily applying section 2019.210.

This case is significant because it illustrates the court's movement toward applying the procedures and policies behind section 2019.210 while retaining their "inherent discretion to manage discovery."

The Southern District court in *Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F. Supp. 2d 980 (1999) was one of the first federal courts to directly apply section 2019. That court recognized that the statute codified the holding in *Diodes, Inc v. Franzen*, 260 Cal. App. 2d 244 (1968), that pre-discovery trade secret identification is necessary to provide reasonable notice of the issues at trial and reasonable guidance in ascertaining the scope of appropriate discovery. The Northern District in *Neothermia Corp. v. Rubicor Medical, Inc.*, 345 F. Supp. 2d 1042 (N.D. Cal. Nov. 14, 2004) followed *Computer Economics* and directly applied section 2019.210.

The Eastern District in *Funcat Leisure Craft, Inc. v. Johnson Outdoors, Inc.*, No. S-06-0533 GEB (GGH), 2007 WL 273949 (E.D. Cal. Jan. 29, 2007) was the first federal court to reject the direct application of section 2019.210. That court found the statute to be a procedural rule that conflicted with the Federal Rules.

Since *Funcat* many district courts have continued to apply section 2019.210 either directly or indirectly. The Northern District applied the statute directly in *M.A. Mobile LTD. v. Indian Inst. of Tech. Kharagpur*, No. C08-02658 RMW (HRL), 2010 WL 3490209 (N.D. Cal. Sept. 3, 2010). The Eastern District in *Hilderman v. Enea Teksci, Inc.*, No. 05cv1049 BTM (AJB), 2010 WL 143440 (S.D. Cal. Jan. 8, 2010), rejected the direct application of section 2019.210, yet held that plaintiffs would be barred from presenting trade secret claims for failing to provide defendants with "fair notice." Moreover, the court in *Applied Materials, Inc. v. Advanced Micro-Fabrication Equipment (Shanghai) Co., Ltd.*, No. C 07-5248 JW PVT, 2008 WL 183520 (N.D. Cal. Jan. 18, 2008), declined to rule on section 2019.210 applicability, but required the plaintiffs to disclose the allegedly misappropriated trade secrets.

Jardin signifies this recent departure from *Funcat's* complete elimination of section 2019.210 from federal court. Indeed, federal courts should not ignore the purposes behind the statute as articulated in *Computer Economics*. It is interesting to note that *Jardin* is from the same Southern District of California as *Computer Economics*. While *Jardin* refused to directly apply section 2019.210, it indirectly applied the statute with the same reasoning set forth in *Computer Economics*.

The Ninth Circuit has yet to resolve the dispute. However, in *nSight, Inc. v. PeopleSoft, Inc.*, 296 F. App'x 555, 560 (9th Cir. 2008) (unpublished), it upheld the dismissal of a trade secret misappropriation claim because the plaintiff failed to identify any trade secret with "reasonable particularly" per section 2019.210. While unpublished, and thus nonbinding, *nSight* may foreshadow the Ninth Circuit's views regarding section 2019.210 applicability.

Moreover, the Eastern District in *N. Am. Lubricants v. Terry*, 2011 U.S. Dist. LEXIS 133672 (E.D. Cal., Nov 18, 2011) recently applied the rationale from *Computer Economics* regarding trade secret identification. *N. Am Lubricants* involved a motion to compel for the plaintiff's failure to identify trade secrets with sufficient particularity in response to an Interrogatory requesting said information. The court noted that although the dispute did not involve section 2019.210, the court found the rationale in *Computer Economics* persuasive regarding the need for reasonably specific identification of claimed trade secrets in response to interrogatories at the outset of litigation. It is notable that the decision was from the same magistrate who decided the *Funcat* case.

Trade secret defendants who find themselves in California federal court should request from plaintiffs the identification of any allegedly misappropriated trade secrets. While some federal courts may not directly apply section 2019.210, the growing trend is for those courts to fashion orders to ensure that the policies of both Rule 26 and section 2019.210 are achieved and that there is a trade secret identification disclosure either before the commencement of discovery or at the infancy of the discovery process. Thus, federal courts are more willing to either directly or indirectly use section 2019.210 because it is a helpful guideline to give defendants proper notice of the claims, enable complete defenses, guide proper discovery, and eliminate disadvantageous surprises at trial.

California Federal Court Holds That Trade Secret Misappropriation Defendant Need Not Respond To Plaintiff's Discovery Requests Until Provided With Identification Of Information Claimed To Have Been Stolen

January 12, 2012 by Paul Freehling

The trend of some recent judicial decisions seems to reflect an increasing concern by courts that, notwithstanding trade secret misappropriation plaintiffs' understandable reluctance to disclose proprietary information in more detail than absolutely necessary, they must describe with considerable specificity whatever is alleged to have been purloined. For example, a California district court ruled recently that "Whatever [the plaintiff] wishes to claim as trade secrets that [the defendant] misappropriated, it must identify each particular composition, formula, technology and manufacturing techniques, application and manufacture of [the applicable product] without further delay." *Delphon Industries, LLC v. International Test Solutions, Inc.*, Case No. C 11-01338 PSG (N.D. Cal., Jan. 4, 2012).

Plaintiff Delphon develops and manufactures gel products used in safely transporting delicate technology devices within and between laboratories. The gels are polymers created using proprietary formulas consisting of mixtures, blends and balances of specific chemical elements. In response to an interrogatory from Defendant ITS seeking identification of the trade secrets that allegedly were misappropriated, Delphon stated that it "customizes the composition of its gel materials to its customers' needs" and that the trade secrets are "The 'recipe' for its different gel materials - including the amount of each ingredient used, the process . . . [and] methods of combining the ingredients, the use of solvents with gel materials, and the blending, mixing and dispersion of additives into the gel material." ITS told Magistrate Judge Paul Grewal that Delphon had not identified its trade secrets with the specificity required by Section 2019.210 of the California Code of Civil Procedure, and he agreed.

Section 2019.210 provides that, before commencing discovery relating to a trade secret allegedly misappropriated, the alleging party must "identify the trade secret with reasonable particularity." According to Judge Grewal, the statute provides a "flexible standard" which does not require "every minute detail" of the claimed trade secrets but must be adequate "to permit the defendant to learn the limits of the secret and develop defenses [and] to permit the court to understand the secret and fashion discovery." He held that Delphon had fallen short. First, it had admitted that its depiction of the trade secret was imprecise; the court added that "In fact, the description is so general that Delphon did not even bother to protect the description under the terms of the Stipulated Protective Order." Second, Delphon's Director of Materials Technology conceded at her deposition that the

disclosures were “conceptual” and lacked specific details even though Delphon has this information. Third, the court explained that Delphon had offered “no credible expert testimony suggesting that those in the field would be able to review Delphon’s designations and distinguish the alleged trade secrets from information in the field.”

The lessons learned from this case are that a trade secret misappropriation plaintiff should 1) insist on the entry of a protective order; 2) should state that the description of the confidential information is covered by that order, and 3) should avoid referring to the disclosed information as “general” or simply “conceptual.” Finally, the plaintiff should consider seeking to retain a qualified expert witness to the extent necessary to testify that the unique characteristics of the trade secrets have been described sufficiently to differentiate the trade secrets from public information.

After Ohio Jury Finds Trade Secret Misappropriation But Awards Zero Damages, Trial Judge Enters Injunction Order But Sets Royalty Payment As Alternative

January 10, 2012 by Paul Freehling

A manufacturer engaged an independent contractor to improve the efficiency of certain machinery. After the task was completed, the contractor did the same for a competitor of the manufacturer. The manufacturer, claiming that the improvements were its trade secrets, sued the competitor in an Ohio state court for misappropriation. The case went to trial before a jury which returned a verdict of liability, answered special interrogatories consistent with that verdict, but awarded no damages. The trial judge entered judgment on the verdict and enjoined the competitor from using the trade secrets for five years unless the manufacturer was paid a specified royalty. On cross-appeals, the Ohio appellate court recently affirmed the judgment in all respects. *Columbus Steel Castings Co. v. King Tool Co.*, 2013 Ohio 6826 (10th Appellate Dist. Court of Appeals, Dec. 30, 2011).

Columbus manufactures steel bolsters that support and stabilize railroad cars. In 2003, Columbus retained King Tool to build a new, more efficient machine. As a result, Columbus' productivity increased three-fold. Then, Columbus' competitor Alliance Castings retained King for the same purpose and achieved production six times its former output. Columbus, claiming that the improvements to its machine made it "unique as a whole" and afforded a competitive advantage, sued King and Alliance for misappropriation of trade secrets. The defendants sought and obtained summary judgment, but Columbus appealed. In 2008, the Ohio Court of Appeals identified genuine issues of material fact and, therefore, reversed and remanded for a trial.

Columbus settled with King and tried, to a jury, the dispute with Alliance. The jury returned a general verdict in favor of Columbus on liability but awarded no monetary relief. In answers to special interrogatories, the jury found that (a) the "machine made by King Tool for Columbus Steel was not generally known to, or readily ascertainable by proper means by, someone who might obtain economic value from its use," (b) Columbus "made reasonable efforts to maintain the secrecy of the design of the" machine, (c) the design was a trade secret of Columbus, and (d) Alliance misappropriated Columbus' trade secret. The trial court enjoined Alliance's use of its new machine for five years but, as an alternative, established a royalty of $10.60 -- approximately 1% of the average sales price -- for Alliance to pay Columbus for each bolster manufactured on the machine during that period. Both parties appealed.

Columbus argued that the jury's zero damages verdict resulted from misleading jury instructions. The Court of Appeals determined, however, that the instructions "as a whole" did not mislead "the jury in a manner affecting [Columbus'] substantial rights."

Alliance maintained that the case should not have been submitted to the jury at all because there was no evidence to support Columbus's claims that (a) the machinery design qualified as a trade secret, (b) Columbus took "reasonable steps to protect the secrecy of the design," (c) Alliance misappropriated the design, and (d) "Alliance's alleged misappropriation caused Columbus damage." The appellate tribunal, reviewing de novo, rejected all of these contentions and affirmed the judgment in its entirety. The court held that it must affirm "if substantial evidence exists to support" the verdict and "reasonable minds could reach different conclusions on essential elements of the claim." As to Alliance's contentions:

1. Trade secret. The design qualified as a trade secret under the Ohio Uniform Trade Secrets Act, even though certain components "were readily ascertainable, because the machine as a whole was unique and afforded a competitive advantage to Columbus Steel."

2. Protection of confidentiality. There was some evidence that Columbus had told King that the design was to be kept confidential and not shared with Columbus' competitors. Further, Columbus "had security guards, fences, and locked entryways, and that the sketches and engineering drawings for the new machine were kept in a locked office." Alliance claimed that the improvements were readily ascertainable by viewing the machine, but the appellate court pointed to evidence that Alliance's representatives "obtained unauthorized access by means of false representation in order to view the new machine."

3. Misappropriation. Alliance may have used improper means to acquire knowledge of the trade secrets. There was some evidence that an Alliance misrepresented to King that he was working for both Alliance and Columbus. The Court of Appeals said it was the province of the jury to determine whether there was a misrepresentation and whether Alliance had reason to know of it.

4. Damage. There was evidence from which a jury could have found that Columbus lost an indeterminate amount of profits due to misappropriation. In trade secret cases, "it is often difficult to prove money damages or lost profits" with certainty. The injunction provided "some relief for the misappropriation [because] the facts and circumstances of this case, particularly the zero damages verdict, lend themselves to a presumption of [irreparable] harm and a finding that money damages could not adequately compensate Columbus Steel."

This decision provides insights with respect to proper jury instructions and special interrogatories in trade secret misappropriation cases. It shows that appellate courts will strive to reconcile all aspects of a jury's verdict and a trial court's judgment.

US Companies Have Options Against Chinese Companies For Trade Secret Misappropriation

January 9, 2012 by Eddy Salcedo

Expanding what until recently had been very limited options for U.S. companies to enforce their rights against Chinese companies misappropriating trade secrets, the Federal Circuit in *TianRui Group Co. v. International Trade Commission*, Fed. Cir., Case No. 2010-1395, held that the International Trade Commission has statutory authority to review and rule on conduct occurring in China in the course of a trade secret misappropriation investigation. The primary effect of this decision is that US companies are now afforded the ability to sue Chinese parties in the United States, an avenue previously foreclosed such companies because, generally, in such cases a substantial amount of the wrongful activity would have taken place in China, and the Chinese parties are thus beyond the reach of most long arm statutes. In sum, the decision allows US companies through the International Trade Commission to block the importation of products produced by a foreign company using trade secrets stolen from a U.S. competitor.

The relevant factual particulars of *TianRui* are as follows. Amsted Industries, an American manufacturer of cast steel railway wheels, granted a license to Datong, a Chinese manufacturer of the same product, for a proprietary foundry process for the manufacture of these wheels. There was no question that the process was a trade secret belonging to Amsted. TianRui, another Chinese manufacturer, approached Amsted in 2005 and attempted to negotiate a similar license as Datong for the process. However, an agreement was never reached with Amsted. After the failure of the negotiations, TianRui hired away nine Datong employees trained in Amsted's manufacturing process. Notably, all of these former Datong employees had actual knowledge that the manufacturing process was a confidential trade secret belonging to Amsted, and moreover eight of the nine had signed confidentiality agreements with Datong covering, amongst other trade secrets, the Amsted process. In addition to having their trade secrets misappropriated, Amsted was further injured because TianRui ultimately sold the wheels it manufactured with the process in the U.S. through a joint venture.

Amsted there after filed a complaint with the International Trade Commission, alleging that the importation of the wheels into the U.S. violated § 337 of the Tariff Act of 1930, 19 U.S.C. §1937, by reason of TianRui's use of the Amsted manufacturing process which was developed in the U.S. and therefore subject to protection by U.S. trade secret laws. TianRui interposed a defense that no action against it could lie because Congress did not intend for § 337 to apply to territories outside the U.S., including China. After hearing the matter, the International Trade Commission rejected TianRui's reading of Congressional intent on § 337, and issued a limited exclusion order relating to the wheels produced with the Amsted manufacturing process. TianRui sought review of the decision by the Federal Circuit after the International Trade Commission elected not to review the decision itself.

Ultimately, the Federal Circuit found that § 337 was properly applied by the International Trade Commission based upon TianRui's conduct within the U.S., specifically the importation of the wheels, by its joint venture, into the U.S. Significantly, the Federal Circuit further found that despite the fact that most of the offending conduct, the misappropriation of Amsted's trade secret and production of the wheels using these misappropriated secrets, took place in China, the International Trade Commission's exclusion order was nevertheless proper because the Commission was empowered under § 337 to set the circumstances pursuant to which products may or may not be imported into the U.S., including the exclusion of products found to be manufactured by means of misappropriated U.S. trade secrets.

In sum, an ITC proceeding can be a powerful tool to protect trade secrets that are misappropriated by the foreign competitors of U.S. companies.

At Long Last, New Jersey Passes Trade Secrets Act

January 9, 2012 by David Monachino

Legislation intended to help protect the trade secrets of New Jersey businesses has been signed into law by Gov. Christie. The New Jersey Trade Secrets Act (S-2456/A-921) establishes by law specific remedies available to businesses in the event that a trade secret – such as a formula, design, a prototype or invention – is misappropriated. New Jersey was one of the four remaining states that have not adopted some or all of the provisions of the Uniform Trade Secrets Act (Massachusetts, New York and Texas are the others), but instead NJ courts have relied wide range of common law decisions in order to establish a trade secret misappropriation claim.

The New Jersey Senate approved the bill 39-0; the Assembly approved the measure 79-0. The law takes effect immediately, except it does not apply to misappropriation that occurred prior to the effective date or to a continuing misappropriation that began prior to the effective date of the law and continued after the effective date of the law.

The new law provides for damages for both actual loss suffered by a plaintiff and for any unjust enrichment of the defendant caused by the misappropriation of trade secrets. Damages also may include a reasonable royalty for unauthorized disclosure or use of the trade secrets. In cases of willful misappropriation, punitive damages and attorneys' fees may be awarded. In addition, if a claim for misappropriation is brought in bad faith, attorneys' fees may be awarded.

The New Jersey Act also has a couple of unique and helpful provisions, including a requirement that a court "preserve the secrecy of an alleged trade secret by reasonable means consistent with" court rules. There is also "a presumption in favor of granting protective orders in connection with discovery proceedings" as well as provisions limiting access to confidential information to only the attorneys for the parties and their experts, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

It remains to be seen if New York will now follow New Jersey's lead and adopt similar legislation.

What Does It Take to Plead a Claim for Trade Secret Misappropriation Claim Under the Uniform Trade Secrets Act?

December 23, 2011 by David Monachino

In *Eastman Chemical Company, v. Alphapet Inc., et al.*, Civ. Action No. 09-971-LPS-CJB 2011 U.S. Dist. LEXIS 127757 (Dist. DE) (November 4, 2011) (unpublished) Plaintiff Eastman Chemical Company ("Eastman" or "Plaintiff') filed an amended complaint alleging patent infringement, breach of contract and trade secret misappropriation. Plaintiff alleged that former Eastman employees at the direction of one or more of the Defendants, improperly disclosed Eastman's confidential, proprietary, and trade secret information relating to the manufacture of certain products in violation of a technology license agreement. Defendants moved to dismiss the trade secret misappropriation claim based on a failure to specifically plead this claim.

Defendants argued that Plaintiff's claim for trade secret misappropriation failed to satisfy the pleading standard of Fed. R. Civ. P. 8 in three principal respects. First, Defendants asserted that the amended complaint failed to identify which of the Defendants allegedly obtained Eastman's trade secrets, and which individuals were involved in the allegedly illicit disclosure and use of that information. Second, Defendants argued that the description of the trade secrets that were allegedly used or disclosed is "so broad as to be meaningless." Finally, Defendants contended that "Eastman failed to adequately plead that any [particular] defendant actually used or disclosed" any trade secrets.

For purposes of its analysis, the Magistrate Judge considered case law from other states that have adopted the Uniform Trade Secrets Act to be persuasive authority. Viewing Plaintiff's misappropriation claim and the associated facts in the light most favorable to Plaintiff, the Magistrate Judge found that Defendants had not shown that this misappropriation claim should be dismissed pursuant to Rule 8. Having outlined and considered the contours of Plaintiff's factual allegations, the Magistrate Judge found that Defendants have been given sufficient factual information to provide adequate notice of the plausible grounds for Plaintiff's misappropriation claim under the Twombly/Iqbal standard.

2011 Trade Secrets Webinar Series - Year in Review

December 20, 2011 by Robert Milligan

Throughout 2011, Seyfarth Shaw LLP'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: *Trade Secrets in the Financial Services Industry*, *The Anatomy of a Trade Secret Audit*, *Georgia's New Non-Compete Statute*, *Managing and Protecting Trade Secrets in the Brave New World of Cloud Computing and Social Media*, *Choosing the Right IP Protection: Patent, Trade Secret or Both?*, *and Key Considerations Concerning Trade Secrets and Non-Competes in Business Transactions*. As a conclusion to this well-received 2011 webinar series, we have compiled a list of key takeaway points for each of the webinars, which are listed below. For those clients who missed any of the programs in this year's webinar series, the webinars are available on compact disc upon request and CLE credit is available as discussed below. We are also pleased to announce that Seyfarth Shaw LLP will continue its trade secrets webinar programming in 2012 and has several exciting topics lined up.

Trade Secrets in the Financial Services Industry

The first webinar of the year, *Trade Secrets in the Financial Services Industry*, was led by Seyfarth attorneys Scott Humphrey and Scott Schaefers. The financial services industry has unique concerns with respect to trade secret protection. This webinar had a particular focus on a financial institution's relationship with its FINRA members and also covered practical steps that can be implemented to protect trade secrets and what to do if trade secrets are disclosed.

- Enforcement of restrictive covenants and confidentiality obligations for FINRA and non-FINRA members are different. Although FINRA allows a former employer to initially file an injunction action before both the Court and FINRA, FINRA, not the Court, will ultimately decide whether to enter a permanent injunction and/or whether the former employer is entitled to damages as a result of the former employee's illegal conduct.

- Address restrictive covenant enforcement and trade secret protection before a crisis situation arises. An early understanding of the viability of your restrictive covenants and the steps that you have taken to ensure that your confidential information remains confidential will allow you to successfully and swiftly evaluate your legal options when an emergency arises.

- Understand the Protocol for Broker Recruiting's impact on your restrictive covenant and confidentially requirements. The Protocol significantly limits the use of restrictive covenants and allows departing brokers to take client and account information with them to their new firm.

The Anatomy of a Trade Secret Audit

The second webinar was led by Robert Milligan, Bob Niemann and David Monachino. This webinar dissected what is involved in an audit of your company's trade secret protections, including, identifying trade secrets and secrecy protections and implementing effective secrecy protections and hiring and termination protocols. The webinar also discussed employing a comprehensive trade secret protection plan, as well as managing and working to protect computer-stored data, including responding to emergency issues related to computer fraud and security breaches.

- The issues relating to all the aspects of trade secrets can be overwhelming to those that deal with it on rare occasions or in emergencies. Having effective checklists are helpful to marshal evidence, evaluate your claims, and be pro-active to pursue litigation and defend against claims. Ask your Seyfarth Shaw attorney for sample checklists.

- Use a forensic computer investigator to assess former employees' computer activities, including use of email and USB devices to unlawfully transmit company data. Ensure that you have strong computer usage restrictions that prohibit unauthorized and unpermitted computer activities on your computer network.

- Mark your confidential documents confidential and treat them as such, including having company policies requiring that they not be removed from the workplace and that they be returned at time of termination. Also establish clear employee entrance and exit policies to ensure that trade secret information is adequately protected throughout the hiring and termination process.

Georgia's New Non-Compete Statute

The third webinar of the year, led by Bob Stevens and Erika Birg with guest panelist Kevin Levitas, former member of the Georgia House of Representatives, focused on Georgia's Revised Restrictive Covenant Act. The webinar addressed the fundamental paradigm shift toward enforcing restrictive covenant agreements in Georgia and addressed the underlying legislation, legislative history that led to the 180 degree change for enforcement of such agreements in Georgia and detailed the significant changes to the law.

- There has been a fundamental change in Georgia public policy toward enforcement of restrictive covenant agreements, including non-competes and non-solicits.

- The Georgia Revised Restrictive Covenant Act addressing restrictive covenants permits courts for the first time to blue pencil or modify agreements entered into after May 10, 2011 to make overbroad agreements enforceable. The old Georgia law still applies to agreements entered into prior to January 1, 2011. Due to arguments over the constitutionality over Georgia's Restrictive

Covenant Act passed in late 2010, the law regarding agreements entered into between January 1, 2011 and May 10, 2011 is still uncertain.

- Employers operating in Georgia should have their non-compete agreements evaluated by competent counsel to ensure that they comply with the new Act and provide employers with the greatest protections under Georgia law.

Managing and Protecting Trade Secrets in the Brave New World of Cloud Computing and Social Media

2011's fourth trade secrets webinar focused on cloud computing and social media and their impact on trade secret status and protection efforts. Robert Milligan, Jason Stiehl and Jason Priebe led this highly attended webinar. This webinar discussed a technological overview of cloud computing and social media, "both sides of the coin" look at cloud computing adoption as a business decision, trade secrets and reasonable secrecy measures, key considerations in selecting a cloud provider from a security and trade secrets perspective, effective vendor and employment agreements and policies to protect trade secrets in the cloud, and effective social media policies to protect trade secrets.

- When utilizing cloud computing, generally follow a three-step process: (1) ensure you understand and define your trade secrets internally through a trade secret audit before consider placing such information in the cloud; (2) create necessary barrier/security protocol to protect those secrets; and (3) develop comprehensive and cohesive social media and restrictive covenants/confidentiality policies to avoid disclosure.

- Identifying and collecting information to fulfill an organization's duty to preserve and/or discovery obligations can be tricky in cloud environments. While the information may belong to your company or organization, the underlying software structure belongs to a service provider, and the data may be scattered over multiple locations. It is a good idea to consider potential issues of data control, ownership, and jurisdiction when evaluating a software as a service (SAAS) cloud-based platform solution.

- Carefully review the proposed service agreement with the cloud provider and ensure that provider agrees to keep data confidential and has reasonable security measures in place to protect your information; also consider avoiding contractual limitations on provider liability depending upon bargaining power. If the secrets involved are "bet the company" type information, the cloud may not be the place to store it.

Trading Secrets

Choosing the Right IP Protection: Patent, Trade Secret or Both?

The fifth webinar, led by Brian Michaelis, Dan Schwartz and Jim McNairy, focused on choosing the best legal tool to protect particular types of intellectual property. The topics discussed in this webinar included a definition of a patent and what information is patentable, defining a trade secret and what information qualifies for trade secret protection, the pros and cons of patent vs. trade secret protection, which types of information/technology may be best protected through both trade secret and patent protection, the impact the new America Invent Act (Patent Reform Legislation) has on the decision to seek patent or trade secret protection.

- There may be "tension" between patent protection and trade secrets; for instance, patents require public disclosure in return for a government granted monopoly whereas trade secret require that the information remain secret throughout its life. Once information is no longer secret or otherwise becomes available, trade secret protection will be lost.

- The remedies available under patent laws and trade secret law differ significantly. A patent owner is always entitled to at least a "reasonable royalty" for any infringement. There is no statutory floor of damages such as a "reasonable royalty" for trade secret owners.

- Recent changes to the patent laws provide trade secret owners with additional defenses to allegations of patent infringement where the trade secret owner has maintained as a trade secret a later patented method or system.

Key Considerations Concerning Trade Secrets and Non-Competes in Business Transactions

The final webinar of 2011 was led by Todd Hunt, Erik Weibust and Jim McNairy. This webinar included a discussion of which relationships other than employer/employee relationships require trade secret protections, the most significant risks to the trade secret status of your valuable confidential information under the Uniform Trade Secrets Act and best practices for protecting trade secrets in business transactions.

- Broader non-competes are better tolerated in the sale of a business context, but care should be taken to carefully assess your specific facts and applicable law to help ensure that time, place, and subject matter restrictions, if any, are consistent with law in the jurisdiction(s) at issue. Pay special consideration to choice of law and choice of forum issues as they impact enforceability.

- Adequately protecting trade secrets and goodwill in business presentations and transactions requires careful planning and forethought. The often large and frequent exchange of information in

these contexts requires use of Non-Disclosure/Confidentiality Agreements.

- All business relationships are potential threats to trade secret status and opportunities for misappropriation. Given this, it is imperative to identify any trade secrets at issue and proactively assess any aspects of the business relationship or transaction that may present risks of unintended or unauthorized disclosure or use of trade secrets, as well opportunities for bad actors to improperly acquire your trade secret information.

2012 Trade Secrets Webinar Series

Beginning in January 2012, we will begin another series of Trade Secret webinars. The first webinar of 2012, *Latest Developments in the Computer Fraud and Abuse Act, Social Media and Privacy*, will be held on January 26. 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.*

For client attorneys licensed in Illinois, New York or California, who are interested in receiving CLE credit for viewing recorded versions of the 2011 webinars, please e-mail *CLE@seyfarth.com* to request a username and password.

If you have any questions, please contact the Seyfarth Shaw attorney with whom you work or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (www.seyfarth.com/tradesecrets).

Use Of Even A Small Amount Of Commercially Valuable Confidential Information Obtained From Someone Without Authority To Convey It Constitutes Actionable Trade Secret Misappropriation According To Eighth Circuit

December 19, 2011 by Paul Freehling

A recent Eighth Circuit Court of Appeals decision, extremely favorable to a plaintiff alleging trade secret misappropriation, holds that protection may be accorded to a compilation of information if reasonable efforts were made to keep the compilation secret, where the compilation adds value to the information, regardless of the amount of the information that already was in the public domain. The defendant, who used the compilation after obtaining it from a third party who was not authorized to provide it, was hammered by the court.

Rolls-Royce developed procedures, approved by the FAA, for repairing and overhauling helicopter engines. The procedures were compiled and disclosed in documents provided to its Authorized Maintenance Centers (AMCs) with, in at least some instances, a proprietary rights legend on the front page. AvidAir, which was not an AMC, acquired the information partly from public sources and partly by a purchase from an AMC that did not have permission to sell it. When AvidAir began using the procedures, Rolls-Royce demanded that AvidAir deliver the compilation documents to Rolls-Royce and cease using them. AvidAir proceeded to file suit in a Missouri federal court seeking a declaratory judgment that the information was not a trade secret and accusing Rolls-Royce of antitrust violations and tortious interference. Rolls-Royce countered with a misappropriation lawsuit in an Indiana federal court. Both Indiana and Missouri have adopted the Uniform Trade Secrets Law. The two cases were consolidated in the Missouri court.

On cross-motions for summary judgment, the trial court ruled in favor of Rolls-Royce and dismissed AvidAir's claims. A jury then awarded Rolls-Royce $350,000 in damages. The trial court entered judgment on the jury verdict and awarded permanent injunctive relief to Rolls-Royce. The Eighth Circuit affirmed in all respects. *AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, No. 10-3444 (8th Cir., Dec. 13, 2011).

AvidAir asserted that the non-public information in the compilations was too trivial to be accorded protection. The appellate court rejected that assertion, stating that a compilation has value if it gives the compiler "a competitive advantage," even if the compiled information itself is generally available. Contrasting a trade secret with a patented invention, the court said that engineering advances are not a prerequisite to trade secret protection: "Unlike patent law, which predicates

protection on novelty and nonobviousness, trade secret laws are meant to govern commercial ethics." Rolls-Royce's compilation was a trade secret because (a) it consisted of information with value "independent of older publicly available versions," and (b) Rolls-Royce made "reasonable efforts to keep it secret." The court stressed that Rolls-Royce showed that the compilation required "a substantial investment of time, effort, and energy," and so the fact that others *could* have duplicated it by legitimate means is not a defense to a misappropriation claim. Indeed, "AvidAir's repeated [unsuccessful] attempts to secure the [compilation] without Rolls-Royce's approval belies its claim that the information in the documents was readily ascertainable or not independently valuable."

AvidAir maintained that Rolls-Royce did not try very hard to protect the confidentiality of the compilation. The court responded: "Reasonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required." Rolls-Royce's use of a proprietary legend is evidence of Rolls-Royce's attempt, and its "[m]isplaced trust in a third party who breaches a duty of confidentiality does not necessarily negate efforts to maintain secrecy."

The lesson of this ground-breaking decision is that one who makes commercial use of even a minimal amount of confidential information, after obtaining it from a source without authority to provide it, runs a risk of incurring the wrath of a court adjudicating a trade secret misappropriation lawsuit (at least in the Eighth Circuit).

Colorado Magistrate Judge Outlines Stringent Pleading Requirements Which Must Be Satisfied Before Plaintiffs Alleging Trade Secret Misappropriation Can Compel Responses To Discovery Requests; Judge Also Encourages Filing Pleadings Under Seal

December 8, 2011 by Paul Freehling

A recent opinion issued by a U.S. Magistrate Judge for the District of Colorado with respect to a discovery dispute in a trade secret misappropriation case may please defense counsel, but create headaches for plaintiffs' lawyers, because the Court set harsh pleadings standards that plaintiffs must meet. The Court seems to have been more sympathetic (a) to the defendants' and the court's desire to have identification "with reasonable particularity" of the supposedly misappropriated trade secrets, than to (b) the justifiable reluctance of plaintiffs to disclose detailed confidential information. If the Court's reasoning becomes generally accepted, plaintiffs may decide that some trade secret misappropriation claims are better left unfiled rather than making disclosures with the requisite specificity.

The Court recognized that "the case law does not provide clear guidance" as to the pleading requirements. However, basing her ruling primarily on unreported (plus a few reported) decisions, she 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." *L-3 Communications Corp. v. Jaxon Eng'r'g Maintenance, Inc.*, Civ. Ac. No. 10-cv-02868-MSK-KMT (D.Colo., Oct. 12, 2011) (emphasis added).

According to the Court, allegations that defendants misappropriated broad categories, such as "customer lists, pricing templates and labor rates, vendor lists, drawings, designs and processes," are inadequate. Plaintiffs must identify the actual "parts and vendors, the actual methods by which they use their equipment, or the actual software they use to process the generated raw data." The Court faulted the plaintiffs in the case before her both for inadequate pleading and for not filing, or at least seeking to file, the requisite disclosures of their trade secrets under seal. Accordingly, the Court determined that the plaintiffs were not entitled to compel discovery responses.

Massachusetts Judge Finds Statutory Trade Secrets Misappropriation, Despite Contrary Jury Verdict in Parallel Common Law Action, and Awards Plaintiff Draconian Injunctive Relief and Millions of Dollars in Damages, Fees and Costs

November 30, 2011 by Paul Freehling

When the evidence of trade secret misappropriation and resulting substantial damages is compelling, defendants should expect to get hammered in court. A recent Massachusetts case is in point. There, despite a jury verdict for the defendants, the trial court entered judgment for the plaintiff which included a permanent injunction prohibiting the defendants from using the plaintiff's manufacturing process trade secret and an order directing the defendants to dismantle the production line where the trade secret had been used. Defendants were forbidden from manufacturing a competing product *for five years by any means* and were assessed $8 million in damages, fees and costs.

STR's common law and statutory trade secret misappropriation claims were tried in the Superior Court simultaneously, the former to a jury and the latter to a judge. At trial, STR described its five-year effort to develop "an innovative method to produce a specialized encapsulant used in making solar cells." STR showed how its 25% share of worldwide sales of that product declined when JPS begin making and selling a competing product, using the identical process, within one year after a key STR employee defected to JPS. An expert witness calculated JPS' profits resulting from the wrongdoing.

Answering a special interrogatory, the jury found that STR's trade secret had not been misappropriated. The trial judge disagreed. In addition to granting equitable relief, she awarded STR more than $1 million in damages (which she trebled pursuant to the applicable state statute), $3.9 million in attorney's fees, and costs in excess of $1.1 million. The Appeals Court of Massachusetts affirmed and indicated that STR also would be entitled to reimbursement of its fees and costs incurred on appeal. *Specialized Technology Resources, Inc. v. JPS Elastomerics Corp.*, No. 11-P-776 (Mass. App. Court, Nov. 23, 2011).

Several Massachusetts cases hold that (a) there is no right to a jury trial on statutory claims of the type involved here, and (b) the jury's verdict with respect to common law causes of action parallel to the statutory claims is not binding on the judge in deciding whether the statute has been violated. So, the Superior Court judge was permitted to disregard the jury verdict. The defendants maintained, however, that no Supreme Judicial Court decision authorizes a trial judge, in a case where the statutory and common law actions are tried together, to decide questions of fact contrary to the findings of the jury as reported in special interrogatory answers. Nevertheless, one prior appellate court ruling upheld a trial

judge's finding, in a breach of warranty lawsuit, that the defendants were not liable notwithstanding the jury's directly contrary answers to special verdict questions. Relying on that precedent, the decision below in favor of STR was affirmed. The entirety of the trial judge's award of injunctive and monetary relief was determined to be within her discretion.

Social Media and Trade Secrets Collide: Whose Twitter Is It, Anyway?

November 18, 2011 by Gary Glaser

The United States District Court for the Northern District of California recently ruled that PhoneDog, an "interactive mobile news and reviews web resource," could proceed with its lawsuit against Noah Kravitz, a former employee, who it claims unlawfully continued using PhoneDog's Twitter account after he quit. *PhoneDog v. Noah Kravitz*, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D.Cal.)(James)(November 8, 2011)(unpublished).

PhoneDog asserted 4 causes of action, two of which arose from its contention that Kravitz unlawfully misappropriated and/or converted PhoneDog's trade secrets: namely, the compilation of subscribers to its Twitter account and the password used to access the account. And it was these claims anchored in PhoneDog's trade secret claims that survived Kravitz's motion to dismiss.

PhoneDog reviews mobile products and services and provides users with the resources that they can use to research, compare prices, and shop from mobile carriers. Kravitz worked for PhoneDog as a product reviewer and video blogger. He was given access to PhoneDog's Twitter Account "@PhoneDog_Noah", using a password and used the Account to send out information and promote PhoneDog's services on its behalf. The centerpiece of PhoneDog's trade secret claims are that all PhoneDog_Name_Twitter Accounts and the passwords to such accounts used by PhoneDog's employees -- like the one to which Kravitz was given access to and use of – constitute proprietary, confidential information. PhoneDog contends that the Twitter Account to which Kravitz was allowed to use on its behalf generated about 17,000 Twitter followers during Kravitz's employment.

Kravitz countered by arguing that the Twitter Account cannot be a trade secret because the names of the Twitter Account followers are, and have always been "publically available for all to see at all times." The passwords, he argues, are not trade secrets because they don't derive any independent economic value as required under the Uniform Trade Secrets Act ("UTSA"), since they don't provide any "substantial business advantage." Instead, all they do, Kravitz contends, is permit the individual logging in to view information that is already publicly known. He argued that the password is also not protectable as a trade secret because he, and not PhoneDog, initially created the password, and that PhoneDog did not take reasonable efforts to maintain its secrecy.

In addition, Kravitz contended that PhoneDog failed to allege that he engaged in any act that constitutes "misappropriation," as it is defined under the UTSA. Instead, he argued, PhoneDog merely alleged, in conclusory terms, that he used "improper means" to obtain the Twitter password and to continue to use the Twitter Account, which belonged to it, rather than him.

The Court denied Kravitz's motion to dismiss both the misappropriation of trade secrets and the conversion claims. As to the misappropriation claim, the Court held that PhoneDog had described the subject matter of the trade secret with "sufficient particularity" and satisfied its pleading burden as to Kravitz's alleged misappropriation by alleging that it had demanded that Kravitz relinquish use of the password and Twitter Account, but that he has refused to do so. And, with respect to Kravitz's challenge to PhoneDog's assertion that the password and the Account followers do, *in fact,* constitute trade secrets -- and whether Kravitz's conduct constitutes misappropriation, the Court ruled that the such determinations require the consideration of evidence outside the scope of the pleading and should, therefore, be raised at summary judgment, rather than on a motion to dismiss.

The Court followed a similar approach in denying Kravitz's motion to dismiss PhoneDog's conversion claim. Kravitz challenged such claim on the ground that PhoneDog had not sufficiently alleged that it owns or has the right to immediately possess the Twitter Account. He also argued that PhoneDog failed to adequately allege that he had engaged in his alleged act of conversion "knowingly" or "intentionally." The Court, however, found that these issues lie "at the core of [the] lawsuit" and that, accordingly, an evidentiary record outside the pleading had to be developed before the Court could resolve such fact-specific issues.

The last two of the claims were dismissed by the Court, both of which alleged interference with prospective economic advantage — one intentional, and the other negligent. The basis for the dismissal of these claims was that California law does not protect "mere 'potential' relationships that are 'at most a hope for an economic relationship and a desire for a future benefit'." Here, the Court found that it was unclear who the "users" of PhoneDog's mobile news and review services *are — in other words, whether they are the 17,000 Account followers, consumers accessing PhoneDog's website, or some other individuals, and what the nature of PhoneDog's purported economic relationship is with these users.* The Court also agreed with Kravitz that PhoneDog had failed to adequately allege any actual disruption of the relationship between it and its users or actual economic harm. With respect to the *negligent* interference with prospective economic advantage claim, the Court also agreed with Kravitz that PhoneDog had failed to allege that Kravitz owed it a duty of care.

The writer eagerly awaits the decision of this Court once a complete evidentiary record has been developed. However it ultimately rules, though, one can rest assured that this is but one more chapter in what we can anticipate will be a long line of cases addressing the issues of whether social media passwords and social media analogs to the classic customer list are "trade secrets," and who, *if anyone*, truly "owns" them? And, more broadly, whether any information available on the web can be considered a "trade secret."

At Long Last, New Jersey Is Poised To Pass The “New Jersey Trade Secrets Act”

November 16, 2011 by David Monachino

New Jersey is one of the four remaining states that have not adopted some or all of the provisions of the Uniform Trade Secrets Act (Massachusetts, New York and Texas are the others), but instead NJ courts have relied wide range of common law decisions in order to establish a trade secret misappropriation claim. On September 26, 2011, the New Jersey Senate approved a bill known as the "New Jersey Trade Secrets Act" (A - 921), which provides statutory remedies and procedural guidance for the misappropriation of trade secrets. This proposed bill provides for damages for both actual loss suffered by a plaintiff and for any unjust enrichment of the defendant caused by the misappropriation of trade secrets. Damages also may include a reasonable royalty for unauthorized disclosure or use of the trade secrets. In cases of willful misappropriation, punitive damages and attorneys’ fees may be awarded. In addition, if a claim for misappropriation is brought in bad faith, attorneys’ fees may be awarded.

The New Jersey Act also has a couple of unique and helpful provisions, including a requirement that a court "preserve the secrecy of an alleged trade secret by reasonable means consistent with" court rules. There is also "a presumption in favor of granting protective orders in connection with discovery proceedings" as well as "provisions limiting access to confidential information to only the attorneys for the parties and their experts, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval."

The NJ Assembly has to vote on the Senate’s amended version of the bill before it is presented to Governor Chris Christie for his signature. The bill is expected to be voted upon after the November recess and Governor Christie then has 45 days to sign the bill into law. If the bill is singed, it will become effective immediately, but will not be retroactive. Assuming the law eventually passes, it is still important for companies doing business in NJ to define what may constitute proprietary information, especially if that definition is broader than the "trade secret" definition found in the statute. Either way — whether the bill passes or not — it remains important for a business to continue to take reasonable efforts to maintain the secrecy of any information that it deems confidential or risk losing trade secret protection.

Failure to Specifically Identify Trade Secrets in a Complaint Does Not Bar a Complaint in New Jersey Federal Court

October 27, 2011 by David Monachino

A growing number of courts across the country have required plaintiffs to specify with particularity the trade secret that they are accusing a defendant of stealing, and that plaintiffs' refusal to do so could result in dismissal of the claim. See, e.g., *Dura Global, Tech, Inc. v. Magna Donnelly Corp.*, 2008 WL 2064516 (E.D.Mich. May 14, 2008) (staying discovery until the plaintiffs provided the defendants with a list identifying the trade secrets alleged to have been misappropriated "with reasonable particularity"). Similarly, California has enacted a statutory requirement that requires a plaintiff in a trade secrets case "to identify the trade secret with reasonable particularity . . . before commencing discovery relating to the trade secret." Cal.Code of Civil Proc. Section 2019.210.

A federal district court in New Jersey has failed to follow that trend. In *Reckitt Benckiser Inc. v. Tris Pharma, Inc.***,** 2011 U.S. Dist. LEXIS 19713 (D.N.J. June 21, 2011**)** (unpublished), the underlying action arose out of, *inter alia*, the alleged infringement of several drug patents. Defendants moved to dismiss several of the non-patent counts, including a trade secret misappropriation claim. Defendants argued that plaintiffs' claim for misappropriation of trade secrets must be dismissed as a matter of law, because defendants contended that plaintiffs should have identified the alleged trade secrets in its complaint with particularity since they were "uniquely known to plaintiffs."

The district court disagreed and denied the motion to dismiss holding that under New Jersey law, a claim of misappropriation of trade secret "does not require specific pleading of the precise information that constitutes the trade secret in order to survive a motion to dismiss. Indeed, 'unless there are heightened pleading requirements as to a particular cause of action, the Federal Rules of Civil Procedure do not require a plaintiff to plead all the relevant facts in detail . . . and generally do not require a plaintiff to provide specific information about trade secrets at this stage of the litigation.'"

Plaintiff Receives Million Plus Attorneys' Fees Award In Trade Secret Dispute Despite Small Damages Award

October 24, 2011 by Paul Freehling

A recent trade secret misappropriation action resulted in an award of compensatory damages of $41,000 and punitive damages of $40,000. Then, the plaintiff asked for more than a million dollars in attorney's fees and costs. The defendants protested that (a) the fee request was grossly disproportionate to the damages that were recovered, and (b) the plaintiff's billing was excessive. However, except for reimbursement of the expense of one expert witness the court deemed unnecessary, the entire requested amount was awarded. *SKF USA, Inc. v. Bjerkness*, Civil Action Nos. 08C 4709 and 09 C 2232 (N.D. Ill., Sept. 27, 2011).

An employee of plaintiff SKF left in order to "set up a competing business, taking with him a handful of other SKF employees and thousands of SKF's computer files."

SKF sued and established misappropriation. The court granted injunctive relief plus what it described as "a modest damages award." SKF proceeded to file a fee request for $1.3 million. While not challenging SKF's attorneys' hourly rates, the defendants characterized as "outrageous" the more than 2700 hours billed. The defendants stressed that they had made substantial settlement offers, two of which were in amounts in excess of the damages ultimately recovered, and that SKF had rejected each while declining to make a counter-proposal.

SKF objected to the defendants' argument based on settlement offers, but case law supports the court's consideration of such information in adjudicating a fee request.

Case law also indicates that proportionality of the fee request is a relevant factor, but compared to what? Some courts weigh the ultimate result against the amount sought in the complaint and some look at the plaintiff's reasonable expectations. The Seventh Circuit has declined to adopt a specific rule.

SKF's success in obtaining injunctive relief — particularly in light of its claim that the recovery of monetary damages was not its initial primary goal — was deemed relevant in reducing the significance of the comparison between the judgment amount and the fee request. Three other factors also influenced the court: (a) the extent to which the defendants' tenacious litigation strategy impacted the amount of SKF's fees; (b) the fact that shortly before the defendants jumped ship, SKF was acquired and the purchase price "assigned great value to the trade secrets used in the business;" and (c) SKF's payment of the fees in full.

Trading Secrets

This decision teaches two lessons. First, it provides a road map for use by a party prevailing on the merits in a fee-shifting case who then seeks reimbursement of a very substantial amount of expenses, especially where the reimbursement request is a high multiple of the damages award. Second, the ruling reminds us that a party who has lost on the merits in a hard-fought fee shifting case, and who then aggressively protests the fee request, is likely to face an incredulous judge.

Employers' Obligation to Defend and Indemnify Rogue Employees In California?

October 14, 2011 by Robert Milligan and Joshua Salinas

On October 12, 2011, the California Court of Appeal in *Nicholas Laboratories, LLC v. Christopher Chen*, No. G044105, 2011 WL 4823329 (Cal. Ct. App. Oct. 12, 2011), held that Labor Code section 2802 does not require an employer to reimburse its employee for attorney fees incurred in the employee's successful defense of *the employer's action* against the employee. While reaffirming the traditional American rule in non-wage related litigation between employees and employers, the decision serves as a reminder to California employers of the implications involved in providing a defense and indemnifying employees in suits brought by third parties, including suits brought by their former employers against employees for trade secret theft.

Labor Code section 2802 provides:

(a) An employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer, even though unlawful, unless the employee, at the time of obeying the directions, believed them to be unlawful.

(b) All awards made by a court or by the Division of Labor Standards Enforcement for reimbursement of necessary expenditures under this section shall carry interest at the same rate as judgments in civil actions. Interest shall accrue from the date on which the employee incurred the necessary expenditure or loss.

(c) For purposes of this section, the term "necessary expenditures or losses" shall include all reasonable costs, including, but not limited to, attorney's fees incurred by the employee enforcing the rights granted by this section.

Nicholas Laboratories, LLC (Nicholas Labs) filed suit against employee Christopher Chen for alleged theft of company property, misuse of the company credit card, and diverting business opportunities away from Nicholas Labs. The trial court entered judgment for Chen and against Nicholas Labs on the complaint and awarded Chen his costs. Chen then moved for attorney fees per Labor Code section 2802. The issue before the Court of Appeal was whether Nicholas Labs was required to "indemnify" its ex-employee, defendant Christopher Chen, for attorney fees incurred by Chen during his successful defense of the action.

Chen asserted that various statutory (Lab. Code, § 2802, subd. (a); Corp. Code, § 317, subd. (d)) and/or contractual indemnity provisions obligated Nicholas Labs to reimburse Chen. Additionally, Chen argued that California's strong public policy favors indemnification of employees by their employers.

The Court of Appeal rejected Chen's argument and held that Labor Code section 2802 does not require an employer to reimburse its employee for attorney fees incurred in the employee's successful defense of the employer's action against the employee. The court stated that indemnification only applies to suits from third-parties and not the employer itself. The court further concluded that Corporations Code section 317 did not apply because Nicholas Labs was a limited liability company and not a corporation.

This case highlights the situation where a new employer provides a defense for and indemnification for a new employee in a lawsuit brought by his or her former employer. Specifically, the issue may arise in the context of an ex-employee's alleged trade secret misappropriation on behalf of or for the benefit of the new employer. Under Labor Code section 2802, an employer is required to indemnify employees in defense against third-parties for "all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer." The broad language of the statute can make new employers, who have little knowledge of miscreants' actions on behalf of their employer, responsible not only for their defense but for indemnification for any money judgment obtained against the employees. Employers need to be particularly vigilant before hiring such high risk employees from competitors to make sure the potential "baggage" in having such employees is worth the risk. Additionally, counsel that represent both the ex-employee and new employer in such suits may have potential conflicts of interest in these joint representation scenarios, which must be constantly monitored.

New Federal Trade Secret Bill Introduced

October 7, 2011 by Robert Milligan

U.S. Senators Herb Kohl (D-WI) and Christopher Coons (D-DE) introduced an amendment to the Currency Exchange Rate Oversight Reform Act yesterday aimed at protecting American trade secrets and innovation.

Currently, Title 18 of the US Code only permits the Attorney General to bring a civil action in federal court for trade secret theft. The amendments would open the federal courts to private parties as follows:

(b) Private Civil Actions

1) *In General-Any person aggrieved by a violation of section 1832 (a) may bring a civil action under this subsection*
2) *Pleadings-A complaint filed in a civil action brought under this subsection shall-*

(A) describe with specificity the reasonable measures taken to protect the secrecy of the alleged trade secrets in dispute; and

(B) include a sworn representation by the party asserting the claim that the dispute involves either substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country.

The amendment also provides for immediate *ex parte* seizure orders and damages for the unlawful conduct.

Senators Kohl and Coons cited two examples of trade secret theft to support their amendment- a Chinese national convicted of stealing trade secrets valued between $50 and 100 million for a Chinese competitor, and a disgruntled Wisconsin employee that attempted to sell aviation related trade secrets valued at hundreds of thousands of dollars to a competitor. Their amendment would enable victims of trade secret theft to seek injunctive relief and compensation for their losses in federal court.

It is important to note that the amendment only provides private civil action when the trade secret theft victim shows a (1) substantial need for nationwide service of process or (2) misappropriation of trade secrets from the US to another country. A nationwide service of process would apply to cases where a state court may have difficulty acquiring personal jurisdiction over multiple defendants residing in

different states. Thus, the amendment would provide relief in cases where the federal court's jurisdiction extends beyond the territorial limitations of the state court.

The amendment aims to primarily protect American business against international and foreign misappropriators. Therefore, trade secret owners should not necessarily view this amendment as a free pass to federal court to assert trade secret claims.

Trade Secrets Along the Time-Space (Internet) Continuum or “Lost in Translation”

September 6, 2011 by Jason Stiehl

Last month, Judge Walls of the U.S. District Court of New Jersey became yet another pioneer in the evolving world of trade secret protection and the Internet. In a well-reasoned and thorough analysis of case precedent, Judge Walls utilized two historic landmark public disclosure cases, *DVD Copy Control Ass'n, Inc. v. Bunner*, 116 Cal. App. 4th 241 (Cal. App. 6th Dist. 2004), and *Data General Crop. v. Digital Computer Controls, Inc.*, 357 A.2d 105 (Del. Ch. 1975), as his guidepost in determining whether certain code language found within Syncsort's Reference manual and scripts remained trade secrets, despite posting of both parts, and, in some instances, all of the language on various websites.

The Guiding Hand of History

Data General and *DVD Copy* present a clear contrast of partial disclosure versus unlimited disclosure. In *Data General*, a pre-Internet disclosure case, a minicomputer manufacture made publicly available, through manuals, general technical information governing its products. The Court held that, unlike a logic diagram, the manuals did "not contain sufficient logic design [ ] to permit their being successfully used of the purpose of either duplicating such machine or in assembling a computer substantially identical to" the Data General's minicomputer. *Data General*, 357 A.2d at 110-11. In contrast, in *DVD Copy*, a foreign computer programmer, through his license agreement, began widespread distribution of the DIVX code associated with copyright protection on DVDs. Rather than suing this individual, the association tasked with protecting the copyright status on DVD's went after a host of United States' individuals who had posted portions of the code on their websites and blogs. Ultimately, by the time the matter came to preliminary injunction, the information had been distributed to over a million people, thus, according to the court, eviscerating the trade secret status of the code, holding that information "in the public domain cannot be removed… under the guise of trade secret protection." *DVD Copy*, 116 Cal. App. 4th at 255.

Bytes and Pieces

In *Syncsort*, the Plaintiff developed a language which allowed users to translate data from one form to another. Syncsort's competitor, Innovative Routines, Int'l ("IRI"), also maintained proprietary software which allowed for a similar translation. However, because the languages were unique, it was difficult and time-consuming for a Syncsort customer to simply switch to IRI's program. To solve this problem, IRI improperly, through a Syncsort distributor, came into possession of a Syncsort Reference Guide which contained over 400 pages of description and definition related to Syncsort's language. IRI then took this guide and developed a translator for Syncsort's translation device-- called ssu2scl-- which

could translate Syncsort scripts to IRI's program language. IRI also requested, from Syncsort customers, examples of Syncsort scripts to run against the ssu2scl to determine the effectiveness of the translation device. The activities of both the distributor and the customers were controlled and governed by confidentiality and licensing agreements prohibiting such disclosures.

Once sued for its activities, IRI went about a hunt throughout the Internet to locate Syncsort's Reference Guide and scripts to demonstrate that, although they may have procured the information from an improper source, the information was publicly available, and therefore should not be afforded trade secret status. Mostly unsuccessful, IRI was initially able to locate only four partial sources and, ultimately, three full sources, where Syncsort's information was available. As to the partial sources, Judge Walls applied the logic of *Data General* and held that the information, in its fragmented and limited form, was not sufficient to recreate the Syncsort language. As to the full sources, Judge Walls looked to *DVD Copy*, and, in contrast, found that the full posts-- found on (1) a university password-protected site; (2) a Korean website taken down within days of notice; and (3) a Japanese website taken down within days of notice-- were "sufficiently obscure of transient or otherwise limited" so that it was not "generally known to the relevant people."

A "Manual" Going Forward?

Although it will be tempting for litigants to cite this case for a black-letter type pronunciations, this author would caution against such efforts. First, the facts of this case tilted well against the Defendant. For example, IRI had: (1) admittedly improperly sought out and received the information; (2) only conducted internet searches *after* being sued to determine whether the information was publicly available; and (3) known that the sources of the information were bound by restrictions governing the sharing of that information. Second, this case has a prolonged and protracted history, including a previous trial on the merits and full summary judgment briefing, allowing for a complete record to develop. Third, the breadth and depth of the release of information remains a case-by-case type determination without any precise formulation. For example, imagine if the Korean manual had been up for five years, or if it had been translated from Korean and posted on an US website. With that said, this case presents what will likely become the paradigm for Internet "release" cases in the future.

"Internet Communications" Alone Insufficient To Invoke Florida Long-Arm Statute Against Lindsay Lohan In Trade Secrets Misappropriation Suit

July 21, 2011 by Eddy Salcedo

White Wave International, Inc. filed an action in Florida against Lindsay Lohan, Lorit LLC, a company she has an indirect ownership interest in, and several other defendants arising out of a certain Confidentiality Agreement Between Firms ("CABF") between White Wave and Lorit. It was alleged by White Wave that the CABF provided Lohan, Lorit and the other defendants with a time-limited opportunity to examine and obtain samples of White Wave's product. It was further alleged that although Lorit made an offer to purchase the product from White Wave, the parties were unable to agree on a purchase price and the relationship was terminated. White Wave's action arose, it alleged, when Lorit, Lohan and another defendant introduced a product which was claimed to contain the nearly identical ingredients as White Wave's product.

White Wave's complaint included five counts including breach of contract, theft of trade secrets (under the Uniform Trade Secrets Act), civil conspiracy, intentional interference with contract and deceptive and unfair trade practices. Lohan moved to dismiss the complaint as against her on the basis of lack of personal jurisdiction (notably, the action had been dismissed as against 3 other defendants previously on similar grounds).

Lohan argued that the court lacked personal jurisdiction over her because she did not have sufficient contacts with the State of Florida with respect to the facts that gave rise to the complaint, specifically regarding the CABF, Lorit or its business. White Wave argued that Lohan communicate with Florida citizens "through the internet" regarding Lorit's product, and that consequently her physical presence in Florida was not necessary to confer jurisdiction. Essentially, that her "telephonic, electronic, or written communications into Florida" regarding Lorit's product were enough to invoke long-arm jurisdiction.

The court dismissed the action as against Lohan, finding that none of the activity prescribed to her by White Wave satisfied Florida's long-arm statute (subparagraphs (1)(a) through (h) of § 48.193 of the Florida Statutes). Although the court agreed that "… a defendant does not have to be physically present in the state to commit a tort under § 48.193(1)(b)" and further that "[t]he Eleventh Circuit has consistently applied [a] broader construction of section (1)(b)", it further held that the cases in which the Eleventh Circuit has applied section (1)(b) to foreign torts causing injury within Florida, the conduct was directed at Florida residents, corporations, or property, and the harm was felt exclusively or primarily in Florida. Because the alleged tortious act was the misappropriation of White Wave's trade secrets, a misappropriation alleged to have occurred outside the State, the alleged tortious act was not directed at Florida residents, corporations or property and thus could not be used to invoke the long-arm statute.

As to the allegation that Lohan committed a tortious act within Florida "by making telephonic, electronic, or written communications" into the State, to wit her "internet communications" promoting Lorit's product, the court found that the cause of action alleged, misappropriation of trade secrets, did not arise from said internet communications. Consequently the court ruled that the "tortious conduct" occurred outside of the state, and the damage alleged were insufficient to satisfy Florida's long-arm statute.

The court similarly rejected plaintiff's argument that its civil conspiracy claim satisfied the long-arm statute. White Wave argued that the long-arm statute conferred personal jurisdiction over an alleged conspirator where any other co-conspirator committed an act in Florida in furtherance of the conspiracy. The court found that the complaint failed to allege sufficient facts from which it could be reasonably inferred that the defendants, including Lohan, "…were part of a conspiracy either engineered in Florida or pursuant to which a tortious act in furtherance was committed in Florida."

The court also rejected the argument that personal jurisdiction over Lohan could be established by the breach of contract provision of the Florida long-arm statute because the CABF was between White Wave and Lorit, and Lohan was only, at best under the facts alleged in the complaint, a member of the limited liability corporation. Consequently, the court found that she could not be personally liable for any liability of the limited liability corporation under the facts alleged, and therefore, jurisdiction under under the Florida long-arm statute failed there as well. As a result, the court did not reach Lohan's due process arguments.

White Wave may decide to pursue its suit against Lohan in another forum where she is subject to personal jurisdiction, such as California.

California Federal Court Recently Invokes "Trade Secret" Exception to California's Anti-Noncompete Statute To Effectively Blue Pencil Noncompete Agreement

July 14, 2011 by Scott Schaefers

In a recent decision involving whether a former employer could obtain a temporary restraining order under its broad non-competition agreement with its former employees and former software development company, the federal court in *Richmond Technologies, Inc. v. Aumtech Business Solutions,* No. 11–CV–02460–LHK, 2011 WL 2607158 (N.D.Cal. July 1, 2011) granted plaintiff's request and enjoined defendants from competing with plaintiff while using its proprietary information. The court attempted to balance plaintiff's property interests in its confidential data and business reputation against California's long held public policy against noncompetition agreements. Ultimately, the court held there was sufficient evidence of defendant's alleged wrongdoing to justify a TRO.

The *Richmond* court effectively "blue penciled," or reformed, plaintiff's broad non-compete agreement, rolling back its provisions to conform with California's "trade secret exception" to California's statutory bar on employee non-competes. Such blue penciling is arguably inconsistent with several recent California state court decisions prohibiting such reformation of overbroad noncompetes. In the end, the case highlights the difficulty in applying a trade secret exception to Business and Professions Code section 16600 and determining whether sued-upon noncompete covenants are necessary to protect an employer's trade secrets.

Plaintiff's Allegations in *Richmond Technologies*

The plaintiff in *Richmond* was a distributor of enterprise planning software. Plaintiff sued defendants, which were plaintiff's source-code company and plaintiff's former employees, for misusing plaintiff's source code and proprietary customer data to unfairly compete with plaintiff, before and after defendants terminated their relationships with plaintiff. In doing so, defendants (plaintiff alleged) breached their noncompete, non-solicitation, and non-disclosure agreements with plaintiff, violated California's unfair competition statute, and were liable under other related common law theories. Notably, plaintiff did not make a claim for trade secret misappropriation under California's Uniform Trade Secret Act (Cal. Civ. Code § 3426.1 *et seq*.).

The noncompete agreement prohibited defendants from competing with plaintiff for one year after their relationships terminated, and the non-solicitation agreements prohibited defendants from soliciting plaintiff's customers during defendants' employment and for one year thereafter. There appeared to be no significant difference in the broad application of the non-solicitation and noncompete agreements; in

fact, the non-solicitation agreements, which contained certain exceptions regarding time lapse and the employees pre-existing relationship with the customer, were narrower than the noncompete. The non-disclosure agreement prohibited defendants from using plaintiff's proprietary data.

The Court's Decision

Even though the court denied an injunction based on plaintiff's non-solicitation agreements because they were overbroad and likely unenforceable under California's statutory bar against restrictive covenants (Cal. Bus. & Prof. Code § 16600), the court issued a limited injunction based on the non-competition agreement. The court noted and discussed at some length the "trade secret exception" under Section 16600, which, despite California's strong public policy against non-competition agreements, permitted claims for breach of noncompete agreements if necessary to protect a trade secret. *Retirement Group v. Galante,* 176 Cal.App.4th 1226, 1237, 98 Cal.Rptr.3d 585 (Cal.Ct.App.2009) and *Edwards v. Arthur Andersen LLP,* 44 Cal.4th 937, 81 Cal.Rptr.3d 282, 189 P.3d 285 (2008). Plaintiff presented sufficient evidence, the court found, that:

- defendants had access to Richmond's customers' specialized requirements;
- defendants set up their competing business almost a year prior to terminating relationship with plaintiff;
- prior to terminating, defendants stopped using their Richmond e-mail accounts to communicate with plaintiff's customer, and instead began using their Aumtech e-mail accounts;
- defendants listed plaintiff's customers on Aumtech's website as Aumtech customers;
- defendants contacted specific plaintiff customers and induced them to switch to defendants; and
- one of the individual defendants, prior to resigning from plaintiff, wiped her Richmond computer using three wiping programs, thus forever deleting many customer files and e-mails that Richmond needed to carry on its business with those customers.

In light of this evidence, the court found that there were, at a minimum, "serious questions going to the merits" of plaintiff's claims which justified its TRO.

Nevertheless, to balance plaintiff's interests against California's policy against noncompetes, the court "narrowly" drew its injunction, such that defendants were prohibited from:

- holding out plaintiff's customers on Aumtech's website as defendants' customers;

- *initiating* contact with plaintiff's customers that defendants knew of or had contact with during their employment with plaintiff (except for broad-based marketing of its products), but defendants were not prohibited from *responding to* requests initiated by such customers;

- using plaintiff's proprietary data to negotiate or do business with plaintiff's customers, but defendants were allowed to do business with those customers so long as defendant's did not use such plaintiff's proprietary information; and

- using plaintiff's source code in their business, but defendants were allowed to market and sell similar products so long as they did not use plaintiff's trade secrets.

The Court's Decision and State Court Authority

The court's findings are arguably inconsistent with recent California state court decisions; however, this is just a decision on the temporary restraining order and not a preliminary injunction. On the one hand, the *Richmond* court held that plaintiff's broad non-solicitation agreements were unenforceable under Section 16600 because they were not "narrowly tailored" to protect plaintiff's trade secrets, even though the agreements contained certain exceptions. Plaintiff's noncompete agreement, however, was just as broad, if not more so - it provided that, upon defendants' termination of their relationships with plaintiff and without exception, they "will not compete with [plaintiff] with similar product and or Service using its technology for a period of one year thereafter." Nevertheless, the court issued the injunction under the noncompete.

In effect, the court blue-penciled or reformed the noncompete to conform to the trade-secret exception under Section 16600. Such blue-penciling has been held impermissible by several California cases, including those which held that employers violate California's unfair competition statute (Cal. Bus. & Prof. Code § 17200) by even requiring employees to sign overly broad noncompete agreements at the beginning of their employment. *See Kolani v. Gluska*, 64 Cal.App.4th 402, 407-08 (1998) (holding that trial court properly declined to rewrite illegal covenant not to compete into a narrow bar on theft of confidential information); *D'Sa v. Playhut, Inc.,* 85 Cal.App.4th, 927, 934-35 (2000) (refusing to narrowly construe invalid covenant not to compete so as to make it enforceable); *Dowell v. Biosense Webster, Inc.,* 179 Cal.App.4th 564, 579 (2009).

Lessons Learned

The takeaways from the *Richmond* decision are that (1) California courts still struggle with whether there is a trade secret exception to Section 16600 that would permit certain narrow noncompete restrictions; (2) when drafting restrictive covenants, employers should make sure they are tailored to protect against the misuse of trade secrets; (3) employers should monitor employee's conduct and keep an eye out for unlawful activity (defendants in *Richmond* allegedly engaged in unlawful activity for

almost a year without plaintiff knowing), and (4) when suing a former employee for breach of contract and trade secret theft, recognize that courts will likely impose heavy pleading and proof burdens, and diligently investigate and document alleged misconduct.

Wiener v. Wiener: A Wiener Controversy Of A Different (Trade Secrets) Sort

June 27, 2011 by James McNairy

There is wiener controversy brewing, but this one does not involve Twitter™ or a Representative from New York. Rather, this dust up concerns a Chicago hot dog dynasty and allegations of misappropriated trade secrets, false advertising, unfair competition, and trademark infringement.

On June 21, 2011, District Court Judge Sharon Coleman denied Vienna Beef LTD's motion for a temporary restraining order which sought to enjoin competitor hot dog maker Red Hot Chicago , Inc. ("RHC") and its founder, Scott Ladany (collectively, "Defendants"), from engaging in various alleged conduct, including using Vienna Beef recipes or claiming that their recipes are century old, date back to 1893, or that they are Sam Ladany or Ladany family recipes. Vienna Beef claims, among other things, that its hot dog recipes are trade secrets and that RHC is using them without permission.

Scott Ladany is the grandson of company founder Samuel Ladany, who in 1893 began selling sausages using a family recipe. Scott Ladany began working for Vienna Beef in 1971 and obtained a 10% stock interest. The Ladany family sold Vienna in the early 1980s to plaintiff Vienna Beef ("Vienna"). Scott Ladany remained employed by Vienna until 1983, when he sold his 10 percent stake in Vienna. At the time Ladany left Vienna, he signed agreements which prohibited him from using or disclosing Vienna's trade secrets and competing with Vienna for a specified term.

In 1986, at the end of the non-compete term, Ladany started RHC.

As to its trade secrets claim, Vienna offered the following evidence of misappropriation (1) that Defendants included language in their advertising stating that Defendants have been making hot dogs "using" a century-old "time honored family recipe" which "is the foundation for a true Chicago-style hot dog…"; and (2) sworn statements by vendors attesting that Defendants claim their products are made with Vienna's recipes.

In her Memorandum Opinion, Judge Coleman held that Vienna had predicated its trade secrets claim on RHC's advertising materials and that RHC effectively rebutted Vienna's allegations. The Court cited to an affidavit filed by Ladany unequivocally stating that RHC does not use the Vienna recipe developed by Ladany's grandfather, but instead developed its own recipe as early as 1986 through work with Heller Seasonings & Ingredients, which recipe has been used by RHC in substantially similar form for 25 years.

Trading Secrets

The Judge concluded that, in any event, Vienna "has shown no evidence that [its] recipes were used in RHC's business and therefore cannot show that it is likely to succeed on the merits of [its claim for misappropriation of trade secrets]." Likewise, the Court found that Vienna had not shown irreparable harm as, but for one new advertisement, the complained of advertising had been used by RHC "for years", thus negating the need for emergency relief. Accordingly, the Court found that Vienna Beef's application did not pass muster and was denied. Based upon the Court's ruling, it will be interesting to see if there is a round two of the wiener wars in the form a preliminary injunction motion.

Affidavits Not Enough to Obtain Injunctive Relief in Alleged Raiding Case

July 26, 2011 by Marcus Mintz

In a recent case filed in the United States District Court for the Northern District of Florida, *Mainline Information Systems, Inc. v. Fordham*, No. 11-137, 2011 WL 2938435 (N.D. Fl. July 21, 2011), the plaintiff sought a preliminary injunction against an individual defendant for tortious interference with business relationships and for misappropriation of trade secrets. Plaintiff provides integrated IT solutions for businesses and other related products and services. Plaintiff contended that the defendant was soliciting more than 20 of its employees directly, and an additional 14 employees indirectly, to terminate their employment relationships with plaintiff and join a competing company. Plaintiff also argued that defendant was seeking to misappropriate its trade secrets through the solicitation of its employees.

The district court denied plaintiff's motion for preliminary injunction because plaintiff failed to demonstrate a "substantial likelihood" that plaintiff would prevail on the merits of either of its two claims, for tortious interference or misappropriation of trade secrets. At bottom, the court found that plaintiff had run into court without the evidence to support its claims. The court specifically found that plaintiff introduced no witnesses to testify at the preliminary injunction hearing and only presented two affidavits in support of its application for injunctive relief. One such affidavit was dismissed as "threadbare" in that it only asserted that the allegations of the complaint were true and correct. The second affidavit was made by one of plaintiff's senior vice presidents who stated that defendant had, directly and indirectly, solicited plaintiff's employees. Neither affidavit was sufficient to meet plaintiff's burden to obtain a preliminary injunction, particularly in light of the evidence put forth by the defendant that contradicted plaintiff's claims.

In contrast to the plaintiff, the defendant testified at the hearing and denied contacting the majority of the employees that plaintiff claimed were solicited by the defendant. The defendant also presented evidence from several of the purportedly solicited individuals who stated they were never contacted by defendant. Based on the foregoing evidence put forth by defendant, which directly contradicted plaintiff's second affidavit, the court denied the motion for preliminary injunction as it related to tortious interference. Similarly, because no evidence was presented regarding defendant's use of any trade secrets, the preliminary injunction was also denied as to defendant's misappropriation claim.

The court's brief ruling is an instruction to would-be litigants that argument by itself is insufficient to obtain injunctive relief in Florida's district courts.

Award of Damages for Misappropriation Does Not Preclude Also Awarding Injunctive Relief

June 22, 2011 by Paul Freehling

Clarifying the legal principle that an injunction will only be entered if there is no adequate remedy at law, the Ohio Court of Appeals held recently that an award of damages for past trade secret misappropriation is not inconsistent with, and does not preclude granting, injunctive relief to prevent future harm. *Litigation Management, Inc. v. Bourgeois*, 2011 Ohio 2794 (Ct. of App. of Cuyahoga County, OH, June 9, 2011).

Litigation Management, Inc. (LMI) provides litigation support services. A number of LMI employees who had signed not-compete and confidentiality agreements left the company's employ and formed a direct competitor which then used LMI's trade secrets. LMI sued for damages and injunctive relief, and the damages case went to trial. After the close of the evidence, the judge blue-penciled the geographic limitations set forth in the agreements (substituting "the Greater Cleveland Metropolitan Area" for any place in the country) and submitted the case to the jury. It returned verdicts for LMI against all of the defendants.

LMI's post-trial motion for an injunction, however, covering the period of time the defendants had worked in violation of their agreements, was denied. The trial court held that "not only is an adequate remedy at law available, it has been given. The wrong of competing unfairly has been righted by the jury's award: LMI has received fair and reasonable redress."

LMI appealed. The appellate court reversed, agreeing with LMI that the monetary relief was intended as a make-whole remedy only with regard to misconduct *to the date of trial.* The appropriate relief for future, threatened violations is an injunction. So, in the view of the Ohio Court of Appeals, there was nothing inconsistent about granting both compensatory damages and an injunction. The moral is that one who misappropriates trade secrets can be hit with both a monetary award for past wrongs and severely debilitating injunctive relief.

Colorado Statute of Limitations For Misappropriation Of A Trade Secret Begins To Run Upon Knowledge That It, Or Even A Related Trade Secret, Has Been Misappropriated

June 19, 2011 by Paul Freehling

Distinguishing between continuing misappropriation of one trade secret and separate misappropriations of related trade secrets can be a daunting task. The Supreme Court of Colorado recently held that, for statute of limitations purposes, the distinction may be inconsequential where misuse occurs on disparate occasions but the proprietary information was disclosed to the same person at substantially the same time, and in furtherance of the same commercial venture. That constitutes misappropriation of a single trade secret.

Gognat developed proprietary information relating to the methodology for identifying and extracting reserves of oil and gas. In 1997, he shared this information with Ellsworth when they entered into a joint venture to develop reserves in western Kentucky. At about the same time, Ellsworth secretly formed MSD Energy, Inc. (MSD) for the same purpose.

By January 2001, Gognat knew that MSD was using his trade secrets in connection with acquiring leases in the same area of Kentucky as the joint venture. He demanded that the joint venture compensate him. Ellsworth assured him that his demand would be resolved fairly. Relying on that assurance, Cognat deferred filing a lawsuit against Ellsworth and MSD. That proved to be a big mistake.

In 2005, Gognat learned that MSD was using his proprietary information in connection with development of a different area of western Kentucky, and that MSD's activities in the first area were more extensive than he had previously known. He filed suit against Ellsworth and MSD for misappropriation of trade secrets. The defendants moved for summary judgment based on Colorado's three-year statute of limitations, contending that Cognat was aware four years earlier, in 2001, that Ellsworth and MSD were using the trade secrets. Gognat responded that until 2005 he did not know, and had no reason to suspect, that Ellsworth and MSD were using his trade secrets in the second area. The trial court granted the defendants' motion to dismiss, and both the Court of Appeals and the Supreme Court affirmed. *Gognat v. Ellsworth*, 224 P.3d 1039 (Colo. App. 2009), *aff'd*, Case No. 09SC963 (Colo. Sup. Ct., June 6, 2011).

Colorado's Trade Secrets Act is modeled after the Uniform Act. It defines a trade secret as all or part of proprietary information that the owner has taken measures to prevent from becoming available beyond

those to whom the owner has given limited access. In the instance of separate acts of misappropriation with respect to related trade secrets, when does the statute of limitations begin to run? According to the Colorado Supreme Court, the misconduct of Ellsworth and MSD was one continuing misappropriation and, therefore, the cause of action accrued in 2001 when Gognat learned of the first instance of misuse. Further, the fact that what Gognat knew in 2001 may not have been sufficiently damaging to justify the cost of litigating is immaterial.

The *Gognat* decision teaches that litigation with respect to trade secret misuse must be initiated promptly after learning of misappropriation, even though accrued damages may be quite modest. Otherwise, the claim may be held to have been waived by the passage of time notwithstanding a substantial subsequent increase in the amount of resulting damages. Contact a trade secrets attorney at Seyfarth Shaw for assistance in determining whether a potential trade secrets misappropriation cause of action is time-barred.

Electronic “Redactions” Not Always Effective: Greater Caution In Dealing With Sensitive Materials In Trade Secret Cases Necessary

June 6, 2011 by Eddy Salcedo

The ABA Journal reports that a Princeton PhD candidate study has found electronic “redactions” included on PDF documents may not always be effective. Specifically, the study revealed that a computer program was able to scan 1.8 million Pacer filed documents, identify 2,000 documents that contained redactions (in the form of the ubiquitous “black boxes” obscuring the confidential information) and further identify 194 of these redactions which were able to be removed and the “confidential” information revealed. The “flaw” appears to be in the PDF documents themselves, and how they were created. The author of the study, Timothy Lee, explained that PDF documents consist of multiple layers, and that an improperly placed “redaction box” might not completely obscure the confidential information which is sought to be protected. Mr. Lee explains that “retrieving” the redacted information could be as simple as cutting and pasting from the PDF document.

Mr. Lee offers suggestions for legal practitioners looking to avoid the pitfalls of “failed” redactions, but the greater issue raised by the study is the danger in not fully exploring and understanding the technology we as lawyers are using to aid and further the representation of our clients. Although the study focuses on Pacer filed documents, “redacted” PDF files are exchanged by parties regularly during discovery, particularly now in the age of e-Discovery. Where once documents were redacted by-hand before copying was done, and the confidential information never being on the produced document, as Mr. Lee indicated redaction on PDF documents is usually accomplished by adding a “black box” layer to the information sought to be protected. Depending on how the PDF document is then handled, the information might still be accessible. Simply assuming that because you cannot “see” the information on the screen it is “gone” can be a dangerous plan. Attorneys would be well served to ensure that their electronic redactions are as secure as those made by the old fashioned black marker. This means not only looking at the PDF documents before sending them along to opposing counsel and/or electronically filing with the court, but ensuring that the redactions are to all of the layers of the PDF, and that they cannot be otherwise reversed.

Confidentiality agreements, “claw-back” provisions and protective orders may be able to recapture information inadvertently revealed to opposing counsel, but the lurking peril here is that none of these will recapture information lost to a non-party Pacer search similar to the one Mr. Lee ran for his study. Greater caution, and greater familiarity with the technology we are using, is the name of the game, especially if a company's trade secrets are in play.

Delaware Court Enjoins Use of Ex-Employers Trade Secrets

April 16, 2011 by Paul Freehling

Delaware Court of Chancery Vice Chancellor J. Travis Laster, faced with an unreasonable non-compete/non-solicitation agreement, indicated that he would have preferred to hold it invalid but said that he had no choice other than to modify its terms because its Maryland choice-of-law provision requires judicial "blue penciling." He did enjoin the ex-employee from using his ex-employer's customer list, a trade secret, but held that the ex-employee may call on any customer whose name is within his own knowledge.

Delaware Elevator, Inc. ("DEI"), a national elevator installer and servicer, sued ex-employee John Williams who had 20 years of experience in the industry (six of them with DEI) at the time he left that corporation and started his own — one man — competing elevator maintenance company. He had signed an agreement with DEI (a) barring him for three years after leaving its employ from working in a competing business within 100 miles of any DEI office, and (b) prohibiting him from soliciting business from anyone who during the last six months of his employ had been either an actual DEI customer or a potential customer DEI was actively soliciting. While he claimed his signature on the agreement was a forgery, the court said that no rational fact finder could accept his claim.

The agreement contained a Maryland choice-of-law provision and a stipulation that a violation would inflict irreparable harm on DEI. Maryland law upholds non-competes if the restraints are reasonably necessary for the protection of the employer, do not impose an undue hardship on the employee, and are in the public interest. Even DEI recognized the unreasonableness of the territorial restriction as written (within 100 miles of any DEI office) and sought to enforce the agreement within 100 miles of just the Newark, Delaware office where Williams worked.

The Vice Chancellor observed that Williams has 34 years in the workforce, has personal and family ties to the area where he has been working, and could not readily re-locate or find an equivalent job in a new field. Rhetorically, the court asked DEI's attorneys "how they would fare if forced to re-start in a far-off jurisdiction, to re-invent themselves as practitioners in a completely different subject-matter area, or to leave the law entirely and find employment in another industry."

While he might have preferred to invalidate the agreement altogether, the Vice Chancellor stated that Maryland "does not authorize a policy-based refusal to enforce an unreasonable non-compete agreement. Maryland law instead calls on the court to carve back overly broad restrictive covenants by wielding the judicial 'blue pencil.'" Accordingly, he modified the restrictive provisions to a two-year-30-miles-from-Newark-radius (since the two year period began January 17, 2010, Williams' date of

termination, it will expire less than one year after the decision was announced in March 2011). The court observed that, as modified, Williams would be able to earn a living by using his contacts and knowledge of the industry outside the non-compete zone immediately, and within the zone shortly, while at the same time DEI's relationships with existing and prospective customers were adequately protected.

Williams admitted that he took a DEI customer list with him and used it. Because the list was held to constitute a trade secret, he was ordered to destroy all electronic and paper copies. However, the court said he is free to call on customers he knows, even if their names are on the list. A hearing on damages for wrongful use of the list will be scheduled.

Employers should be cognizant of the applicable legal principles when they include a choice-of-law provision in a non-compete or non-solicitation agreement. If DEI's agreement with Williams had provided for application of Delaware law, the agreement might have been voided altogether. By applying Maryland law, the employer salvaged at least some protection. Designation of another state's law might have been even more favorable to the employer. Ask your Seyfarth Shaw trade secrets attorney for advice about choice-of-law provisions.

Michigan Court Orders Corporation to Reveal Facts Regarding Potential Misappropriation

April 1, 2011 by Paul Freehling

Entities do not have the right to claim a privilege against self-incrimination. Accordingly, even though agents of a corporation may refuse, based on the Fifth Amendment, to comply with a court order requiring the individuals to submit an affidavit stating whether their principal has ever possessed specified products that allegedly embody purloined trade secrets, the corporation itself must abide by the order even though the effect may be incriminate the agents.

PCS4LESS, LLC and an affiliated company sued a corporation and certain of its employees in a Michigan state court, alleging that the plaintiffs were the exclusive licensees with respect to certain software, which constituted trade secrets, used in the secondary market for refurbished cell phones. The plaintiffs claimed that the defendants had misappropriated the software. The court was asked to enter a TRO directing the defendants neither to use nor to destroy the trade secrets, and to deliver the products containing the software to the plaintiffs.

Initially, the defendants denied that they possessed, or ever had possessed, the products. However, when the court required submission of an affidavit to that effect, the defendants declined on the ground that the information at issue was protected by the Fifth Amendment. Plaintiffs moved to compel all of the defendants to comply with the earlier order, the court granted the motion, and they appealed.

The Michigan Court of Appeals agreed with the employees that their own privilege against self-incrimination could be compromised if they, individually, were forced to comply. So, the trial court's order was reversed to that extent. But the appellate court affirmed the order requiring the corporate defendant to submit the affidavit, rejecting the argument that compelling the corporation to reveal whether it has possessed the software essentially would disclose the same information that the individual defendants were excused from providing. The court pointed out that "organizations with independent existence apart from their individual members may not assert the Fifth Amendment privilege." Analogizing the individual defendants to custodians of corporate records, the Court of Appeals stated that "the custodian of an organization's records may not refuse to produce records even if those records might incriminate the custodian personally." *PCS4LESS, LLC v. Stockton*, Nos. 296870 and 09-000380-CZ (Mich. Ct. of App., Mar. 8, 2011), *citing Paramount Pictures Corp. v. Miskinis*, 418 Mich. 708, 344 N.W.2d 788 (1984).

The *PCS4LESS* case shows that wrongful possession of someone else's proprietary information can lead not only to a civil suit for damages but also to criminal prosecution. Trade secret counsel should be consulted promptly by anyone charged with misappropriation.

Court Of Federal Claims Details How To Compute Damages For Misappropriation Of An Asset That Has No Readily Ascertainable Market Value

March 8, 2011 by Paul Freehling

A few years after ruling that the Air Force violated the confidentiality clauses of contracts with a government contractor by disclosing its proprietary information relating to the manufacturing process for a conveyor used in assembling smart bombs weighing more than a ton each, the Court of Federal Claims recently determined the contractor's damages. The court treated the controversy as involving a "lost asset" for which there is no known market, and not a "lost profits" case as the Government contended. Therefore, the appropriate measure of damages was an estimate of the amount a willing buyer would have paid a willing seller for the proprietary information. The proper methodology was to multiply the number of conveyor units the Air Force expected to purchase as of the date of the breach, times the contractor's bid price, times a reasonable profit, and then to discount for the "risk that a potential buyer of [the] proprietary information would associate with realizing the profit stream deriving from the use of that asset." *Spectrum Sciences & Software, Inc. v. U.S.*, No. 04-1366C (Court of Fed. Claims, Feb. 14, 2011) (the court's decision regarding liability is reported at 84 Fed. Cl. 716 (2008)).

Over the course of several decades beginning in the early 1970s, the Air Force developed and upgraded the conveyors. In 2000, Spectrum Sciences & Software (Spectrum) self-funded an effort, which ultimately failed, to become the principal supplier of new versions of the conveyor. However, Spectrum needed the Air Force's cooperation in order to refine and test its products. So, the parties entered into a Cooperative Research and Development Agreement (CRADA) which prohibited disclosure by either of them of the other's proprietary information. Since Spectrum's confidential data was expressly identified in the CRADA, protection should have been assured. Moreover, when Spectrum thereafter submitted a proposal to build the conveyor and the proposal contained the data, the cover page of the submission "warned, *inter alia*, that '[t]he data in this proposal will not be disclosed outside the Government and will not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate the proposal.'"

Ultimately, Spectrum's proposal was rejected. However, it was not returned to Spectrum, and contrary to orders the contracting officer opened it and circulated it among a number of Air Force officials. Spectrum's proprietary information then was used extensively by the Air Force procurement team and was incorporated in a subsequent RFP that was distributed to outside vendors, including Spectrum's competitors.

The trial with respect to liability was bifurcated from the damages determination. With respect to liability, in 2008 the Court of Federal Claims held that "the Air Force repeatedly breached the CRADA in failing to

protect adequately Spectrum's proprietary information." *Spectrum*, 84 Fed. Cir. at 744. At the subsequent trial on damages, each party presented an expert witness. Spectrum's expert computed its damages as roughly four times the amount proposed by the Government. The final award was $1.2 million.

A significant reason for the difference between the two valuations resulted from Spectrum's expert basing damages on the number of conveyor units the Air Force *anticipated* buying as of the date of the breach (2003) whereas the Government's expert used the much smaller number that had actually been ordered on the date when the court's liability ruling was issued (2008). The court observed that the number ultimately ordered was irrelevant because it was a function, in part, of the poor performance by Spectrum's competitor that had been awarded the contract, something that could not have been known or anticipated several years before when the breach occurred.

With regard to the per unit price, Spectrum's expert used the company's initial bid. Although that bid had been rejected, and while "unaccepted offers to sell property, like other unconsummated transactions, generally represent poor barometers of value," in this instance use of the bid price was appropriate. It was well below the Government's pre-bid estimate, and it approximated Spectrum's selling price to the United Kingdom for the same product. The Government's expert, by contrast, suggested use of Spectrum's bid for a similar product several years after the breach, but the court disagreed because that bid constituted "a last ditch effort by Spectrum to realize something from its efforts . . . [at a time it was competing] with firms that were being handed its intellectual property *gratis*." Thus, that bid was "based upon a price cut triggered by the Air Force's improper release of Spectrum's proprietary information [and] would effectively reward defendant for the misconduct of its officers in a way that the law simply does not countenance."

With respect to the appropriate profit margin, the court held that a reasonable expectation of profit was the 15% ceiling for federal procurement under a cost-plus-fixed-fee contract (even though this procurement involved simply a fixed-fee contract). Finally, the proper way to compute the discount rate was to take the risk-free interest rate (for short-term Treasuries) plus an equity risk premium, plus or minus factors reflecting the riskiness of investing in stock of a company in Spectrum's industry, of a company Spectrum's size, and of a company like Spectrum that had a key-customer dependence factor. Having decided that "defendant appropriated significant benefits for itself and inflicted significant harm on plaintiff by breaching the CRADA," it is not surprising that substantial damages were awarded.

This opinion is significant for several reasons. First, it is a rare example of a court detailing the method of computing damages in a lawsuit involving misappropriation of proprietary information for which there is no known market. Second, the court clearly differentiated between the valuation of a lost asset and the computation of lost profits.

Emails Sent By Employee To Attorney From Company Computer May Not Be Privileged

February 28, 2011 by Seyfarth Shaw LLP

On January 13, 2011, in *Holmes v. Petrovich Development Company, LLC*, a California Court of Appeal ruled that emails sent by an employee to her attorney from a company computer were not privileged.

Read our Seyfarth Shaw Labor & Employment Department's alert here. This should be of particular interest in all employee-related cases, including trade secrets and non-compete cases. As the alert notes:

This case reminds employers of the importance of having a strongly worded and clearly written policy on employee use of employer-provided technology such as computers, email systems and voice mail systems for personal reasons. These policies also should specify that employees have no expectation of privacy in their non-work communications and that all employer-provided technology is subject to monitoring, even if it is password-protected.

Having clear technology policies are also particularly important to protecting trade secrets and other confidential information.

Jury Must Decide Whether A Manufacturing Process That Is Disclosed In An Expired Patent And Is Not Concealed From Visitors To The Plant Constitutes A Trade Secret

February 21, 2011 by Paul Freehling

When a defendant, sued by a former employer for misappropriating a manufacturing process that allegedly constituted a trade secret, denies that the process is confidential and files a counterclaim alleging that the plaintiff is engaged in sham litigation in order to stifle competition, is it appropriate for the court to instruct the jury that the evidence shows plaintiff does not have a valid trade secret? In a recent case, the trial judge gave such an instruction which led to a multi-million dollar jury verdict for the defendant. The appeal that followed is reported in *Whitesell Int'l Corp. v. Whittaker*, 2010 WL 3564841 (Mich. App., Sept. 14, 2010) (affirming the judgment below; 2-1 ruling that the instruction was appropriate), *vacated on reconsideration*, 2011 WL 165405 (Mich. App., Jan. 18, 2011) (vacating the judgment below and remanding for a new trial; unanimous decision that the instruction was inappropriate).

The sole manufacturer of interconnected "pierce nuts" filed a trade secret misappropriation lawsuit in Wayne County, Michigan, against an ex-employee who allegedly was using the plaintiff's manufacturing process in a competing business. Pierce nuts affix materials to sheet metal.

Responding to the lawsuit, which was the third one between the parties, the ex-employee successfully moved to dismiss the claim on the ground of res judicata. In a counterclaim for tortious interference with a business relationship and expectancy, he denied that the process was confidential, and he demonstrated that the process was readily visible to plant visitors and was disclosed in detail in an old, expired patent. He also proved that the plaintiff's employees were not required to sign confidentiality agreements and that no document referred to the process as confidential. Accordingly, he maintained that the plaintiff was engaging in sham litigation which was a "flagrant violation" of the Michigan Antitrust Reform Act and part of an unlawful effort to preserve a monopoly. Insisting that it had acted reasonably in filing the lawsuit, the plaintiff produced witnesses who testified to their understanding that the process was confidential.

Immediately prior to the start of deliberations following a 25-day trial, the jury was instructed that the manufacturing process did *not* constitute a trade secret. Naturally, the jury then decided the counterclaim for the defendant. Including attorneys' fees and pre-judgment interest, the counterclaimant was awarded more than $8 million.

The manufacturer appealed with interesting results. Initially, the Michigan Court of Appeals affirmed, 2-1. The dissent insisted that the claim should not have been dismissed on res judicata grounds and that the counterclaim instruction was improper and highly prejudicial. On reconsideration, the panel vacated the judgment and remanded for a new trial, concluding that the dissent had been correct in saying that the judge below should have let the jury decide the trade secret question. However, the ruling in the initial opinion regarding res judicata was left unchanged. The judge who initially had dissented now concurred in the portion of the decision on reconsideration remanding because of the improper trade secret instruction, but he continued to dissent with respect to the reiterated ruling on res judicata.

As this case illustrates, in trade secret misappropriation litigation a party alleging that a manufacturing process is confidential has an uphill battle to obtain a sustainable directed verdict where there is a dispute concerning whether the process constitutes a trade secret.

New Article On Trade Secret Litigation In State Courts Released

February 15, 2011 by Robert Milligan

An article published yesterday in the Gonzaga Law Review presents an interesting analysis of trade secret litigation in state courts. Authors David S. Alming, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum, and Jill Weader published the follow-up article to their article last year concerning trade secret litigation in federal courts. According to the new article, they analyzed 2,077 state appellate court decisions issued between 1995 and 2009 and coded 358 of them for 17 relevant factors.

Here are some interesting findings from their article:

- In more than 90% of trade secret cases in both state and federal courts, the alleged misappropriator was either an employee or business partner of the trade secret owner.
- Just five states account for about half of all trade secret litigation in state appellate courts. California leads the pack (16% of cases), followed by Texas (11%), Ohio (10%), New York (6%), and Georgia (6%).
- State appellate courts affirmed 68% of trade secret decisions and reversed 30% of them.
- State appellate courts favor defendants. Alleged misappropriators (the defendants) prevailed in 57% of cases and trade secret owners (the plaintiffs) prevailed in 41%.
- State courts appear to be a tougher venue for trade secret owners who are suing business partners than for those suing employees. Trade secret owners won 42% of the time on appeal when the owner sued an employee, but only 34% when the owner sued a business partner.
- For decades following its 1939 publication, the Restatement (First) of Torts “was almost universally cited by state courts, and in effect became the bedrock of modern trade secret law.” James Pooley, Trade Secrets § 2.02[1] (2010). Those days are over. Only 5% of the cases in the state study cited the Restatement.
- Unlike federal courts, which cite persuasive authority in more than a quarter of cases, state courts cited persuasive authority in only 7% of cases.
- In contrast to the exponential growth of trade secret litigation in federal courts, trade secret litigation in state appellate courts is increasing, but only in a linear pattern at a modest pace.
- Of all the reasonable measures trade secret owners took, only two statistically predicted that the court would find that this element was satisfied: confidentiality agreements with employees and confidentiality agreements with third parties.

Fitness Companies Spar Over Unauthorized Access Of Departing Employee's Personal E-mail Accounts

January 25, 2011 by Robert Milligan and Josh Salinas

Wrongfully accessing someone's personal email account may cost you $1,000 per unauthorized access, even if that person suffers no injury or loss. In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 2010 WL 5222128 (S.D.N.Y. 2010), a New York district court permitted the recovery of statutory damages under the Stored Communications Act (SCA) (18 U.S.C. § 2707(a)) without proof of actual damages sustained.

Lauren Brenner allegedly hired former U.S. Marines Ruben Belliard and Alex Fell to work as "drill instructors" at her Pure Power Boot Camp physical fitness center. While still employed at Pure Power, Belliard and Fell allegedly made plans to open a competing boot camp style physical fitness center. Belliard and Fell left Pure Power, and shortly thereafter opened Warrior Fitness Boot Camp.

Fell alleged that after he left, Benner, or someone from Pure Power, accessed his personal e-mail account and printed e-mails from his personal Gmail, Hotmail, and Warrior Fitness accounts. Fell had left his username and password information saved on Pure Power computers, which allowed access to his email accounts. The emails revealed that Belliard and Fell allegedly copied Pure Power documents, stole Pure Power customers, and shredded their non-compete agreement.

Benner allegedly read these emails and Pure Power Boot Camp brought claims against Belliard and Fell, which included claims for breach of their non-compete agreements and theft of Pure Power's business model, customers, and documents.

Fell counterclaimed against several parties, including Brenner and Pure Power, alleging that the unauthorized access of Fell's account violated the SCA and entitled him to statutory and punitive damages, as well as attorneys' fees.

A significant issue in this case was whether Fell could recover statutory damages under the SCA, even though he failed to allege or prove actual damages. In fact, Fell confirmed in his deposition that he sought only statutory and punitive damages.

On summary judgment, the court held that proof of actual damages is not required to recover under the SCA. The interesting aspect of this case was the court's departure from the holding in *Van Alstyne v. Elec. Scriptorium, Ltd.*,560 F.3d 199 (4th Cir. 2009), the only federal appellate decision to analyze this issue. *Van Alstyne* required proof of actual damages in order to recover the $1,000 statutory damages under SCA. *Van Alstyne* based its decision on *Doe v. Chao*, 540 U.S. 614 (2004), where the Supreme

Court required proof of actual damages for recovery under the Privacy Act. However, the *Pure Power* court criticized *Van Alstyne*'s analysis because the SCA and Privacy Act have different purposes, language construction, and legislative histories.

Indeed, according to the court, an overwhelming majority of jurisdictions decided after *Doe* permit recovery of statutory damages under the SCA absent actual damages. This has been applied to unauthorized access of employee's email accounts (*Cedar Hill Assocs., Inc. v. Paget*, No. 04cv0557, 2005 WL 3430562 (N.D. Ill. 2005)), restricted websites (*In re Hawaiian Airlines, Inc.*, 355 B.R. 225 (D.Haw. 2006)), and social media accounts (*Pietrylo v. Hillstone Restaurant Group*, No. 06-5754, 2009 WL 3128420 (D.N.J. 2009)).

The court, however, rejected Fell's argument that each e-mail that was accessed constituted a separate $1000 violation under the SCA. The court found that, because the period over which the emails were accessed was relatively short (a nine day period), and because there was no evidence indicating the specific number of times each account was accessed, it was appropriate to aggregate the intrusions with respect to each individual e-mail account and find that there had been four independent violations of the SCA --one violation for each unauthorized access of an electronic communications facility, which allowed access to electronic communications while still in electronic storage. The court also rejected Fell's request for punitive damages at this stage in the proceedings because the court was unable to determine as a matter of law which party accessed the email accounts, and the surrounding circumstances, and therefore, there was no basis upon which to decide whether punitive damages were appropriate. The court also rejected Fell's request for attorneys' fees as premature because the court was presently unable to determine which of the parties named in the counterclaim was liable for the four violations of the SCA.

The *Pure Power* court's affirmation of some employee privacy rights and the removal of the actual damages hurdle to a SCA claim have several implications for employers and management. First, increased attention must be given when dealing with employee personal e-mail and social network accounts. The decision does not impair the ability to monitor employee web activity or work provided email accounts, provided that the employer has clear policies articulating that employees have no expectation of privacy. However, extra care must be given to employee personal accounts, particularly when the employee saves login information on the computer and the login information is used to access the employee's personal accounts. Employers should not engage in such conduct.

In *Pure Power*, the access of Fell's email accounts created a cause of action to recover statutory damages for Fell, where the employer may have a solid non-compete/unfair competition suit against the employee. Perhaps more detrimental to employer Pure Power Boot Camp, the court also excluded the highly relevant emails demonstrating alleged employee disloyalty from evidence. Finally, the ability to recover statutory damages without proof of actual damages, as well as punitive damages and

attorney fees, may provide an incentive for employees and their counsel to pursue SCA claims against current and former employers.

Computer Fraud and Abuse Act

Employers May Have Sweat Equity In Their Executives' LinkedIn Accounts, But Employees Score Win In War Over The Applicability Of The Federal Computer Fraud And Abuse Act In The Workplace

January 5, 2012 by Scott Schaefers

In the age of social media and networking, where employees undoubtedly use their company-issued computers to network with customers, vendors, colleagues, and friends, a legal question presents itself: can employers claim an interest in their employees' LinkedIn accounts, or other social networking accounts, which the employees use in part to grow and maintain their relationships for the benefit of their employers?

A. Can An Employer Claim Ownership Of Its Executive's LinkedIn Profile?

A federal court in Philadelphia recently said "Yes," though not definitively. In *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011), the 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. More specifically, the court refused to dismiss employer Edcomm's counterclaims for "misappropriation of an idea" and unfair competition against its former chief executive, Dr. Linda Eagle, who allegedly accessed and used her Edcomm-generated LinkedIn account three weeks after she was terminated. Edcomm had an established policy requiring its executives to create LinkedIn accounts using an Edcomm-prepared template, and requiring them to respond to LinkedIn client and colleague inquiries using an Edcomm template. This policy and participation regarding the executive's LinkedIn account and activities was enough to state a valid claim for misappropriation of Edcomm's alleged ownership of the account. Notably, the court did not cite any social-networking-related precedent in its decision.

And interestingly, the court dismissed Edcomm's claims of statutory trade secret misappropriation and common law conversion to the extent they were premised on Eagle's alleged misuse of the connections and content in her Edcomm LinkedIn account. The court held that such connections could not be trade secret if they were posted on the internet.

There is another active case in the Northern District of California that we previously blogged on that addressed similar issues.

The lesson here is that employers and their lawyers should consider getting more involved in their employees' social-networking activities, particularly to the extent that such activities are used for company business and where employees are required or expected to promote themselves on behalf of the company using these networking sites. The day may come where the employer wished it would have kept a closer eye on departing employees' online profiling.

B. The *Eagle* Court Sides With The Pro-Employee Line Of Cases Which Hold That Employers Cannot Use The Federal Computer Fraud And Abuse Act To Sue Employees Who Misuse Their Employers' Computers

The *Eagle* decision is noteworthy for another reason: it agreed with other federal courts which held that employers may not sue unfaithful employees under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. (CFAA) for stealing or misusing company computer files, so long as the employees had authorized access to the computers for company business.

The court noted the existing divide between federal courts – some which hold that employers may sue employees under CFAA (*e.g. EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2007), *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), *see also U.S. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010)), and some which hold they may not (e.g. *Int'l Ass'n of Machinists & Aerospace Workers v. Werner–Masuda*, 390 F.Supp.2d 479, 498 (D. Md. 2005) and similar Pennsylvania federal cases). Congress and the Supreme Court have yet to resolve this conflict among lower federal courts. Until then, whether employers may sue their employees under the CFAA may depend largely on the federal circuit court of appeals in which the employer or employee is located.

Key Computer Fraud and Abuse Act Case Heard By Ninth Circuit En Banc Panel: Can Rogue Employees Be Held Liable For Data Theft Under The Computer Fraud and Abuse Act?

December 16, 2011 by Robert Milligan

The Ninth Circuit held oral argument on the key United States v. Nosal case yesterday before an en banc panel.

The Court has made the oral argument available on-line.

At stake is whether the government can maintain criminal charges and an employer can maintain a civil cause of action under the Computer Fraud and Abuse Act against an employee who steals company data by "exceeding authorized access" in violation of an employer's computer usage policies.

Ninth Circuit Chief Judge Alex Kozinski repeatedly challenged the Justice Department's position on the scope of the CFAA during the oral argument and questioned why the government should be able to prosecute individuals for providing false information on Facebook, Google, or Match.com in violation of terms of use agreements or using work computers in violation of employer policies.

Ninth Circuit Judge Richard Tallman challenged Nosal's position by questioning why employees should not be held responsible under the CFAA for violating clear and express computer usage policies by stealing company data.

Oral argument revealed that the en banc panel is likely divided on whether to reverse to the Ninth Circuit's April decision which permitted the government to maintain its indictment against the employee for violating the employer's computer usage policies.

Department of Justice Takes Pro-Employer Stance On Amendments To Computer Fraud And Abuse Act: Employers Should Continue To Be Able To Hold Employees Liable For Violations Of Computer Usage Policies Under The Act

November 22, 2011 by Robert Milligan and Joshua Salinas

In connection with proposed Congressional amendments to the federal Computer Fraud and Abuse Act (CFAA), on November 15, 2011, Department of Justice Deputy Chief Richard W. Downing (Computer Crime and Intellectual Property Section) emphasized the importance of an expansive CFAA before the House Committee on the Judiciary and came out against attempts by critics of the CFAA to restrict employers' ability to use the CFAA against employees who steal company data in violation of company computer usage policies. The Department of Justice prepared a statement in advance of Mr. Downing's live testimony.

Mr. Downing addressed concerns that an expansive reading of "exceeds authorized access" under the CFAA might subject computer users to prosecution for merely violating a website's terms of use. We have blogged about recent cases in which courts have applied an expansive view of the CFAA. In *U.S. v. Nosal*, the Ninth Circuit Court of Appeal held that an employee's violations of an employer's computer use policies constituted "exceeding authorized access." A California district court in *Facebook v. MaxBounty* applied *Nosal's* holding and found that Facebook could sufficiently state a claim under the CFAA because the defendant advertising company had violated Facebook's terms of service policies. Note, the Ninth Circuit Court of Appeal recently ordered that *Nosal* be heard before an en banc panel.

Mr. Downing stressed that a restrictive reading of the CFAA would make it difficult or impossible to deter and address serious insider threats, including threats by rogue employees working for competitors to steal their employers' data. Technology has become so pervasive that nearly every employee is required to access database with large amounts of information. Mr. Downing highlighted the importance of protecting the nation's economic security and not just national security. Indeed, businesses should have confidence that their confidential, proprietary, and/or trade secret information is protected.

Mr. Downing provided several examples in which a restrictive reading of "exceeds authorized access" would allow violators to escape any liability for their wrongdoings. For example, in 2006 a contract systems administrator for a medical services provider used his authorized computer access to download thousands of employee names and social security numbers. *See United States v. Salum*,

578 F. 3d 682 (7th Cir. 2009). In 2008, nine employees of Vangent, Inc. used their authorized computer access to obtain and disclose loan records and confidential information regarding President Obama and other well known political figures, celebrities, and sports figures. A restrictive reading of the CFAA would not only hurt employers, but would also hurt the public and customers whose information is often the subject of data theft.

Mr. Downing highlighted that the use of employer agreements and internal computer usage policies are routinely used for prosecuting offenders in such cases. Mr. Downing reiterated the Department of Justice's growing concern that advancements in computer technology have increased the vulnerability of businesses which rely on trade secret, confidential, and/or proprietary information. In the age of Wikileaks, Facebook, Twitter, and rapidly evolving social media, employees are able to leak company information to the entire world in only a matter of minutes. Mr. Downing and the Department of Justice support the ability of companies to be proactive and clearly communicate the restrictions on computer usage to employees and hold them accountable in civil and criminal court for violations of such policies. Restricting the CFAA to only hackers (rather than insiders) through proposed amendments to the CFAA would provide employees a license to steal company data and weaken a company's defenses in protecting its data.

Dead Again? Use of Computer Fraud and Abuse Act By Employers To Combat Employee Data Theft Limited By Ninth Circuit's Latest Ruling

October 29, 2011 by Robert Milligan

The Ninth Circuit Court of Appeals ordered that *U.S. v. Nosal* be reheard en banc by all of the Appeals Court judges 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.

Should the Ninth Circuit reverse the decision, the U.S. Supreme Court may elect to take the decision as a Ninth Circuit 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.

Liability Under Computer Fraud and Abuse Act For Violating Computer Use Policies Gains Momentum In Ninth Circuit

October 6, 2011 by Robert Milligan and Joshua Salinas

The Ninth Circuit's important *U.S. v. Nosal* decision is gaining momentum. On September 14, 2011, a California district court in *Facebook v. MaxBounty,* the Honorable Jeremy Fogel, presiding, became one of the first courts to apply *Nosal*, reaffirming that the violation of computer use policies constitutes "exceeding authorized access" under the Computer Fraud and Abuse Act (CFAA). In doing so, *Facebook* arguably reinforced the legal protections for employers against employees who steal or remove electronic files or data in violation of their employers' written computer-use restrictions.

Facebook is one of the most popular social networking websites with more than 500 million active users. It requires users to agree to its terms of use, which include regulation and restrictions regarding advertising on its website. Facebook's advertising guidelines prohibit advertisements that are fraudulent, deceptive, or misleading.

Maxbounty is an online advertising and marketing company that drives internet traffic to its customers' websites.

Facebook alleged that MaxBounty engaged in impermissible advertising and commercial activity on its website. Facebook alleged that MaxBounty created Facebook pages that were intended to re-direct unsuspecting Facebook users to third-party commercial websites.

Facebook brought a claim, *inter alia*, under the CFAA against MaxBounty for "knowingly and with intent to defraud, access[ing] of a protected computer without authorization or exceeding authority." 18 U.S.C. § 1030(a)(4).

MaxBounty moved to dismiss Facebook's CFAA claim per Federal Rule of Procedure 12(b)(6). MaxBounty argued that it could not act "without authorization" or "exceed authority" because Facebook granted MaxBounty access to the Facebook website.

The district court rejected MaxBounty's argument, citing *Nosal's* holding that "an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed [ed] authorized access." *U.S. v. Nosal*, 642 F. 3d 781, 789 (9th Cir. 2011). The court stated that MaxBounty agreed to Facebook's terms of use, which placed restrictions on Maxbounty's use of Facebook's website.

MaxBounty argued that because Facebook granted it access to the Facebook site, it could not have exceeded its "authorized access" within the meaning of the CFAA. However, the court noted that Facebook alleged that MaxBounty and its affiliates registered for Facebook accounts and accepted Facebook's terms of use, which places restrictions on their use of the Facebook site. In this light, the court found that Facebook's allegations were sufficient to state a claim under the CFAA.

This case is significant because it is one of the first cases to apply *Nosal's* holding that the violation of computer-use policies constitutes "exceeding authorized access" under the CFAA. As discussed in our prior blog, *Nosal* provides employers in the Ninth Circuit with a clear CFAA remedy against dishonest employees who exceed their authorized access of their employers' computer systems. *Facebook* fortifies that protection and encourages employers to take proactive steps with well written computer-use policies and procedures.

Ex-Employee Violated Duty Of Loyalty, Breached Non-Compete, And Committed Computer Fraud Act Violation, But New Employer Not Liable For Misappropriation Of Non-Trade Secret "Confidential Information"

September 11, 2011 by Paul Freehling

A dental products supply company, DHPI, won partial summary judgment from a Wisconsin federal court against its ex-employee, Ringo, for competing with DHPI both while still an employee and soon after resigning. The most interesting issues in the opinion, however, concern application of the Computer Fraud and Abuse Act to Ringo's copying of DHPI's computer hard drive, and DHPI's unsuccessful claim against Ringo's new employer for "misappropriation of confidential information." Additionally, Ringo's Illinois Wage Payment Act counterclaim failed because DHPI is a Wisconsin corporation with its principal place of business in that state. *Dental Health Products, Inc. v. Ringo*, Case No. 08-C-1039 (E.D.Wis., Aug. 24, 2011).

Ringo began working for DHPI in 2002 as a salesman and became Illinois branch manager in 2005. He was subject to a confidentiality and 90-day post-employment non-compete agreement. In 2007, while still employed by DHPI, Ringo began making sales through his own dental equipment sales company. He resigned from DHPI the following year and immediately went to work for his wife's competing company. Not surprisingly, the court held that Ringo breached his duty of loyalty to DHPI and his non-compete agreement.

Before leaving DHPI, Ringo made a copy of his employer's computer's hard drive. In response to DHPI's Computer Fraud and Abuse Act claim, he protested that he had permission to access the computer at the time he copied the hard drive. Further, he emphasized that he had not damaged the computer system, that he knew most of the information or could have developed it with little difficulty, and that he never viewed the copy. The court held that Ringo's authorization to access DHPI's computer ended when he decided to copy the hard drive and quit.

The CFAA has a $5,000 minimum damages provision. DHPI claimed as damages the $16,000 it paid to a computer forensic expert to determine the extent of Ringo's unauthorized conduct. The court concluded that DHPI's expenditure "was a reasonable reaction to the knowledge that one of its key salesmen had left the company in order to compete with it and had made a copy of a company hard drive before doing so."

Ringo counterclaimed under the Illinois Wage Payment and Collection Act for wrongful withholding of earned commissions, failure to compensate him for unused vacation time, and refusal to reimburse him

for health insurance premiums he paid while a DHPI manager. The court held, quoting a 1996 Northern District of Illinois decision, that the Act only applies "to a group of employers and employees, all of whom are in Illinois." Since DHPI was a Wisconsin corporation with its headquarters there, it was not liable.

Lastly, the court rejected DHPI's misappropriation claim. The company conceded that its customer lists and basic financial information did not constitute trade secrets but insisted that the information was confidential and deserving of protection. The court held that there is no statutory or common law basis for a misappropriation claim other than for trade secrets.

This case teaches that the CFAA prohibits an employee's illicit access to a company computer and permits reimbursement of expenditures incurred by the employer to determine the extent of its injury. Further, "misappropriation of confidential information" which is not a trade secret is not actionable. The *DHPI* decision adds to the body of authority limiting the geographic scope of the Illinois Wage Act. Finally, the opinion reminds us that blatant violations of the duty of loyalty and of a reasonable non-compete provision may be summarily punished.

New York Federal Court Dismisses Computer Fraud and Abuse Act Claims For Defendant's Alleged Use Of "Supercookies" And "History Sniffing"

September 4, 2011 by Robert Milligan and Joshua Salinas

A New York federal district court recently dismissed Computer Fraud and Abuse Act (CFAA) claims asserted against defendant advertising company Interclick and some of its advertising clients. Plaintiff consumer Sonal Bose alleged that the defendant advertising company's use of "supercookies" and "history sniffing" invaded her privacy, misappropriated her personal information, and interfered with her computer's operations. The court dismissed the CFAA claims because Bose failed to show the statutorily required damage or loss.

Bose alleged that Interclick used browser cookies to advertise for various companies online. Cookies are small files placed in a computer user's web browser to gather information about the user's online habits and behaviors. Cookies are helpful for users who want to autopopulate data, such as usernames or passwords, when they return to a website. These cookies are also extremely beneficial for marketing companies who can track a users online habits and behaviors. Thus, an advertising company such as Interclick can use this information to provide specifically tailored advertisements based on the user's profile. If a user does not want to be tracked or have this information available, he or she can always delete the cookies from the web browser.

The problem Bose alleged in this case was that Interclick used "supercookies" aka "flash cookies." These supercookies are not as delicious as they sound. When a user deletes his or her cookies, the supercookie "respawns" the deleted cookie without the user's notice or consent. As in this case, Interclick allegedly continued to track Bose and collect her information, despite her attempt to delete the cookies and protect her privacy. Bose also alleged that Interclick used "history sniffing," in which it allegedly looked at her computer's browsing history to tailor its advertisements toward her.

Bose claimed that she suffered: (1) impaired computer services and resources, (2) loss due to collection of personal information, and (3) loss due to interruption of internet service. The defendants moved to dismiss on grounds that Bose failed to allege a cognizable injury to meet the $5,000 threshold statutorily required for CFAA civil claims. (18 U.S.C. § 1030 (c)(4)(A)(I)).

First, the court recognized that physical damage is not necessary for CFAA claims. As we have discussed in previous blogs, courts are expanding the CFAA's definition of "losses" and have recognized computer forensic investigation costs and outside counsel fees as sufficient to meet the statutory threshold. However, the court here stated that Bose failed to quantify her damage and did not specifically show the impairment of her computer functions or any diminution of value.

Second, the court cited *Doubleclick* and stated that Bose's allegations for invasion of privacy, trespass, and misappropriation of confidential data are not cognizable economic losses. (*In re Doubleclick Inc. Privacy Litig*., 154 F. Supp. 2d 497, 524, n. 33 (S.D.N.Y 2001)). The court found Bose claims similar to the California case *La Court v. Specific Media*, Inc. No. SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), which also dismissed supercookie CFAA claims for failure to allege an economic injury. The court emphasized that "advertising on the internet is no different from advertising on television or in newspapers," as marketers and retailers constantly collect consumer personal data and demographic information. In other words, no harm, no foul.

Finally, the court found that Bose failed to allege any specific damage or loss regarding the interruption of her internet service. Bose did not show that the cookies damaged, shutdown, or even slowed her computer.

This case is significant because it demonstrates that courts still require some quantifiable or cognizable loss for CFAA civil claims, despite the growing trend to allow claims absent any damage or interruption of service. Courts will not accept CFAA civil allegations merely based on the invasion of privacy. Indeed, privacy has at least a $5,000 price tag under the statute.

The use of supercookies will continue to rouse privacy advocates. In fact, this summer the European Union issued its "Cookie Directive" to address cookie privacy concerns.

The court dismissed the CFAA claims, but kept the claims against Interclick for alleged deceptive business practices. While supercookies may not be unlawful under the CFAA, how a company uses these tracking devices may still subject them to liability.

This area of law continues to be white hot as the plaintiffs' bar tries to leverage privacy and other claims against companies who collect computer users' data as class actions for large settlements.

Outside Counsel Fees May Be a Qualified Loss to Meet the CFAA's $5000 Jurisdictional Requirement

May 15, 2011 by David Monachino

The Computer Fraud and Abuse Act ("CFAA") requires, among other things, that a plaintiff demonstrate a "loss" of $5,000 or more. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

In Animators at Law, Inc. v. Capital Legal Solutions, LLC, et al., Case No. 10-CV-1341 E.D.Va. (May 10, 2011) (unpublished) (TSE) two former employees of Animators' abruptly left to join a competitor. Shortly thereafter, Animators' president noticed that one of the former employee's laptop containing sales and other confidential information was missing. Thus, Animators initiated an investigation concerning whether defendants copied, deleted, or otherwise misused Animators' confidential information after leaving Animators' employment, including an (i) outside forensic analysis, (ii) internal investigation, and (ii) outside counsel investigation. Capital Legal disputed whether the outside forensic analysis constituted a qualified loss under the CFAA, because Animators did not "actually pay" cash for these services, as well as the propriety of the other two investigations.

The District Court first noted that "hindsight must not guide such an analysis of whether such actions were reasonably necessary in response to a CFAA violation … perpetrators of unauthorized access should foresee that their actions may result in significant investigations and costs far exceeding the actual damage to the system." The District Court then held that "the CFAA does not require losses to be paid for in cash. Indeed, a holding that CFAA losses must be reduced to a cash exchange would conflict with the principle that a CFAA plaintiff may recover damages for its own employees' time spent responding to CFAA violations." Finally, the District Court stated that it appears that well documented internal investigations and outside lawyer's fees also "appear to be" qualifying losses: "[w]hile defendants may contend that [the outside lawyer] is not the appropriate person to oversee the investigation and response to the intrusion, given his high hourly rate and legal, rather than technical expertise, even a reduction or outright elimination of [the outside lawyer] charges would still leave Animators with well over $5,000 in qualified losses."

Accordingly, apart from obtaining the return of their valuable data, the potential recovery of outside counsel fees under the CFAA, as well as computer forensic examiner fees, may provide a necessary element and a significant incentive to companies to pursue CFAA claims should their data be compromised by departing employees.

The Federal Computer Fraud and Abuse Act is Back in Play for Employer Suits Against Dishonest Employees in the Ninth Circuit

May 2, 2011 by Scott Schaefers and Robert Milligan

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.

In *U.S. v. Nosal* (9th Cir. No. 10-10038), the Ninth Circuit held 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).

The court rejected the argument that it was overruling its 2009 decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), which dismissed an employer's CFAA claim against an employee who had e-mailed confidential documents to his personal address when working for the employer, and used those files post-termination to compete with the employer. The Brekka panel said that so long as the employee was authorized to use the computer for any purpose and such authorization had not been completely rescinded, the employee could not be held liable under the CFAA for using files for unauthorized purposes.

In distinguishing *Brekka*, the *Nosal* panel held that the employer in *Brekka* did not place any restrictions on employees e-mailing themselves confidential files, and thus the employees could not be said to have exceeded any such computer-use restriction. The employer in *Nosal*, on the other hand, had password-protected computers, written computer-use agreements with its employees which restricted access to computers to employer business, and automatically placed restrictive legends on its confidential database printouts advising readers that the printouts were confidential and company property.

The employers' computer-use restrictions, the *Nosal* court held, were the key distinction from *Brekka*, and the touchstones for "exceeding authorized access" under the CFAA. The *Nosal* majority noted that it was siding with the First, Fifth, and Eleventh Circuits' decisions in prior cases which similarly upheld employer CFAA claims against dishonest employees for exceeding authorized access by stealing employer files.

The dissent in *Nosal* argued that the majority's decision goes too far, and potentially criminalizes otherwise innocuous employee use and access of his employer's computer. The definition of "exceeding authorized access" under the intent-to-defraud provision of the CFAA (i.e. Section 1030(a)(4)), the dissent said, was inconsistent with the statute's use of the same phrase in section 1030(a)(2), which made such access a crime whether or not the employee intended fraud. Any time the employee even technically violated an employer's restrictions, the employee could be indicted at the whim of the government.

With the *Nosal* decision, employers in the Ninth Circuit now have a clear CFAA remedy against dishonest employees who exceed their authorized access of their employers' computer systems. Employer computer-use restrictions determine whether an employee exceeds authorized access under the CFAA. Conversely, employees looking to avoid federal indictment or civil liability under federal law should strictly adhere to their employers' computer-use restrictions.

To avail themselves of the helpful *Nosal* decision, employers should ensure that they have written computer-use policies which prohibit improper computer use and activities. The policies should prohibit the use of company computers to copy, e-mail, or otherwise distribute company files to compete or help a third party compete with the employer. Computer access should be authorized for work activities only. Employers should also consider prohibitions on the distribution of company data to employees' non-work e-mail accounts and prohibitions or limitations on the use of electronic storage devices, such as external hard drives and data sticks. Employers should also audit employee computer use and access activity to ensure that employees are following company policies. Recurring training on acceptable computer usage is also critical. Employers should carefully circumscribe employee access to company prized data to only those employees who truly need to have access to such data to perform their jobs. Employers should also require employees to return all company data upon termination, as well as all company computers and other electronic devices.

The *Nosal* decision provides employers with a viable remedy to help address employee data theft but employers must be vigilant and ensure that they have crafted thoughtful computer-use policies to maximize their protections under the CFAA.

Private Information Stored On Electronic Devices Subject To Search By Law Enforcement If Arrested In California

March 16, 2011 by Robert Milligan and Joshua Salinas

Police officers are free to review private and confidential information stored on your cell phone if the search is incident to an arrest in California. The Supreme Court of California recently upheld the warrantless search of a cell phone text message folder in *People v. Diaz*, 51 Cal. 4th 84 (2011). The decision places no restraints on the type or amount of data police officers may access when searching an arrestee's cell phone.

Defendant Gregory Diaz allegedly purchased Ecstasy from a police informant. Police officers arrested Diaz, seized his cell phone from his pocket, and transported him to the sheriff's station. Ninety minutes later, a police officer searched Diaz's cell phone text message folder and found an incriminating message. The officer showed Diaz the message and Diaz admitted to the alleged sale of Ecstasy. Diaz later argued that the search of his phone's text messages folder constituted an unlawful warrantless search.

The Supreme Court of California found the cell phone search a valid search incident to lawful custodial arrest. The court compared the search to previous U.S. Supreme Court cases that allowed the search of a cigarette box (*United States v. Robinson*, 414 US 218 (1973) and clothing (*United States v. Edwards*, 415 US 800 (1974) found on the arrestee's person. The court rejected the argument that a warrantless search of property turns on the character of the property. The court found that the seizure and search was valid because of the reduced expectation of privacy resulting from the arrest. The court rejected the argument that cell phones' ability to store vast amounts of personal information warrants heightened privacy interests. The court also found that there was no legal basis for distinguishing the contents of an item found on the person from the item itself.

In the dissenting opinion, Justice Moreno criticized the majority's decision stating it "goes much further, apparently allowing police carte blanche, with no showing of exigency, to rummage at leisure through the wealth of personal and business information that can be carried on a mobile phone or handheld computer merely because the device was taken from an arrestee's person. The majority thus sanctions a highly intrusive and unjustified type of search, one meeting neither the warrant requirement nor the reasonableness requirement of the Fourth Amendment to the United States Constitution."

What does this case mean for those who carry smart phones or other electronic devices that store confidential or private information?

Trading Secrets

1. Confidential and private information contained on electronic devices can be seized by law enforcement if you are arrested. Technological advancements have shrunk the size of storage devices and simultaneously increased their accessibility and storage capacity. iPhones, Blackberries, and other smart phones have become intertwined with business and personal information, including social networking. Diaz's phone search involved text messages. However, this case arguably permits police officers to access confidential emails, documents, and voicemail messages that may contain private business or client information and personal information. Additionally, the character of the property seized is irrelevant. Thus, flash drives, digital cameras, and laptops found on the person may also be searched.

2. Password protecting a device may not be enough. If a device requires a password for access, an arrestee may decide to refuse to provide police officers with his or her password. However, nothing prevents officers from seizing the device and using forensic software to copy and analyze the data and circumvent any password protection.

3. *Diaz* may be headed to the U.S. Supreme Court. Unlike *Diaz*, a 2009 Ohio Supreme Court case found a warrantless search of an arrestee's cell phone unlawful. (*State v. Smith*, 920 N.E. 2d 949 (2009)). While the Court denied *Smith* cert., it may take up *Diaz* in light of the current state split and the scarce case law on cell phone searches.

4. Employers need to be cautious in determining what access to confidential and business information that they permit their employees to have in general, and specifically, through electronic storage devices, such as cell phones, laptops, thumb drives, etc., as sensitive data stored on such devices may be subject to search if the employee is later arrested.

Computer Fraud and Abuse Act Remains Viable Claim For Employers To Assert Against Employees Who Steal Company Data

March 2, 2011 by Robert Milligan and Joshua Salinas

The Computer Fraud and Abuse Act ("CFAA") remains a potent weapon for employers to use against disgruntled employees who steal company data. The Sixth Circuit in *U.S. v. Batti*, No. 09-2050, 2011 WL 111745 (6th Cir. 2011) recently upheld the criminal conviction of an employee who allegedly accessed, copied, and leaked confidential information that belonged to his employer's CEO. The court also awarded the employer restitution for private security investigation costs, despite parallel government investigations. Unfortunately, the court provided no clues into its position regarding the hotly contested "without authorization" interpretation that has split the circuits.

Luay Batti worked in the IT department of Campbell-Ewald, a Michigan advertising company. While employed, Batti allegedly obtained without authorization confidential information that belonged to Campbell-Ewald's CEO. Six months later, Batti met with Campbell-Ewald's General Manager to complain about the IT department's management. Batti also allegedly provided the General Manager a copy of the CEO's files to reveal the weaknesses in the company's computer security. Campbell-Ewald fired Batti and contacted the police.

The FBI conducted an investigation into the alleged security breach. Subsequently, Campbell-Ewald hired a security investigation firm and obtained legal advice from outside counsel regarding the alleged security breach.

Butti was convicted for violating the CFAA. The district court awarded Campbell-Ewald $47,565 in **restitution for the security firm's investigation and advice from counsel.**

One of the issues Batti raised on appeal was whether Campbell-Ewald could receive restitution when the government had already conducted an investigation.

The Sixth Circuit affirmed the lower court and ordered restitution. The court emphasized that courts are required to award restitution to reimburse necessary expenses incurred when victims investigate offenses. (18 U.S.C. § 3663A). The court echoed the growing majority of courts that private investigations are necessary responses to security breaches. Thus, Campbell-Ewald could recover for incurred investigation costs, regardless of whether the government already conducted an investigation. In fact, Campbell-Ewald's continued surveillance allegedly caught Batti attempting to access the company's computer server after his termination.

This holding is welcome news for employers and other victims of CFAA violations. The growing majority of courts permit the recovery of investigation costs in CFAA civil suits. As reflected in *Batti*, criminal proceedings brought by the government against rogue employees who steal company data may be viable options for employers (provided that they can secure the government's attention and support) and reduce the need for costly civil suits, particularly where they can receive restitution for their investigation costs.

Yet, the Sixth Circuit provided no insight into how it would rule regarding the current "without authorization" split. Batti did not raise the issue of authorization on appeal and thus the court was not required to discuss it. The facts of the case provided no opportunity for the court to delve into its interpretation of "without authorization." Batti's alleged purpose in providing the GM with a copy of the CEO's files was to show that someone without authorization could obtain this confidential information. On one side of the circuit split, some courts focus on whether the employee was initially authorized to access the stolen data. On the other side, the Seventh and Eleventh Circuits focus on the purpose and intent of the employee's conduct, which would terminate any previously granted access. Indeed, Batti apparently never had any authorization to access the CEO's files and thus his alleged conduct constituted "without authorization" under any circuit's interpretation.

While *Batti* provides no clear guidance on how it would side in the "without authorization" split, the Court reinforced the employers' ability to use the CFAA as a viable claim to combat computer security breaches by employees in certain situations.

District Court Holds That Computer Forensic Investigation Costs Satisfy "Loss" Requirement of Computer Fraud and Abuse Act

February 9, 2011 by Robert Milligan and Joshua Salinas

A Colorado federal district court recently held that the computer forensic investigator costs of investigating Computer Fraud and Abuse Act (CFAA) violations constitute "loss" under the statute. (*AssociationVoice, Inc. v. AtHomeNet,Inc.*,No. 10-cv-00109-CMA-MEH, 2011 WL 63508 (D.Colo 2011)). The court echoed the growing trend in circuit and district courts, which permit civil claims under the CFAA absent any damage or interruption of service. Consequently, this decision underscores the viability of asserting CFAA claims in cases involving data theft and the importance of utilizing qualified computer forensic investigators in such cases.

The plaintiff and defendants in *AssociationVoice* offered competing web-based software applications for homeowners associations (HOA). The defendants allegedly acted as fictitious HOA customers in order to purchase the plaintiff's software and access the plaintiff's password-protected "site admin" areas. In order to access the web site, the defendants also allegedly entered into a Services Agreement, which prohibited the defendants from reverse engineering and copying the plaintiff's source code or using the plaintiff's confidential and proprietary information.

The defendants allegedly copied, reverse engineered, and misappropriated information from the plaintiff's password-protected site and allegedly added at least forty-four new features to the defendants' own applications.

The plaintiff filed suit against the defendants, alleging, *inter alia*, violations of the CFAA, copyright infringement, trade secret misappropriation, and breach of the Services Agreement.

The plaintiff moved for two preliminary injunctions. The plaintiff sought to enjoin the defendants, per the Services Agreement, from providing the defendants' customers with the allegedly copied, reverse engineered, and misappropriated features. Additionally, the plaintiff sought to enjoin the defendants, pursuant to the CFAA, from further accessing the password-protected "site admin" areas.

The court denied the Services Agreement injunction because the plaintiff did not make a "strong showing" of the four injunction factors to justify altering the status quo. However, the court granted the CFAA injunction.

The noteworthy aspect of this case is the court's analysis of the "likelihood of success" factor in granting the plaintiff's CFAA injunction.

In order to bring a civil claim under the CFAA, the plaintiff was required to prove that the violations resulted in the loss of at least $5,000 within a one-year period. (18 U.S.C. § 1030(g) and (c)(4)(A)(i)). The parties disputed whether the plaintiff's hiring of a third-party computer forensic investigator to assist with its investigations constituted a "loss." Additionally, the defendants argued that the plaintiff could not bring a claim because it suffered no interruption of service.

The court recognized that the majority of courts find the costs of investigations and responses to security breaches constitute "loss," regardless of whether service is interrupted. (*See*, *e.g.*,*A.V. v. iParadigm*s, LLC, 562 F.3d 630, 646 (4th Cir. 2009);*EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 584 (1st Cir. 2001);*SuccessFactors, Inc. v. Softscape, Inc*., 544 F.Supp.2d 975, 980-81 (N.D.Cal. 2008); *Res. Ctr. for Indep. Living v. Ability Res., Inc*., 534 F.Supp.2d 1204, 2111 (D.Kan. 2008);*Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F.Supp.2d 1026, 1036 (N.D.Ill 2008); *NCMIC Fin. Corp. v. Artino*, 638 F.Supp.2d 1042, 1064 (S.D. Iowa 2009)).

The court reasoned that the plain language of "loss" defined in § 1030(e)(11) distinguishes between the costs of responding to CFAA violations *and* the consequential damages from interruptions of service. In fact, the legislative history of the CFAA indicates that it the statute was designed to address situations in which damage never occurred. The court found this case almost identical to the California district court decision in *SuccessFactors.* In *SuccessFactors*, the court held that when confidential information is obtained, it is necessary for the violated party to discover who has the confidential information, how they accessed it, and what the violators were doing with it. Thus, the defendants' alleged access of the plaintiff's protectable confidential information naturally incurred the costs of an investigation. Specifically, the court stated "[i]t, therefore, is not surprising that Plaintiff also had to go to great lengths to uncover Defendants' identity, as well as to uncover the extent of their unauthorized access and the methods they used. Accordingly, Defendants should not be allowed to complain about the costs Plaintiff incurred in doing so."

While the court in *AssociationVoice* followed the growing majority, the Second Circuit and district courts in Florida, Virginia, Connecticut, and Louisiana still require an interruption of service in order to bring a claim under the CFAA. (*See, e.g., Nexans Wires S.S. v. Sark-USA, Inc*., 166 Fed.Appx. 559, 563 (2d Cir. 2006)).

What does this mean? The CFAA remains a viable option to combat data theft. Although some courts have narrowed the applicability of the CFAA, many courts, like the *AssociationVoice* court, recognize CFAA claims even where the defendants' actions do not result in any interruptions of service. Some courts have even extended the "costs to respond" to include investigations into ways to improve security. (*See, e. g., JedsonEng'g, Inc., v Spirit Construction Services, Inc*., (S.D. Ohio 2010). Accordingly, in order to satisfy the "loss" requirement under the CFAA, make sure that qualified computer forensic investigators are utilized (in coordination with legal counsel) to respond to and assess the computer breach as soon as your company learns of the data theft.

Trading Secrets

The Eleventh Circuit Splits with the Ninth Circuit in Interpreting the Computer Fraud and Abuse Act

January 7, 2011 by Paul Freehling and Scott Schaefers

The Eleventh Circuit Court of Appeals' December 27, 2010 decision in *U.S. v. Rodriguez*, Appeal No. 09-15265, — F.3d —, 2010 WL 5253231 (11th Cir. Dec. 27, 2010) may mark a significant split among the federal appellate circuits over the meaning of the phrases "without authorization" and "exceeds authorized access" under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. ("CFAA"). On one side of the fence sit decisions which reject such suits due to the employer's prior grant of access, regardless of the employee's purpose of access or subsequent use of the files. On the other side are decisions which allow CFAA claims where the employee's purpose for accessing the files was unauthorized, even if the access itself was permitted.

In *Rodriguez*, the court upheld the criminal CFAA conviction of defendant Roberto Rodriguez, a former Social Security Administration ("SSA") telephone service representative, because he accessed confidential and sensitive files for "a non-business reason." The SSA had previously established a policy prohibiting employee access of confidential databases "without a business reason," of which Rodriguez was made aware several times. Despite these clear warnings from his employer, Rodriguez accessed more than 100 times confidential, personal information from Social Security files concerning women with whom he had a romantic relationship. Even though Rodriguez's access of the database itself was authorized, the purpose of the access was not, thus triggering the "without authorization" or "exceeds authorized access" provisions of the CFAA.

The Eleventh Circuit thus aligned itself with the Seventh Circuit, which in *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), held that an employee violates the CFAA where he already has decided to quit, and thereafter accesses company files for unauthorized purposes in furtherance of his "breach of duty of loyalty" to the company (i.e. to erase valuable company data). That is, when an employee accesses computer files with a purpose to injure his employer, his access is necessarily unauthorized because by law because he never had permission to work against the company.

On the other side of the split is the Ninth Circuit's September 2009 decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). There, the court dismissed the CFAA suit against the former employee for subsequent misuse of company files because the purpose and misuse of the employee's access was irrelevant, so long as the access itself for was permitted, for any purpose. According to *Brekka*, reading a purpose-related qualification into the CFAA terms "without authorization" and "exceeds authorized access" would run counter to the plain meaning of those statutory requirements. In fact, *Brekka* explicitly rejected *Citrin*'s suggested interpretation along those lines.

Rodriguez did not explicitly reject *Brekka*. *Rodriguez* instead distinguished *Brekka* because in *Brekka* there was no express prohibition against the employee's accessing files and e-mailing them to his home address, whereas in *Rodriguez*, a prohibition against non-business-related access was in place. Nevertheless, *Rodriguez* implicitly rejected *Brekka*, because *Brekka* limited CFAA claims to those instances in which an employee had not received permission to access a computer for "any purpose," or where the permission had been previously rescinded and the employee accessed the computer anyway. Rodriguez had permission to access the SSA database, albeit for a limited purpose, so his conviction likely would have been overturned by the Ninth Circuit, not upheld as the Eleventh Circuit did. Also, because of the unique circumstances in *Rodriguez*, there is a possibility that it could be distinguished on its facts alone.

In any event, the lessons to be learned by corporate counsel and management from this conflict are not limited to whether an employer can sue an employee for violating the CFAA. These decisions serve as reminders to management that they must carefully and vigilantly create and enforce employee computer-use policies, including the following:

- Write clear computer-access policies, disseminate those policies among employees, and periodically remind employees of their obligations;
- Require employees, whether professional, clerical, or otherwise, to sign non-disclosure and computer confidentiality agreements, where access to computers is strictly limited to furthering company business; and
- Develop a limited-permission structure so that employees are provided access only to those files needed to do their job.

You may contact Seyfarth Shaw's Trade Secret Protection attorneys for further ideas and discussion of issues related to employee misuse or theft of company intellectual property.

Non-Compete & Restrictive Covenants

Oklahoma Supreme Court Nixes Overly Broad Non-Compete Agreement

December 30, 2011 by Rebecca Woods

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. The *Howard* ruling is consistent with prior rulings by the court that evidence a hostility to the U.S. Supreme Court's broad interpretation of the Federal Arbitration Act ("FAA"). The court also found the non-compete agreement at issue was in such serious violation of Oklahoma's statutory limitations on non-compete agreements, *see* Title 15 O.S. 2001 § 219A, that it refused to blue pencil the agreement and struck it in its entirety.

An employer, Nitro-Lift Technologies, LLC ("Nitro-Lift") sought to enforce against two former employees non-compete agreements that prohibited the former employees from, in relevant part, (1) owning, managing, operating, joining, controlling, participating, being connected with (as an officer, director, employee, consultant, etc.), loaning money to, or selling or leasing equipment to any business or person engaged in the nitrogen generation business in the oil and gas industry in the U.S; (2) canvassing, soliciting, approaching, or enticing away any past or present Nitro-Lift customers or suppliers; and (3) engaging, employing, soliciting, inducing, or attempting to influence any Nitro-Lift officer or employee to terminate their employment. This non-compete was to apply for a period of two years post employment. After Nitro-Lift served the employees with a demand for arbitration for allegedly violating the non-compete, the employees filed a motion for declaratory judgment, seeking a determination that the non-competes were null and void. The trial court held that the arbitration agreement was valid and enforceable and dismissed the employees' complaint. On appeal, the Oklahoma Supreme Court reversed the dismissal and held that the employees were entitled to permanent relief.

The *Howard* ruling rebukes the U.S. Supreme Court's broad application of the FAA and concludes that state courts should determine, in the first instance, whether a contract is valid and enforceable, even if the validity of the arbitration clause is not at issue. Combined with the court's prior rulings, and with the court's unwillingness to blue pencil the contract, the *Howard* ruling also indicates an apparent hostility by the court to arbitration clauses in employment contracts.

The *Howard* court quickly dispatched U.S. Supreme court precedent by invoking its own ruling in *Bruner v. Timberlane Manor Ltd. Partnership*, 2006 OK 90, 155 P.3d 16, which contained an

"exhaustive review" of U.S. Supreme Court decisions that "were found not to inhibit our review of the underlying contract's validity." Without analysis, the *Howard* court then broadly declared that "the existence of an arbitration agreement in an employment contract does not prohibit judicial review of the underlying agreement." At issue in the *Bruner* decision was whether a nursing home agreement, which required arbitration of all disputes, was enforceable when Oklahoma law had an anti-arbitration statute with respect to claims against nursing homes. The *Bruner* court concluded that the nursing home contract did not involve interstate commerce and thus, Oklahoma's anti-arbitration statute for nursing home contracts was not preempted by the FAA. The *Howard* court engaged in no analysis of interstate commerce. If it had, it would have been difficult to conclude that interstate commerce was not involved, as the multi-state employer at issue also sought to enforce the non-compete across state lines. Nor was there any issue in the *Howard* case of a direct conflict between state law and the FAA. The issue in *Howard* was simply whether a non-compete was enforceable under Oklahoma law and whether that determination should be made by a court or an arbitrator. The *Howard* decision makes clear that, in Oklahoma, the enforceability of a contractual provision is for courts, not arbitrators.

This ruling is directly at odds with the U.S. Supreme Court's rulings with respect to the broad application of the FAA. For example, in *Buckeye Check Cashing, Inc. v. Cardenga*, 546 U.S. 440 (2006), the Supreme Court held that a challenge to a check-cashing contract as illegal under various Florida lending and consumer protection laws was improper, and that such challenges, even as to void contracts, should be heard in the first instance by an arbitrator. *Id*. at 5 ("[U]nless the challenge is to the arbitration clause itself, the issue of the contract's validity is considered by the arbitrator in the first instance.") The Supreme Court rejected the Florida Supreme Court's conclusion that "enforceability of the arbitration agreement should turn on 'Florida public policy and contract law.'" *Id*. at 6 (citation omitted). It is difficult to see a ready, and material, distinction between the *Cardenga* ruling and the *Howard* facts: in *Howard*, there was no contest as to the arbitration clause itself, and the employer was merely seeking to enforce a statutorily impermissible (as opposed to illegal) contract.

With respect to the non-compete agreement, it was plainly at odds with Oklahoma law. Oklahoma law provides, in relevant part, that employees "shall be permitted to engage in the same business as that conducted by the former employer or in a similar business as that conducted by the former employer as long as that former employee does not directly solicit the sale of goods [or] services . . . from the established customers of the former employer." 20 Title O.S. 2001 § 219A. Any provision at odds with this section "shall be void and unenforceable." The court concluded that Oklahoma allows an employer to bar a former employee from soliciting goods or services from the employer's established customers only. The court then readily found all three prongs of Nitro-Lift's non-compete agreement to be in violation of the statute. The court then declined to modify the agreement, characterizing the agreement as "offensive" and concluding that revising the agreement to comply with Oklahoma law would require the court to "decimate its provisions."

Lessons for employers with contracts to which Oklahoma law applies? (1) Do not rely upon an arbitration clause to avoid litigation of any non-compete agreement; and (2) limit the agreement to the statutory limitations or it may be voided in its entirety.

Montana Supreme Court Holds That Employer May Not Enforce Non-Compete Agreement Where Employee Was Terminated Without Cause

December 22, 2011 by Paul Freehling

As a result of a recent ruling by the Montana Supreme Court in a case of first impression in that state, an employer there — as in several other states — ordinarily 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. Significantly, the ruling might be different if the employee misappropriated trade secrets.

Wrigg, a CPA, started working for JCCS in Helena as a staff accountant in 1987 and was promoted to shareholder in 2003. She signed a series of two-year employment agreements each of which contained a provision which had the effect of imposing a monetary penalty if, during the 12 months after termination "for any reason," she rendered certain professional services to a competitor of JCCS. In May 2009, JCCS informed Wrigg that the agreement which would be expiring June 30, 2009 would not be renewed. After she left JCCS, she was hired by another accounting firm but for significantly less compensation because, allegedly, of that firm's concerns about the JCCS covenant. She filed a declaratory judgment suit against JCCS, seeking to invalidate the non-compete. JCCS counterclaimed based on the penalty clause and prevailed at trial, but the Montana Supreme Court reversed in all respects. *Wrigg v. Junkermier, Clark, Campanella, Stevens, P.C.*, Case No. DA 11-0147, 2011 MT 290 (Nov. 22, 2011).

In its unsuccessful effort to persuade the Supreme Court to affirm, JCCS cited *Dobbins, Deguire & Tucker, P.C. v. Rutherford, MacDonald & Olson,* 218 Mont. 392, 394-97, 708 P.2d 577, 578-80 (1985), a decision also involving an accountant. In *Dobbins*, that court reversed and remanded a lower tribunal's holding that a non-compete covenant virtually identical to the one in *Wrigg* was unenforceable. But JCCS' reliance on *Dobbins* was misplaced, according to Montana's highest court in *Wrigg*, because the trial court in *Dobbins* did not address the issue of whether the "covenant served a legitimate business interest." In both cases, the high court stressed that "Montana law strongly disfavors covenants not to compete" but added that it may be enforceable if it does not impose an unreasonable burden on the parties and the public. So, according to *Wrigg*, all that the *Dobbins* Court meant was that the trial court needed "to make factual findings as to the covenant's reasonableness."

In *Wrigg*, by contrast, the Supreme Court said that because JCCS was responsible for Wrigg's termination, it could not show that its "legitimate business interest" would be furthered by enforcement of the non-compete (according to Wrigg's appellate brief, the accountants in *Dobbins* left their employment voluntarily). Therefore, under the circumstances in *Wrigg* (involuntary termination) but not

necessarily in *Dobbins* (voluntary), penalizing an accountant for pursuing her livelihood during the 12 months after her employment ended apparently was considered to be an unwarranted punishment. JCCS' contention that Wrigg repeatedly had consented to the non-compete provision as written — "termination for any reason" — did not carry the day.

The Montana Supreme Court asserted in *Wrigg* that the applicable legal principle where an employee is terminated without cause is that "courts should scrutinize highly a covenant's enforcement given the involuntary nature of the departure." Intense scrutiny is required because the employer could have prevented harmful competition "simply by maintaining the employment relationship." Further, "An employer's decision to end the employment relationship reveals the employer's belief that the employee is incapable of generating profits for the employer. It would be disingenuous for an employer to claim that an employee was worthless to the business and simultaneously claim that the employee constituted an existential competitive threat." The court said that its ruling is supported by decisions from Iowa, New York, Pennsylvania, Tennessee, and the Seventh Circuit Court of Appeals (interpreting Illinois law).

Employers be aware: A non-compete provision in an agreement with an employee who is discharged without cause and who does not misappropriate trade secrets may be unenforceable.

Can The Seller Of A Business Who Also Becomes Employed By Purchaser Be Held To Non-Compete Agreement Under California Law? The Idaho Supreme Court Says Yes

December 14, 2011 by Molly Joyce

The Idaho Supreme Court, in the case of *T.J.T., Inc. v. Mori*, 2011 WL 5966870, No. 37805 (Id. Nov. 30, 2011), recently found that a two-year non-compete agreement executed in connection with the sale of a business was enforceable under California law, despite the fact that the seller also became an employee of the purchasing company as a result of the sale. The Idaho high court also remanded the case for consideration of whether the non-compete agreement's overbroad geographic restriction could be "blue-penciled" to comply with California law.

The case arose out of a 1997 non-compete agreement between plaintiff, T.J.T., and defendant, Mori, executed in connection with the sale of Mori's tire and axel recycling business, Leg-It Tire Company, Inc., based in California. The agreement prohibited Mori from operating anywhere within 1,000 miles of any facility owned or operated by T.J.T. or Leg-It for two years following the termination of his employment with T.J.T. Although Mori became an employee of T.J.T. as part of the deal, his employment was governed by a separate employment agreement.

Mori worked for T.J.T. until February 7, 2007. Within weeks of his resignation, Mori began work with a competitor of T.J.T. In June 2007, T.J.T. filed a complaint seeking injunctive relief and a constructive trust based on several claims, including breach of fiduciary duty and breach of contract. The district court denied T.J.T.'s request for injunctive relief and ultimately granted Mori's motion for summary judgment, finding that the agreement was void under California law. The district court concluded that the agreement was tied to Mori's employment instead of the sale of his business, and that the durational and geographical scopes of the agreement were too broad.

The Idaho Supreme Court reversed and remanded the district court's opinion. First, the court held that the non-compete provision was indeed enforceable. The court recognized that, as a general proposition, California has a strong public policy against non-compete agreements. An exception, however, to this prohibition is in the case of the sale of the goodwill of a business, citing California Business and Professions Code § 16601, the purpose of which "is to permit the purchaser of a business to protect himself or itself against competition from the seller which competition would have the effect of reducing the value of the property right that was acquired." Citing *Monogram Industries, Inc. v. SAR Industries, Inc*., 64 Cal. App. 3d 692, 701, 134 Cal. Rptr 714, 720 (Ct. App. 1976).

Mori argued that the non-compete provision was clearly tied to his employment with T.J.T., and therefore unenforceable. The Idaho Supreme Court disagreed, noting that "California courts have held that a non-competition agreement can be incidentally linked to the seller's employment agreement with the buying business without offending section 16600 [which prohibits non-compete agreements generally]." Even though Mori's non-compete agreement referred to Mori's employment with T.J.T. to determine its duration and enforceability, the court found that such an "incidental" link does not necessarily mean the provision is unenforceable. Instead, the court reasoned that Mori's employment only came about as part of the larger transaction — the sale of the business to a competitor — and was therefore enforceable.

The Idaho Supreme Court also found that non-compete provision's duration, which was to last for a period "ending two (2) years following Seller's termination of employment with the Company for any reason," was not unreasonable. Mori argued that the non-compete was not enforceable beyond six years (his term of employment, which was four years, plus two years). Yet, the court found that because the language of the non-compete agreement was not tied to the employment agreement, it existed independently of the employment agreement and operated pursuant to its own plain terms. Again relying on the language of California Business and Professions Code §16601, which provides that a seller may agree to refrain from competing *so long as* the buyer carries on a like business, the court found that the agreement was not unreasonable because T.J.T. continued to operate in the same line of business that Mori's former business (Leg-It) did at the time of the alleged breach.

Finally, the Supreme Court remanded the case to the district court for consideration of whether geographical component of the non-compete, which prohibited Mori from working anywhere within 1,000 miles of any facility owned or operated by T.J.T. could be judicially narrowed, or "blue-penciled," to comply with California law. The court recognized that the geographical restriction was indeed overbroad under California law as written, but queried whether the provision could be narrowed. The court reasoned that courts construing California agreements have the authority to narrow otherwise enforceable provisions pursuant to the portion of Section 16600 of the California Business and Professions Code that provides that "[e]xcept as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind *is to that extent void*." The agreement at issue also contained a "Reformation" clause, giving courts the power to reform the agreement to the extent necessary to be enforceable. The court was careful to note that while California courts refuse to modify the agreements before them, they do have a continuing ability to narrow the scope of an otherwise valid agreement.

The *T.J.T.* court concluded that the key factor in determining a covenant's proper geographic scope is the determination of what area is necessary to protect the goodwill of the sold business from competition by the seller. The Idaho Supreme Court refused to narrow the agreement, finding that the parties demonstrated a genuine issue of material fact as to the scope of Leg-It's business. It

nonetheless remanded the case to the district court to determine the question of fact and whether the agreement could be narrowed within a scope that was reasonably necessary to protect the goodwill of the sold business.

Although this case involves an Idaho court construing California law, *T.J.T.* serves as a reminder that one should not automatically assume that a California non-compete agreement with certain employees (particularly those selling their interest in a business) is always unenforceable – even if the party seeking to enforce the agreement is the employer or former employer of the defendant. Likewise, just because a California non-compete agreement contains an overbroad restriction, that might not render the entire non-compete agreement unenforceable if it can be narrowed in scope by the court.

Illinois Supreme Court Affirms Legitimate Business Interest Test For Restrictive Covenants And Provides Some Guidance On How To Analyze A Legitimate Business Interest

December 1, 2011 by Scott Humphrey

Illinois courts have traditionally followed the three pronged rule of reasonableness test when determining whether to enforce a restrictive covenant:

a. is the restriction no greater than what is required to protect the legitimate business interest of the employer;

b. does the restriction impose undue hardship on the employee;

c. is the restriction injurious to the public.

However, on September 23, 2009, the Illinois Fourth District Appellate Court, in *Sunbelt Rentals, Inc. v. Ehlers*, 394 Ill.App.3d 421, held that a court need not consider the first prong of the rule of reasonableness test, an employer's legitimate business interest, when determining whether to enforce a restrictive covenant. We previously blogged on this decision. The *Sunbelt* decision has been widely criticized since its publication and Illinois' four other Appellate districts have declined to follow it.

Today, the Illinois Supreme Court effectively reversed, and ended all further discussion on *Sunbelt* in *Reliable Fire Equipment Co., v. Arredondo*, 2011 IL 111871 (December 1, 2011). While writing that it "emphatically disagreed" with the *Sunbelt* decision, the Illinois Supreme Court scolded the Fourth District Appellate Court for "overlooking or misapprehending" Illinois Supreme Court precedent that calls for a court to consider all three prongs of the rule of reasonableness test, including an employer's legitimate business interest, when determining whether to enforce a restrictive covenant.

The *Reliable Fire* decision also resolves another dispute that has been raging in the Illinois Appellate Courts for sometime; what is the proper test for assessing whether an employer has a business interest worthy of restrictive covenant enforcement/protection. Some Illinois Appellate courts have ruled that only "trade secrets" and "near permanent customer relationships" establish a legitimate business interest. Other Illinois Appellate courts have taken a more flexible approach, and look at the following seven factors when assessing whether an employer has a legitimate business interest:

1) the number of years required to develop the customer;

2) the amount of money invested to acquire customers;

3) the degree of difficulty in acquiring customers;

4) the extent of personal customer contact by the employer;

5) the extent of the employer's knowledge of its customers;

6) the duration of customer association with the employer; and

7) the intent to retain employer-customer relations.

In *Reliable Fire*, the Illinois Supreme Court sides with the more flexible approach. Specifically, the Illinois Supreme Court informs its lower courts that *only* considering whether an employer has trade secrets and/or near permanent customer relationships is insufficient when assessing a legitimate business interest. Rather, Illinois Courts are to consider "the totality of the facts and circumstances of the individual case" when assessing whether a "legitimate business interest exists." The "totality of the facts and circumstances" can include, but is not limited to, an evaluation of near permanent customer relationships, the former employee's access to confidential information, the seven factors identified above, and/or anything else found in the common law. Moreover, the *Reliable Fire* decision declines to place any weight on the possible "facts and circumstances" that could create a legitimate business interest because "the same identical contract and restraints may be reasonable and valid under one set of circumstances, and unreasonable and invalid under another set of circumstances."

Thus, *Reliable Fire* appears to expand what an employer can state/argue is a legitimate business interest, and gives the trial court significant discretion when deciding what factors establish a legitimate business interest and whether to enforce a restrictive covenant. We will continue to monitor Illinois courts to see if the *Reliable Fire* holding leads to any changes in how trial courts assess and enforce restrictive covenants.

Virginia Employers Should Update Their Non-Compete Agreements In Light of New Virginia Supreme Court Ruling

November 22, 2011 by Guest Author for TradeSecretsLaw.com

As previously reported on this blog, the Virginia Supreme Court recently issued an important new non-compete decision which impacts the enforceability of non-compete agreements in Virginia and serves as a reminder that employers may want to review their agreements with employees and update them as appropriate. Here is a Seyfarth One Minute Memo on this important new case.

Virginia Supreme Court Clarifies Obligations Of Employer Seeking To Enforce Non-Compete

November 14, 2011 by Marcus Mintz

Earlier this month, the Virginia Supreme Court issued an opinion in which it clarified the burdens an employer must meet to enforce a non-compete against a former employee. Specifically, that the employer must 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. *Home Paramount Pest Control Cos., Inc. v. Shaffer*, No. 101837, 2011 WL 5248212 (Va. Nov. 4, 2011). In doing so, the Virginia Supreme Court overruled a 1989 opinion in which it upheld the exact same non-compete brought by the plaintiff's predecessor-in-interest. *See Paramount Termite Control Co. v. Rector*, 238 Va. 171, 380 S.E.2d 922 (1989). While a dissenting justice took issue with the court's departure from its prior decision and the effect it may have on parties looking to rely on established precedent, the majority held that its 1989 opinion was effectively eroded over time and its current holding reflected the current state of the law.

The case itself focused on the "function," or activity, restrictions within the non-compete which the plaintiff, Home Paramount Pest Control Companies, Inc. ("Pest Control"), sought to enforce against its former employee, Justin Shaffer ("Shaffer"). Pest Control claimed that Shaffer's new employment with a direct competitor violated his non-compete. The specific language at issue prohibited Shaffer from "engage[ing] directly or indirectly or concern himself/herself in any manner whatsoever in the carrying on or conducting the business of exterminating, pest control, termite control and/or fumigation services as an owner, agent … stockholder" for two years in any area in which the employee worked on behalf of Pest Control. However, the case never went to the merits because the circuit court held that the activity restriction of the non-compete was overbroad on its face and consequently, was unenforceable.

Upon appeal, the Virginia Supreme Court affirmed the circuit court and held that the function restriction was facially over-broad because it could prevent Shaffer from performing ***any*** duties at a competitor, irrespective of whether such duties were similar to the duties Shaffer held at Pest Control or would have any effect on Pest Control's legitimate business interests. For example, the court noted that on its face, the non-compete prohibits Shaffer from owning stock in a publicly-traded company which owned a pest control business and Pest Control was not found to have a legitimate business purpose "in such a sweeping prohibition." After comparing the instant restrictions to non-competes which were upheld in several recent cases, the court affirmed the circuit court's ruling that Pest Control failed to prove that its chosen language furthered its legitimate business interests and did not unduly burden Shaffer's right to earn a living.

Ultimately, employers seeking to enforce a non-compete under Virginia law (as well as many other jurisdictions) must take care to utilize language which narrowly tailors the activity restrictions of a non-compete to actual services and/or activities which actually or potentially compete with the former employer and threaten its legitimate business interests.

Because Arizona's "Fundamental Policy" Regarding Non-Compete Clauses Is So Different From That Of The State Of Washington, Arizona Federal Court Refuses To Enforce Clause's Provision Calling For Applicability Of Washington State Law

November 12, 2011 by Paul Freehling

Courts around the country are split as to the circumstances under which the parties' choice of law set forth in a non-compete agreement will be honored. In a recent diversity jurisdiction case ruling, Arizona U.S. District Court Judge David Campbell recently refused to enjoin violations of a non-compete clause which said that the law of Washington State applied. He held that Arizona had a greater interest than Washington in the case before him, and that Arizona's "fundamental policy" (a) requires courts in that state to be less tolerant than courts in Washington with regard to enforcing broad non-compete clauses, and (b) prohibits Arizona jurists (unlike their Washington counterparts) from using a "blue pencil" to make such clauses reasonable. He concluded that an Arizona court would be unwilling to enforce the parties' agreement in the circumstances here. *Pathway Med. Technologies, Inc. v. Nelson*, Case No. CV11-0857 PHX DGC (D.Ariz., Sept. 30, 2011).

For two years, Nelson was a sales representative in Arizona for Pathway, a developer, manufacturer and seller of medical devices for the treatment of arterial disease. While employed, he signed a confidentiality agreement in which he promised that for one year after his employment ceased, he would not "divert or take away," or "attempt or assist" anyone else in diverting or taking away, any Pathway customer. The agreement recited that it is governed by Washington law.

Following his resignation from Pathway, he was hired by a direct competitor and allegedly engaged in the prohibited conduct for the benefit of the competitor and the detriment of Pathway. Pathway sued Nelson and the competitor, and moved for temporary and preliminary injunctive relief. Judge Campbell denied both motions.

Arizona courts determine the enforceability of a choice of law provision in a non-compete clause by applying Sections 177 and 188 of the Restatement (Second) of Conflicts of Laws. According to the court's reading of those sections, the parties' choice will be honored only if they "could have agreed in their contract to the same provisions that the chosen law would impose, and could have done so under the law of the state with the most significant contacts with the transaction." Washington law differs from that of Arizona in the two respects described above. First, Arizona "requires that non-compete provisions be narrowly drafted and no greater than necessary to protect the employer's legitimate interests," whereas Washington enforces agreements "even if they are quite broad and last for long

periods of time." Second, in contrast to the law of Washington, Arizona "courts may not rewrite non-compete agreements to make them reasonable."

The contract was negotiated and signed in Arizona, the state where Nelson lived and where he performed his duties both for Pathway and for its competitor. The court held that application of Washington law in this case would be contrary to the "fundamental policy" of Arizona law. The non-compete clause here had no express geographical limitations. Further, it applied to all Pathway customers including those with whom Nelson never had had contact. Finally, the phrases "divert or take away any customer," and "attempt or assist" such diversion or taking away, were deemed to be unduly vague.

Employers who want to enforce non-compete agreements containing a choice of law provision must take care to select operative language that meets legal requirements not only of the chosen state but also those of the likely forum state if its law is different.

A Pennsylvania District Court Finds That A Non-Compete Agreement Is Not Subject To Automatic Stay in Bankruptcy

November 8, 2011 by David Monachino

Once triggered by a debtor's bankruptcy petition, the automatic stay suspends a parties' right to commence or continue an action against property of the debtor's estate. In general, a party can seek relief from the automatic stay for a variety of reasons, including for cause, lack of adequate protection or that the debtor has no equity in the property and the property is not necessary for reorganization. In a case of first impression, a district court in Pennsylvania has found that an injunction enforcing a non-compete provision in a franchise agreement was not a "claim" against the bankruptcy estate, under 11 U.S.C.S. § 101(12), since the injunction was a form of equitable relief for which an award of damages was not a viable alternative, and, thus, the injunction was not subject to the automatic stay.

In *In Re Stone Resources, Inc.,* __ B.R. __, 2011 U.S. Dist. LEXIS 4017925 (E.D. Pa. Bankr. September 11, 2011) (unpublished) the debtor entered into a franchise agreement in 2000 which allowed it to use the franchiser's trademarks and proprietary processes in its stone restoration and maintenance business. The agreement contained a covenant that prohibited the debtor from competing with the franchiser or its affiliates for two years after the agreement ended, and the franchiser sued the debtor in federal district court in May 2010, seeking an order enforcing that covenant. The U.S. District Court for the Eastern District of Pennsylvania issued a preliminary injunction in December 2010, which required the debtor to cease its business operations and turn over assets to the franchiser.

The franchisee declared Chapter 11 bankruptcy in February 2011, and the franchiser asked the bankruptcy court to dismiss the debtor's bankruptcy case pursuant to 11 U.S.C.S. § 1112(b) or, in the alternative, to grant the franchiser relief from the automatic stay under 11 U.S.C.S. § 362(d) (1) so it could enforce the preliminary injunction. The bankruptcy court denied the franchiser's motion holding that there was no evidence that the debtor declared bankruptcy in bad faith, and lifting the stay so the franchiser could enforce the district court's injunction would have made it impossible for the debtor to reorganize its business and pay its creditors.

The franchisor then appealed to the District Court. The District Court held that the bankruptcy court abused its discretion in denying franchisor's motion for stay relief in order to enforce preliminary injunction ordering a debtor to, inter alia, cease and desist in the operation of a business in accordance with the terms of a covenant not to compete. The District Court found that where the only remedy available for a cause of action is an equitable remedy that claim is not dischargeable in bankruptcy and not subject to the automatic stay.

Massachusetts Legislature Hears Testimony on Non-Compete Bill

November 1, 2011 by Kate Perrelli, Erik Weibust, and Ryan Malloy

On September 15, 2011, the Massachusetts legislature's Joint Committee on Labor and Workforce Development heard testimony on House Bill 2293. The bill, originally introduced in 2009 as House Bill 1799, and as previously blogged on here, here, and here, aims to codify Massachusetts 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 to the Previous Draft

The revised bill was re-filed in January 2011. 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. Additionally, it permits garden leave clauses of up to 2 years if the affected employee receives adequate compensation (the 1-year limit to non-compete agreement duration otherwise remains).

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.

Like its predecessor, Bill 2293 does not apply retroactively, nor does it affect non-solicitation, non-disclosure, or other non-employment related non-compete agreements, such as those in the context of the sale of a business. The bill continues to reject the inevitable disclosure doctrine, and provides that non-compete agreements must be in writing and signed by both parties.

The Legislative Hearing

Nearly 15 affected individuals, ranging from hairdressers and parents of college-age children to attorneys and legislators, testified before the Committee last Thursday. Although most testified in favor of the bill, some voiced concerns about mandatory attorneys' fee awards and the perceived threat of an upswing in costly litigation. For instance, a representative of the Smaller Business Association of New England (SBANE) insisted that small business owners, who must now pay to comply with the Wage Act and mandatory employee healthcare legislation would suffer an added financial hardship if this bill is

passed and opined that the bill would permit judges to ignore contract terms and create an atmosphere of unpredictability surrounding non-compete agreement validity.

Other critics expressed concern about the bill, and in particular three specific issues: 1) the unclear definition of "fair and reasonable consideration"; 2) the presumption that a 6-month non-compete agreement is sufficient to protect employer interests; and 3) the court's ability to deny enforcement of otherwise valid contractual obligations. There was a shared belief by some that the present state of the common law provides adequate coverage and that statutory modification of the law would adversely affect local industries, particularly in the current economic climate.

Others praised the bill's efforts to reform a complex and unpredictable realm of common law. The Massachusetts Employment Lawyers Association (MELA), an employee-rights organization, asserted that non-compete reform is necessary because abusive practices are pervasive and employees are being exploited under the current law. Other concerns expressed about the status quo include that unlimited non-competes create a chilling effect on hiring. Of course, the common law does not generally permit unlimited non-competes, but rather only those that are reasonably limited in time and geographic scope. Likewise, Secretary of Housing and Economic Development Greg Bialeck voiced the Patrick administration's view that reform is necessary and that now is the time to do so.

The drafters of the bill insist that it is not intended to alter the substance of existing common law. Instead, the point of the statute is purportedly to add consistency and procedural protections for the benefit of employers and employees alike. In the drafters' view, it will be easy for employers to avoid the mandatory payment of legal fees, for example, if they comply with the bill's safe harbors.

As evidenced by the testimony of both the bill's drafters and constituents, several important issues remain outstanding in Massachusetts, particularly in the areas of attorneys' fees and the court's equitable power. Compromise will be necessary on many of these points. It may be some time before the dust settles and a final draft is presented to the legislature, but efforts to create a statutory scheme to guide the use and enforcement of non-compete agreements is well underway.

Controlling The Forum: Nebraska Federal Court Transfers Non-Compete Declaratory Relief Action To Minnesota Federal Court

November 1, 2011 by Paul Freehling

Lane, a 16-year employee of food distributor Nash Finch Co. ***in Nebraska***, was terminated in June 2011. He promptly filed a declaratory judgment suit in a Nebraska state court against his former employer, challenging the enforceability of non-competition clauses in a series of incentive compensation plans in which he was a participant. His challenge included, but was not limited to, the Minnesota forum selection and choice of law provisions — Nash Finch was headquartered in Minnesota — which were included in the 2010 Long-Term Incentive Program (LTIP) but in none of its predecessors. After removing the case to federal court based on diversity of citizenship, Nash Finch moved to dismiss for improper venue or, alternatively, to transfer the entire case pursuant to 28 U.S.C. §1404(a), including the dispute over the plans without forum selection and choice of law requirements, to the federal court in Minnesota as a more convenient forum. The Nebraska court denied the motion to dismiss but, over Lane's objection, granted the motion to transfer.

Lane maintained that the non-competition clauses, as written, were not reasonably necessary to protect Nash Finch's legitimate business interests and were unduly harsh and oppressive. He contended, among other things, that the clauses identified by name so many competitors for whom he was prohibited from working that he effectively was precluded from employment in the food distribution industry. He also insisted that (a) there was no consideration for the forum selection and choice of law provisions in the LTIP, and (b) the outcome of the case, if it was tried in a Minnesota court, would be contrary to Nebraska public policy because Minnesota permits blue penciling of restrictive covenants if necessary to protect a legitimate business interest whereas Nebraska courts do not. The Nebraska federal court declined to rule on the merits of those contentions. However, it reasoned that the Minnesota court would be obligated to follow the same Restatement (Second) of Conflicts of Laws rules as would a Nebraska court in deciding whether to enforce the choice of law provision. *Lane v. Nash Finch Co.,* Case No. 8:11 CV 241 (D.Neb., Sept. 26, 2011).

Another interesting part of the opinion deals with denial of Nash Finch's Federal Rule of Civil Procedure 12(b)(3) motion to dismiss for improper venue because of the forum selection clause. After examining the split of authority regarding such motions in similar circumstances, the court decided that venue was proper under 28 U.S.C. §1391. However, even though the other incentive programs did not contain a mandate that litigation must be filed in Minnesota, the court decided that judicial economy would be better served by resolution of all of Lane's claims in a single forum.

This case involves an interesting application of Section 1404(a) to forum selection and choice of law provisions included in only the last of a series of employment agreements each of which contains a non-competition clause. The court decided that the plaintiff's choice of a forum, in a lawsuit alleging that all of those clauses were unenforceable, was insufficient to prevent transfer to the federal court in the selected forum state even though only one of the agreement contained forum selection and choice of law provisions. As many seasoned non-compete litigators can attest, the forum selected for a non-compete action often plays a prominent role in whether the forum court will enforce the non-compete.

Georgia Court Blue Pencils / Rewrites Overbroad Restrictive Covenant

October 20, 2011 by Bob Stevens and Daniel Hart

As we have discussed on this blog before, on May 11, 2011, Georgia reissued its new Restrictive Covenant Act (the "New Act"). The New Act reflected a fundamental change in Georgia's law regarding restrictive covenants because it permitted Georgia courts to "blue pencil" (i.e., partially enforce) restrictive covenants that otherwise would be overbroad and, therefore, completely unenforceable under then-existing Georgia case law. While the New Act permits Georgia courts to partially enforce overbroad restrictive covenants, it does not require that they do so.

For the first time since Georgia passed the New Act, a Court in Georgia has elected to exercise its discretion to blue pencil restrictive covenants that it found to be overbroad. In *Pointenorth Insur. Group v. Zander*, No. 1:11-cv-3262-RWS, 2011 U.S. Dist. LEXIS 113413 (N. D. Ga. Sept. 30, 2011), the Court found that, among other things, the non-solicitation covenant contained in the employment agreement at issue was overbroad because it extended to any of the former employer's clients, not just the ones with whom the former employee had contact during her employment.

Rather than attempting to excise or mark out the overbroad provision and enforce the remaining restrictive covenants, the Court modified or altered the restrictive covenant and enjoined the former employee only from soliciting the clients with whom she had contact while employed by the plaintiff. The Court also enjoined the new employer from soliciting the same clients.

This suggests that at least the Court interprets the New Act as providing it with the discretion to re-write restrictive covenants to make them enforceable, rather than merely providing a court with the power to remove overbroad covenants. It remains to be seen if other courts in Georgia follow the *Pointenorth* Court's lead and use the New Act as a basis for re-writing restrictive covenants that are found to be overbroad. For the time being, this decision represents the lone voice on the stage and indicates that there may be a willingness to modify restrictive covenants instead of simply excising them and enforcing the remaining provisions.

Federal Court Reverses Prior Decision on Retroactive Impact of New Georgia Restrictive Covenant Act

August 14, 2011 by Dan Hart

As we have written on this blog before, on May 11, 2011 Georgia reissued its new Restrictive Covenant Act ("New Act") in order to resolve concerns about the constitutionality and effectiveness of a nearly identical statute that the state's legislature had previously enacted in 2009. The 2009 version of the statute was contingent on voters' approval of a ballot referendum to amend the Georgia Constitution, which voters overwhelmingly approved on November 2, 2010. The 2009 statute was clear that it was not retroactive and did not apply to contracts entered into before the purported effective date of the statute (November 3, 2010). Following the same approach, the New Act is also clear that it is not retroactive and does not apply to agreements entered into before May 11, 2011.

Despite the clear inapplicability of the New Act to agreements entered into before May 11, 2011, a question has emerged about whether courts must nonetheless apply Georgia's current public policy when deciding whether to honor choice of law provisions in agreements that predate the New Act.

We previously reported about the recent decision of a federal district judge in the Northern District of Georgia in *Boone v. Correstaff Support Servs., Inc.*, 2011 WL 2358666 (N.D. Ga. June 9, 2011). In that case, the court held that, when deciding whether to honor a choice of law provision in an agreement with restrictive covenants, a court should look to Georgia's current public policy rather than the public policy that existed at the time that the agreement was signed. The court has now reversed course and held that it must apply Georgia's public policy as it existed at the time that the agreement was signed, even though the state's public policy has now changed. *Boone v. Correstaff Support Servs., Inc.*, 2011 WL 3418382 (N.D. Ga. Aug. 3, 2011).

In the *Boone* case, a former employee and his current employer sought a declaratory judgment and injunctive relief prohibiting the employee's former employer from enforcing a non-compete agreement. Although the employee resided in Georgia, the agreement in question contained a Delaware choice-of-law provision. Before the plaintiffs filed their declaratory judgment action in Georgia, the defendants had filed their own lawsuit in Delaware seeking to enforce the agreement. The defendants, therefore, moved the Georgia court to dismiss the declaratory judgment action so that the Delaware could rule on the enforceability of the agreement under Delaware law.

The Georgia federal district court initially granted the defendants' motion, reasoning that, although Georgia's public policy at the time the agreement was signed was hostile to restrictive covenants, Georgia's public policy has now shifted such that Georgia law is no longer inconsistent with Delaware law (which is more lenient toward restrictive covenants than was prior Georgia law). The court thus

reasoned that application of Delaware law to the dispute would not violate Georgia's public policy and that a court in Delaware would be in a better position to apply Delaware law than a court in Georgia.

After the plaintiffs filed a motion for reconsideration, the court reversed its own earlier judgment and denied the motion. In reversing course, the court cited the Georgia Court of Appeals' recent decision in *Bunker Hill Int'l, Ltd. v. Nationsbuilder Ins. Servs., Inc.,* 710 S.E.2d 662 (Ga. Ct. App. 2011). In that case, the Georgia Court of Appeals had refused to honor an Illinois choice of law provision in a restrictive covenant agreement between a Georgia employee and his former employer. Although the Court of Appeals recognized that Georgia law changed in November 2010 with Georgia voters' adoption of a constitutional amendment permitting broader enforcement of restrictive covenants, the agreement at issue was entered into in 2008. Thus, the Court of Appeals applied the law that existed in Georgia prior to the constitutional amendment.

The federal court in *Boone* interpreted the *Bunker Hill* decision as requiring it to apply Georgia's public policy as it existed at the time that the agreement at issue was entered into – and not the state's current public policy – when determining whether to enforce the Delaware choice-of-law provision. The court also cited two other opinions of the Georgia Court of Appeals that, at least in the federal court's view, had reached the same conclusion. See *Gordon Document Products, Inc. v. Serv. Techs., Inc.*, 708 S.E.2d 48, 52 n.5 (Ga. Ct. App. 2011) ("Our analysis in this case is unaffected by any recent legislative proposals or changes."); *Cox v. Altus & Hospice, Inc.*, 706 S.E.2d 660, 663-64 (Ga. Ct. App. 2011) ("We therefore apply the law of restrictive covenants as it existed before [ratification of the constitutional amendment in November, 2010]."). Because the federal court previously had applied Georgia's current public policy to the case, the court reasoned that it had made a clear error of law in its prior order and, accordingly, reversed its prior decision.

At first glance, the federal court's newest decision in *Boone* may seem to suggest conclusively that courts may never consider Georgia's current public policy on restrictive covenants when interpreting agreements entered into before the effective date of the New Act and/or the related constitutional amendment. On closer inspection, however, that answer appears less conclusive because the *Boone* court did not consider one important procedural nuance. The *Boone* court noted that the Georgia Court of Appeals' decision in *Bunker Hill* came "after the effective date of the New Act." Although that is a correct observation, the *Boone* court neglected to note that the lower court judgment that was on appeal in *Bunker Hill* was entered on October 6, 2010 – long before the effective date of the New Act and nearly a month before voters approved the constitutional amendment ballot referendum on November 2, 2010. The lower court judgments that were on appeal in the other two cases cited by the *Boone* court likewise were entered prior to the effective date of either the New Act or the constitutional amendment – specifically, the *Cox* judgment was entered on March 3, 2010, while the *Gordon* judgment was entered on December 17, 2009.

This fact is significant because, at the time that the lower courts entered their judgments in those cases, Georgia's current public policy was not yet in effect. Since the Georgia Court of Appeals' jurisdiction on appeal was limited to determining whether the lower courts had committed reversible error, the Court was required to consider the public policy that existed at the time that the lower courts issued their opinions and not the public policy that existed at the time that the Court of Appeals issued its decisions in those cases. A far different scenario exists where a trial court is tasked with making a *de novo* determination about whether enforcement of a contractual choice of law provision would contravene Georgia's public policy regarding restrictive covenants. In such situations, a trial court arguably is required to apply the public policy of Georgia as it currently exists, even if that public policy contravenes the public policy that existed in Georgia at the time that the agreement in question was entered into. Only time will tell whether Georgia courts follow this approach or the approach followed by the *Boone* court.

California Appellate Court Rules that Five-Year Employee Noncompete Agreement of Unlimited Geographic Reach is Enforceable as a Sanction Against Reticent Defendant

July 20, 2011 by Scott Schaefers

In a recent decision, a California Second District Appellate Court upheld a trial court "issue sanction," which effectively enforced, albeit temporarily, a five-year, unlimited geographic scope employee noncompete agreement against the defendant former employee. *NewLife Sciences v. Weinstock*, — Cal.Rptr.3rd —, No. B223212, 2011 WL 2739653 (July 15, 2011). While such noncompete agreements are normally void and unenforceable under California's well-known statutory bar against employee noncompetes (*see* Cal. Bus. & Prof. Code § 16600), the court stated that the temporary enforcement of the employee noncompete was a permissible issue sanction against the former employee, who time and time again refused to appear for depositions or answer hundreds of deposition questions. The court did not appear to rule on plaintiff's argument that the noncompete fell within the sale-of-business exception under Section 16601, even though the court acknowledged that argument in its opinion. Section 16601 makes enforceable a reasonable non-competition clause executed by any "person who sells the goodwill of a business, or any owner of a business entity selling or otherwise disposing of all of his or her ownership interest in the business entity...." Section 16601 protects the purchaser of a business against competition from the seller.

Some may argue, and the dissent so stated, that the decision may conflict with California's settled public policy against employee noncompetes. Nevertheless, the decision is an example that courts sometimes find ways to enforce noncompetes if there is strong evidence of the former employees' untoward conduct, particularly discovery abuses.

The Parties and the TMR Device

Plaintiff NewLife Sciences ("NLS") purchased from defendant Weinstock and his company the patent rights to a Therapeutic Magnetic Resonance Device ("TMR"), which was developed for pain management therapy, and all the other assets of the company. As part of the transaction, NLS hired Weinstock (who was not a doctor) as its chief science and technology officer and board chairman for five years. Weinstock's employment contract provided, in relevant part, that he (i) could be terminated at any time for "fraudulent or unlawful conduct," (ii) could not compete with NLS while working there, and, (iii) for five years after his employment, could not compete "directly or indirectly with any activity now or in the future engaged in by NLS." The post-employment noncompete contained no geographic limitation.

NLS terminated Weinstock in December 2007 for administering TMR services outside of a physician's presence, in violation of California law, FDA rules, and NLS policy. NLS demanded that Weinstock return to NLS all of its property, including the patented TMR devices. Weinstock did not do so. He continued marketing the devices, and administering treatments.

NLS's Lawsuit and the Trial Court's Ruling

NLS sued Weinstock, claiming breach of the noncompete, and other tortious conduct directed at NLS. NLS produced evidence that Weinstock was smearing NLS in the marketplace, appeared on a television show pawning himself off as the owner of the TMR patent, and soliciting customers and investors for the TMR operations. The trial court denied Weinstock's early motion to strike, which was based on the Section 16600 noncompete bar. Weinstock subsequently refused to appear for his deposition, answer relevant deposition questions, and produce documents as ordered by the court. Weinstock cited the statutory bar as justification for his refusal to respond to discovery. As punishment for what the trial court called his "arrogant and contemptuous disregard for the orders of this court," the trial court entered a severe issue sanction against Weinstock, such that the following issues were established for all purposes in the litigation:

1. Weinstock breached his employment contract by competing with NLS while still employed;

2. The noncompete was enforceable;

3. Weinstock breached the noncompete post-employment by using the TMR device without proper physician supervision; and

4. Weinstock's breach caused NLS damages.

Based on the issue sanctions and NLS's evidence, the trial court entered a preliminary injunction against Weinstock and his affiliated companies from competing with NLS throughout the litigation, including an injunction against making or marketing the TMR device or something similar, and soliciting new, potential or existing customers for TMR devices. The trial court later entered terminating sanctions against Weinstock, and awarded NLS default judgment against Weinstock. He appealed.

Appellate Court Decision and Dissent

The Appellate Court upheld the trial court's preliminary injunction and default judgment. The court did not examine the merits of the Weinstock's Section 16600 or NLS's 16601 argument. Rather, the court held that the trial court did not abuse its discretion by entering the issue sanction, and later awarding default judgment in favor of NLS and against Weinstock. Defendants' repeated and willful non-compliance with the trial court's discovery orders, the Appellate Court held, were sufficient to warrant the court's sanctions.

The dissent stated that the trial court should not have enforced an illegal noncompete by way of a discovery sanction. The trial court and the Appellate Court majority should not have set aside, in the name of discovery sanctions, California's strong public policy against employee noncompetes. At a minimum, the dissent stated, the trial court should have held an evidentiary hearing on whether the noncompete fell under the Section 16601 sale-of-business exception.

Does the New Georgia Restrictive Covenant Act Have a Retroactive Impact?

July 18, 2011 by Bob Stevens

As we have written on this blog before, Georgia reissued its new Restrictive Covenant Act("New Act") on May 11, 2011. The New Act is intended to resolve concerns regarding the constitutionality and effectiveness of the New Act based on the November 2010 ratification of the amendment to the Constitution of Georgia adopting the law and reflects a fundamental change in Georgia's law regarding non-compete, non-solicit and non-disclosure agreements. Perhaps the most dramatic change is permitting courts to "blue pencil" overbroad agreements. These changes likewise reflect a significant and fundamental change in the public policy of Georgia regarding the enforcement of restrictive covenants. The New Act is clear, however, that it is not retroactive and does not apply to contracts entered into before its enactment. Given that, the New Act does not apply to agreements entered into before May 11, 2011.

Despite that, a significant and substantial question has arisen regarding what law applies to Agreements entered before May 11, 2011 when the agreement contains a choice of law provision for a state other than Georgia. In a recent case, *Boone, et al. v. Correstaff Support Services, Inc., et al.*, 2011 U.S. Dist. LEXIS 61666 (N.D. Ga. June 9, 2011), the Court held that it would honor the parties' choice of Delaware law in an agreement entered into in 2008 because Georgia's public policy had changed. The Court determined that, although the New Act does not apply retroactively, in determining whether to honor the parties' agreement to apply Delaware law, the Court should look to Georgia's public policy at the time it reviews the agreement and not at the time the parties executed the agreement. Based on that assumption and concluding that Georgia's current public policy (which has dramatically shifted) is no longer in contravention to Delaware law on restrictive covenants, the Court held that it would apply Delaware law to the 2008 agreement.

Assuming the Court's ruling is correct, if you have an Agreement executed before the New Act with a choice of law provision electing another state's law, it is quite possible that the previously overbroad and once unenforceable provisions in Georgia have just gained new life. Indeed, parties should be very careful running to Georgia seeking a declaratory judgment that an agreement entered into before the New Act is overbroad and unenforceable when that agreement contains a choice of law provision electing another state's law.

Of course, this debate is not over and it is not likely to go away quickly. The Georgia Court of Appeals in *Bunker Hill Int'l, Ltd v. Nationsbuilder Ins. Svcs, Inc.*, 2011 Ga. App. LEXIS 376 (Ga. Ct. App. May 5, 2011) applied Georgia's old public policy when interpreting the application of a choice of law provision (albeit it did so without a detailed analysis of the very issue addressed in *Boone*). Moreover, on June

17, 2011, plaintiffs in *Boone* filed a Motion to Alter or Amend Judgment, or in the alternative, for Reconsideration, arguing that "it would be a clear error of law and a manifest injustice to Plaintiffs to retroactively apply a shift in Georgia public policy to the restrictive covenants Correstaff and Boone signed in Georgia in 2008." That issue is now pending before the Court. This issue, like numerous other issues regarding Georgia's New Act, will be decided by the Courts.

The Unemployment Rate, Mismatched Skills, and ... Non-Competes?

July 5, 2011 by Michael Elkon

A Robert Samuelson piece in the Washington Post on the mismatch between the skills of job seekers and the requirements for open positions may seem like an unlikely place to find an angle on non-compete restrictions. However, in his column on the unemployment rate, Samuelson makes an argument that touches on the role that non-competes can play for employers and employees. In explaining why many individuals who are currently unemployed have struggled to find jobs despite the fact that a number of employers have listed openings, Samuelson theorizes as to why many companies have not responded to the situation by increasing training for new employees:

Companies traditionally provided much training, but that may also have changed. Loyalties have weakened. Companies are more willing to fire; workers are more willing to jump ship. Training may seem a poor investment because workers won't stay long enough to earn a return. In the McKinsey [Global Institute] survey, companies denied cutting training budgets. But [Georgetown's Anthony] Carnevale and others think the training has altered. Before, firms provided more basic training in business or technology skills; now, firms expect workers to come with these skills and focus training on firm-specific practices and systems.

In a nutshell, Samuelson's argument is that a fluid job market acts as a disincentive for employers to train new employees on the general skills required for a position. Rather, they are looking for employees who have the general skills already.

If this analysis is correct, then one potential response by employers to the situation would be greater use of restrictive covenants because such covenants are an important tool for employers to protect their investment in training. An employer is more likely to spend time and money to train an employee if it knows that the employee is likely to stay for a significant period of time. A non-compete restriction acts as an incentive for an employee to stay. Moreover, the law in many states recognizes the linkage between training and non-compete provisions in that a significant expenditure in training can be a legitimate interest to support the enforcement of such a covenant. In short, if an issue in the job market is a concern that money spent on training will be wasted, then use of non-compete provisions can be a solution.

Texas Supreme Court Allows Stock Options as Consideration for Non-Compete Agreements

June 30, 2011 by Robert Milligan

A recent decision by the Texas Supreme Court makes it easier for employers to enforce restrictive covenants in Texas. Employers often seek to obtain these types of contracts with key employees to prevent them from going to work for competitors or to leave to start competing businesses. The enforceability of such contracts is typically governed by state law, resulting in a patchwork of differing standards across the United States, with some states favoring enforcement, and others precluding such agreements altogether. Please read Seyfarth Shaw's One Minute Memo on the new case.

What Georgia's Restrictive Covenant Act Means — and Doesn't Mean — for Employers

May 16, 2011 by Dan Hart

Following Georgia Governor Nathan Deal's signing of House Bill 30 ("H.B. 30") on May 11, Georgia's Restrictive Covenant Act is now law, effective immediately. The Governor's signing of the bill caps months of debate and speculation about the effective date of a nearly identical bill that the Legislature enacted in 2009. That legislation, H.B. 173, was contingent on voters' approval of a ballot referendum to amend the Georgia Constitution – a measure that voters overwhelmingly approved last November. Although the legislature clearly intended the 2009 bill to become effective the day after last November's election, uncertainty about the effective date of the constitutional amendment raised concerns about the effective date of the statute. Accordingly, the legislature enacted H.B. 30 to fix these problems. (For our previous posts on this issue, see here and here.) The new law thus applies to all restrictive covenants entered into on or after the statute's May 11 effective date.

The statute effects a sea-change in the law in Georgia, which historically has been an inhospitable forum for employers seeking to enforce restrictive covenants against former employees. Among other changes, the Act creates statutory presumptions under which courts must presume that restraints two years or less in duration are reasonable in time and that restraints more than two years in time are unreasonable. It also eases the drafting requirements for specific restrictive covenants, abolishes the previously existing requirement of a time-restriction for non-disclosure provisions, and creates a statutory burden-shifting regime whereby, if employers can meet an initial burden of showing that restrictive covenants are in compliance with the statute, parties challenging such restrictive covenants bear the burden of establishing that the covenants are unreasonable. Perhaps most significantly, the new law also 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.

With the new law now officially enacted, should employers now assume that Georgia courts will always uphold restrictive covenants against their employees? Not exactly. As ESPN's Lee Corso might say, "Not so fast, my friends!" Employers should continue to exercise caution in this area for at least three reasons:

First, the Restrictive Covenant Act applies only to restrictive covenants entered into on or after May 11, 2011. Existing Georgia case law applies to restrictive covenants entered into on or before November 2, 2010 (the day that Georgia voters approved a constitutional amendment upon which the new law depends), and might also apply to restrictive covenants entered into between November 3, 3010 and May 10, 2011. For that reason, employers may continue to face an uphill battle in enforcing restrictive

covenants that predate the new law unless they meet the narrow requirements that previously existed under Georgia law.

Second, while the Act *permits* Georgia courts to partially enforce overbroad restrictive covenants, it does not *require* that they do so. Until case law develops under the new statute, employers and their lawyers cannot be certain of what situations Georgia courts will exercise or decline to exercise their blue-penciling power. Based on law in other jurisdictions, however, it appears likely that Georgia courts may decline to exercise their blue-penciling power in cases where they believe that employers have unreasonably overreached for the purpose of creating an *in terrorem* effect on employees. Thus, employers should continue to exercise restraint when drafting restrictive covenants and should avoid drafting unreasonably broad covenants with the expectation that they will be fixed by the courts.

Third, although most provisions of the Act are beneficial to employers, the Act places restrictions on the types of employees who may be subjected to true non-compete provisions (as opposed to non-solicitation or nondisclosure provisions). Such provisions may be enforced only against employees who:

- "Customarily and regularly solicit for the employer customers or prospective customers;"
- "Customarily and regularly engage in making sales or obtaining orders or contracts for products or services to be performed by others;"
- Perform specified management duties (which are set forth in the Act using language that closely follows the U.S. Department of Labor's ("DOL) definition of the Fair Labor Standards Act's ("FLSA") "executive" exemption);
- Perform the duties of a "key employee" (which the Act defines as " an employee who . . . has gained a high level of influence or credibility with the employer's customers, vendors, or other business relationships or is intimately involved in the planning for or direction of the business of the employer or a defined unit of the business of the employer" or "an employee in possession of selective or specialized skills, learning, or abilities or customer contacts or customer information who has obtained such skills, learning, abilities, contacts, or information by reason of having worked for the employer"); or
- Perform the duties of a "professional" (which the Act defines using language that closely follows the DOL's definition of the FLSA's "professional" exemption.

Before requiring employees to execute new non-compete agreements, employers should ensure that employees who are subject to the restriction fall within one of the definitions included in the statute.

Notwithstanding these necessary precautions, employers might consider revamping their standard restrictive covenants to take full advantage of the changes created by the Act. When undertaking such an effort, employers may want to consider the following issues:

- ***Are your non-solicitation provisions consistent with the language approved by the Act?*** The Act provides that "[a]ny reference to a prohibition against 'soliciting or attempting to solicit business from customers' or similar language shall be adequate [for non-solicitation restrictions] and narrowly construed to apply only to: (1) such of the employer's customers, including actively sought prospective customers, with who the employee had material contact; and (2) products and services that are competitive with those provided by the employer's business." Because this provision loosens the previously-existing rules for drafting non-solicitation covenants, employers may be able to streamline the language that they use for such covenants.

- ***Are your definitions of restricted geographic territories and competitive activities consistent with the language approved by the Act?*** The Act provides that "[a]ctivities, products, or services [covered by a restrictive covenant] shall be considered sufficiently described if a reference to the activities, products, or services is provided and qualified by the phrase 'of the type conducted, authorized, offered, or provided within two years prior to termination' or similar language containing the same or a lesser time period." Likewise, the Act provides that "[t]he phrase 'the territory where the employee is working at the time of termination' or similar language shall be considered sufficient as a description of geographic areas if the person or entity bound by the restraint can reasonably determine the maximum reasonable scope of the restraint at the time of termination." These provisions significantly loosen rules that previously existed for drafting restrictive covenants in Georgia and may likewise provide some employers with an opportunity to streamline their agreements.

- ***Are your nondisclosure provisions drafted as broadly as reasonable?*** Existing case law in Georgia requires nondisclosure provisions to bear a reasonable time limitation (usually a period of two years or less) with respect to any information that does not constitute a "trade secret" as defined by relevant law. Consistent with this requirement, many employers in Georgia historically have drafted their nondisclosure covenants to apply to a period of two years or less. Because the Act abolishes the requirement of a time limitation for nondisclosure covenants, employers should consider whether they want to revise the language in their existing nondisclosure covenants.

If you are interested in reviewing your existing restrictive covenant agreements for compliance with the new statute, or if you would like assistance drafting such agreements for your workforce, contact a Seyfarth Shaw Trade Secrets Group attorney.

Iowa - Sophisticated Employees Bound by Reasonable Restrictive Covenants; Plaintiff to Post $2 Million Bond

May 11, 2011 by Paul Freehling

A recent Iowa U.S. district court decision upheld two-year, geographically reasonable, non-compete agreements signed by 26 veterinarians while they were employed by Iowa Veterinary Specialties, P.C. (IVS), a Des Moines, Iowa clinic they owned. When two of the vets and IVS's operations manager learned that its sale to ISU Veterinary Services Corporation (VSC) was imminent, they used IVS's business information and facilities to assist them in opening a competing veterinary clinic. VSC is a non-profit subsidiary of Iowa State University (ISU) which is home to the oldest veterinary college in the U.S. The purchase of IVS was made with public funds and was intended to be part of ISU's mission to regain and enhance its veterinary college academic preeminence. The acquired assets included the non-compete agreements.

VSC sued the two vets and the operations manager, seeking a preliminary injunction. Except as against the operations manager, who had not signed a non-compete agreement, the injunction was entered. The court held that VSC had met its burden of showing a likelihood of success on the merits and that the balance of the equities favored VSC, and the court concluded that "enforcement of valid non-competition agreements serves the public interest." However, the court did order VSC either to post a $2 million surety bond or to provide a binding representation from ISU that it will pay any judgment the vets may obtain against the University. *ISU Veterinary Services Corp. v. Reimer*, 2011 WL 1595337 (S.D. Iowa Apr. 27, 2011).

The vets contended that an injunction would bankrupt them, but the court turned that contention against them by stating it showed that VSC had no satisfactory remedy at law. Moreover, VSC proved that the purchased entity had experienced a decline in its revenue and in the number of its patients since the defendants became competitors, thereby showing how harmful denial of injunctive relief would be.

The court also rejected arguments made by the vets regarding the supposed unfairness or ambiguity of the non-compete agreements, adding that the vets were highly compensated, sophisticated and well-educated, and that the non-compete had substantial monetary significance. So, they should have retained counsel for advice before signing. Assertions that Iowa law prohibits public bodies from competing with private enterprise, and that Iowa's Veterinary Practice Act prohibited VSC from practicing veterinary medicine, likewise were to no avail.

Iowa law says that "discharge by the employer is a factor opposing the grant of an injunction" to enforce a non-compete agreement. One of the vets had not been offered a position by VSC. However,

that individual had “expressed a complete unwillingness to remain” after the acquisition, and so an offer to him of employment would have been futile.

The principal message of the *VSC* case is that sophisticated signatories to reasonable non-compete agreements have an uphill battle when faced by an injunction action. Nevertheless, a very substantial bond requirement (as here) could prove to be a significant obstacle to enforcement of an injunction.

Georgia Governor Signs New Restrictive Covenant Act

May 11, 2011 by Seyfarth Shaw LLP

As we have posted previously, there is some question regarding the effective date of Georgia's Restrictive Covenant Act, O.C.G.A. § 13-8-50 *et seq.*, the statute passed by the Georgia General Assembly in 2009 and authorized by passage of an enabling constitutional amendment in November 2010. The RCA changes Georgia's legal regime regarding restrictive covenants. Because of the uncertainty regarding the statute's effective date (and resulting potential constitutional issues), the General Assembly has been considering a bill - House Bill 30 - that would re-enact the RCA to end any constitutional questions.

HB 30 also addresses a second issue regarding the RCA. There has been some debate as to the meaning of the provisions of O.C.G.A. § 13-8-56, specifically whether it applies only to in-term covenants. HB 30 revises that section of the non-compete statute by making it clear that the presumptions contained in O.C.G.A. § 13-8-56 apply to in-term ***and*** post-term covenants. This provision is important to businesses and employers for a number of reasons, including that Georgia employers will be permitted to list specific competitors in place of specifying a geographic area in a non-compete restriction.

On Tuesday, February 22, 2011, the House of Representatives passed HB 30 by a margin of 104 to 58. The bill is now before the Senate. We will continue to monitor the progress of the bill.

"Under Pressure" Not Enough To Make Agreement Unenforceable

May 6, 2011 by Eddy Salcedo

Employment Agreement's forum, venue and personal jurisdiction clause upheld despite argument that the agreement was signed "under extreme pressure" and without sufficient time for counsel to review. CLP Resources, Inc. v T. Salerno, 2011 WL 1597677 (W.D.Wash.) (April 27, 2011).

Plaintiff CLP Resources, Inc. ("CLP"), a large provider of temporary construction workers, sued a former employee, defendant Salerno, and his new business, Defendant Alliance Project Staffing ("Alliance"), claiming causes of action for breach of contract, misappropriation of trade secrets and tortious interference with existing and prospective contracts. CLP's causes of action were based upon allegations that Salerno, while employed as an Account Manager at CLP, started a directly competing business, Alliance, using CLP resources. CLP asserted that Salerno's conduct violated the terms of his Employment Agreement with CLP.

Defendant Salerno moved to dismiss the action upon the arguments (1) that the Western District of Washington lacked personal jurisdiction and (2) that venue was not proper in that court as he had worked for CLP in central California, not Washington.

In response, CLP argued that the action was commenced in the United States District Court for the Western District of Washington pursuant to the terms of the Employment Agreement, which directed that venue for any action to enforce the agreement would be either the State Court in Pierce County Washington, or the Federal Court in the Western District of Washington. It was further argued that the Employment Agreement also contained covenants that Salerno would submit to the personal jurisdiction of either of those courts, would not raise personal jurisdiction as a defense to any action premised upon the Employment Agreement, and finally that the laws of the State of Washington would govern any dispute.

Salerno attempted to counter the enforceability of the Employment Agreement by claiming that he signed the agreement "under extreme pressure," three days after he began working for CLP, and after he had irrevocably relocated from Tennessee to work for CLP in California. He further claimed that he did not have an attorney review the document, and did not have time to review it himself, thereby making the jurisdiction, venue and are unenforceable due to duress and fraud. Finally, he claimed that the agreement was not supported by consideration because he had already begun working at the time he signed it.

In addition to his common law defenses to the agreement, Salerno added a statutory defense, alleging that the Employment Agreement also contained a non-competition provision which was not consistent, and as such void under, California Code §16600.

The Western District of Washington rejected all of Salerno's arguments, denying his motion in its entirety. In denying the motion and upholding the jurisdiction, venue and choice of law provisions of the Employment Agreement the court held as follows.

First, whether California Code §16600 would ultimately be dispositive of CLP's claims was not relevant at this stage in the litigation because "it plainly does not apply to the consent to personal jurisdiction, forum selection and choice of law provisions." Further holding that "[t]his California statute is not a defense to jurisdiction or venue in this Court."

Next, with respect to Salerno's argument that the Employment Agreement was procured by fraud or duress, or was otherwise not enforceable because Salerno was "coerced" into signing without adequate time to review the document, and without the benefit of the advice of counsel, the court held that "[t]here is no authority for the proposition that such time or attorney review is a prerequisite for the execution of a binding Employment Agreement. Nor is it novel that one seeking employment is offered the same conditioned on the acceptance of the terms of an employment agreement."

Finally, with respect to Salerno's claim that he did not see the actual agreement before he began working for CLP, the court found that "…it is undisputed that his employment was always expressly conditioned upon his agreement to those terms. His claim about the consideration provided for his agreement is not enough, therefore, to negate his assent to the terms of the Employment Agreement."

Indiana Court Upholds A Covenant Not To Solicit Recent Customers, But Prohibitions Against Contact or Accepting Referrals With Such Customers Are Stricken

May 4, 2011 by Paul Freehling

A recent Indiana Court of Appeals opinion, designated as non-precedential, discussed that state's law concerning non-competition agreements. Most significant, the court upheld a commitment not to solicit the employer's current or recent customers for two years even though the covenant contains no geographical limitation. However, provisions precluding any "contact with" such customers, and forbidding acceptance of "referrals of" them, were "blue penciled." The court reversed the entry of summary judgment for the ex-employees and remanded for trial. *Think Tank Software Dev. Corp. v. Chester, Inc.*, No. 64A03-1003-PL-172 (Ind. Ct. Appeals, Apr. 11, 2011).

Think Tank Software Development Corporation, and a number of companies affiliated with it (collectively, "Think Tank"), sued 10 former employees almost all of whom went to work for defendant Chester, Inc. Think Tank and Chester are competitors, engaging in what the court called "computer-related business activities." Think Tank alleged violation of covenants not to compete and misappropriation of trade secrets.

After more than five years of motion practice and discovery, the trial court granted summary judgment to the defendants on the grounds that the covenant not to compete "is overbroad and is therefore unenforceable . . . and cannot be reformed," and that the property rights in which Think Tank claimed confidentiality did not constitute trade secrets. What the trial court apparently viewed as the covenant's fatal flaw was that it was unlimited as to an applicable territory. Further, the affidavit of a former Think Tank director of technology seemingly demonstrated that the company had no protectable business information.

The Court of Appeals disagreed. Although upholding a two-year restriction on *solicitation* of recent former customers, the appellate court struck as unreasonable the prohibition against contacting them. Similarly, the court approved a ban on selling to, servicing, consulting, or negotiating with those customers, but a prohibition on acceptance of referrals of new customers -- for example, by the ex-employer's customers -- was invalidated. Indiana recognizes "blue penciling" as an option for a court. The absence of a territorial restriction was not fatal, according to the court, because "the class of prohibited contacts [customers who had been such within two years of the former employees' termination] is well defined and specific, thereby eliminating the need for any geographical limitation."

As for trade secrets, the appellate tribunal held that Think Tank sufficiently raised genuine issues of material fact with respect to whether the company's "customer identities" and "tailored solutions to the

customers' information technology needs combine to form confidential information." Similarly, Think Tank provided enough evidence of "its extensive security provisions in protecting" that information to withstand a motion for summary judgment.

The enforceability of a non-compete and non-solicitation agreement in a particular case frequently turns on the applicable facts and circumstances, the precise wording of the restriction, and the jurisdiction. The question of whether particular information qualifies as a trade secret also is fact-intensive. When in doubt, contact a Seyfarth Shaw Trade Secrets Group attorney.

Georgia House of Representatives Passes “Fix” to Restrictive Covenant Act

February 25, 2011 by Michael Elkon

As we have posted previously, there is some question regarding the effective date of Georgia's Restrictive Covenant Act, O.C.G.A. § 13-8-50 *et seq.*, the statute passed by the Georgia General Assembly in 2009 and authorized by passage of an enabling constitutional amendment in November 2010. The RCA changes Georgia’s legal regime regarding restrictive covenants. Because of the uncertainty regarding the statute’s effective date (and resulting potential constitutional issues), the General Assembly has been considering a bill - House Bill 30 - that would re-enact the RCA to end any constitutional questions.

HB 30 also addresses a second issue regarding the RCA. There has been some debate as to the meaning of the provisions of O.C.G.A. § 13-8-56, specifically whether it applies only to in-term covenants. HB 30 revises that section of the non-compete statute by making it clear that the presumptions contained in O.C.G.A. § 13-8-56 apply to in-term ***and*** post-term covenants. This provision is important to businesses and employersfor a number of reasons, including that Georgia employers will be permitted to list specific competitors in place of specifying a geographic area in a non-compete restriction.

On Tuesday, February 22, 2011, the House of Representatives passed HB 30 by a margin of 104 to 58. The bill is now before the Senate. We will continue to monitor the progress of the bill.

Injunctive Relief and a Substantial Monetary Judgment Awarded to National CPA Firm Against Former Employees Who Breached Non-Compete Agreements

February 14, 2011 by Paul Freehling

The national CPA firm of Mayer Hoffman McCann P.C. ("MHM"), based in Missouri, scored a major victory when the Eighth Circuit Court of Appeals affirmed a trial court's injunctions and liquidated damages award of $1,369,921 against four former stockholder-employees in Minnesota. The injunctions prohibited them from soliciting MJM's clients, directed them and their employees to make their office and home computers available to a computer forensic expert, and enjoined them from using (and ordered them to return) MJM's trade secrets and confidential information. The appellate court's decision is notable because of its analysis of when non-compete covenants and contractual liquidated damages provisions are enforceable, but also because of the court's view that non-solicitation agreements are unenforceable.

In 2005, the individuals executed a Stockholders Agreement pursuant to which they covenanted not to solicit MHM's clients and customers for two years after leaving MHM's employ. However, in 2008, immediately after their resignation from MHM, the individuals started a competing firm which proceeded to serve at least 124 MHM clients.

The covenants were challenged as lacking in consideration, being contrary to Missouri law, and having unenforceable remedy terms. The court discussed and rejected almost every challenge. *Mayer Hoffman McCann, P.C. v. Barton*, 614 F.2d 893 (8th Cir. 2010).

With regard to consideration, the defendants relied on a 1996 Missouri appellate court decision that invalidated, for lack of sufficient consideration, a non-compete clause contained in a buy-sell agreement. That court, however, was influenced by the absence of a contemporaneous employment contract and the failure of the buy-sell agreement to state that the clause was intended to protect special interests of the buyer. In the *Mayer Hoffman* case, the individuals who signed the covenants were employees. Further, the Agreements contained mutual promises, recited that the purpose of the covenants was protection of MHM's legitimate special interests — its proprietary trade secrets to which the individuals had access — and did not include restrictions greater than fairly required. So, consideration was adequate.

Several Missouri appellate court opinions identify the types of agreements in which restrictive covenants are permissible. No reported case involved a covenant ancillary to a shareholder's agreement relating to a professional corporation. But the Eighth Circuit Appeals Court held that since a few decisions upheld covenants in agreements with various kinds of close corporations, and a

professional corporation is a type of close corporation, the covenants at issue are enforceable. The two-year covenant was without geographical restrictions, but it was limited to MHM clients who the defendants solicited, and that was held to conform with Missouri law.

The defendants claimed that the non-compete clause failed because MHM had no protectable interest in clients who the individuals had begun servicing before signing the Stockholder Agreements. The court disagreed. MHM had invested money, time and effort in strengthening the pre-existing relationships. The court did concur with the defendants that, under Missouri law, MHM had no protectable interests in the defendants' co-workers' continued employment, and so the non-solicitation clause was unenforceable.

The Agreements provided that a violator of the covenant not to compete would owe liquidated damages equal to the sum of MHM's total billings, for the two years prior to violation of the covenant, to the clients the violators successfully solicited. Overruling the defendants' contention that the damages clause created an unenforceable penalty, the court held that the clause was valid because an accurate estimate of damages was difficult to make, and two years' billings was a reasonable forecast of the harm caused by the individuals' breach of contract.

The injunctive and monetary award in *Mayer Hoffman* might be harsher than some courts would have rendered. However, the contract violation here was particularly egregious. In any event, the opinion suggests how to draft enforceable trade secret protection agreements, non-compete covenants, and liquidated damages clauses. The decision shows the horrendous consequences that may be faced by anyone who misappropriates trade secrets and breaches a covenant not to compete. For questions about the *Mayer Hoffman* case or other trade secret issues, please contact the Trade Secrets Team at Seyfarth Shaw.

Massachusetts Legislature Considers Revised Non-Compete Bill

February 4, 2011 by Erik Weibust

On January 20, 2011, Massachusetts State Representatives Lori Ehrlich, William Brownsberger, and Alice Hanlong Peisch re-filed the Massachusetts non-compete bill, aptly entitled "An Act Relative to Noncompetition Agreements." The bill was originally submitted in late 2009 as House No. 1799, and since that time has undergone significant review, comment, and revision. While much of the bill remains the same, its sponsors made changes to address several concerns the business community had expressed about particular provisions. There is no current timeline for a vote on the bill, but we do expect there to be ample opportunity to provide additional input.

What Remains the Same As the Prior Bill?

The bill applies to non-compete agreements in the context of employment, including forfeiture for competition agreements (agreements that impose adverse financial consequences if an employee engages in competitive activities). However, the bill specifically excludes non-solicitation agreements (both of customers and employees); non-compete agreements outside the employment context, such as those that are executed in the sale of a business; forfeiture agreements (agreements that impose adverse financial consequences as a result of termination regardless of whether the employee engages in competitive activities); and agreements not to reapply for employment. The bill does not apply to non-disclosure or confidentiality agreements.

In essence, the bill codifies the existing common law rules, which provide that non-compete agreements are enforceable only if they are reasonable in duration, geographic reach, and scope of proscribed activities necessary to protect the employer's trade secrets, confidential information, or goodwill, and are consonant with public policy. In addition, the bill does not change current Massachusetts law permitting courts to reform or modify unreasonable non-compete agreement provisions.

The bill requires non-competes to be in writing, signed by both parties, and "to the extent reasonably feasible," they must be provided to the employee at least seven business days in advance of employment. If the agreement is executed after the commencement of the employment relationship, the employee must be provided with notice and "fair and reasonable" consideration (beyond continued employment).

The bill restricts non-compete agreements to one year, except for "garden leave" clauses (agreements by which the employer agrees to pay the employee during the restricted period), which may last up to two years.

The bill mandates the payment of attorneys' fees to employees if a court refuses to enforce "a material restriction or reforms a restriction in a substantial respect," or if it finds that the employer acted in bad faith. Attorneys' fees are not mandated, however, if a particular provision is "presumptively reasonable," as defined by the statute, or if the employer made "objectively reasonable efforts to draft the rejected or reformed restriction so that it would be presumptively reasonable," even if a court refuses to enforce or reforms the provision. An employer may be entitled to its legal fees if it prevails only if they are otherwise permitted by statute or contract, the agreement is presumptively reasonable, the non-compete was enforced, and the employee acted in bad faith.

What Has Changed From the Prior Bill?

Perhaps the most significant change in the current version of the bill is that it no longer restricts the use of non-compete agreements to employees making more than $75,000 per year. Instead, the bill calls for courts to consider the economic circumstances of, and economic impact on, the employee. This is important because there are many companies doing business in the Commonwealth, oftentimes start-ups, that employ individuals who are paid less than $75,000 per year, but who are otherwise provided with potentially lucrative equity interests, stock options, or the like. The departure of these employees to a competitor can cripple a start-up company and can even cause hardship to well-established companies that may utilize these other types of non-monetary compensation and pay key employees less than $75,000. This salary benchmark was also a concern for companies that employ part-time or seasonal employees, and staffing agencies, to name a few, which may not meet the $75,000 salary benchmark in a calendar year.

Another change in the bill relates to the award of mandatory attorneys' fees to employees. While this provision remains in the bill, as discussed above, an employer can avoid paying fees if the court determines that it undertook "objectively reasonable efforts to draft the rejected or reformed restriction so that it would be presumptively reasonable," even if unsuccessful. This provision, however, does not provide clear guidance to employers as to the parameters of such "objectively reasonable efforts," and remains a significant departure from existing law that litigants pay their own attorneys' fees, win or lose.

Like some other states, including California, the bill, in its prior and current versions, explicitly rejects the inevitable disclosure doctrine (which holds that even in the absence of an enforceable non-compete agreement, a former employee may be prevented from working for a competitor based on the expectation that the employment would inevitably lead to the disclosure of trade secrets or confidential information of the former employer). The newest version of the bill, however, recognizes that employers

may nevertheless protect themselves using other laws and agreements, including applicable trade secrets laws and non-disclosure agreements.

Other changes from the last version of the bill include: (a) non-competes executed after the commencement of employment no longer must be accompanied by a 10% increase in salary to be presumptively reasonable; now, they must simply be supported by "fair and reasonable consideration"; (b) non-compete agreements no longer need to be separate documents; (c) garden leave clauses are permitted; and (d) the scope of restrictions placed on forfeiture agreements has been limited.

Finally, it is important to note that the bill is not retroactive, and will not apply to agreements entered into before January 1, 2012.

Seyfarth Shaw plans to monitor and participate in the legislative process and will report on the status and evolution of this bill on our blog, Trading Secrets, at www.tradesecretslaw.com. If you have any questions or would like to provide input on the bill, please contact the Seyfarth Shaw attorney with whom you work or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (www.seyfarth.com/tradesecrets) Click here for Seyfarth Shaw's Management Alert on the bill.

Illinois House of Representatives Revisits Non-Compete Statute

February 6, 2011 by Scott Humphrey

We informed our readers on March 31, 2009 about Illinois House Bill 4040, titled "Illinois Covenants Not to Compete Act" (link). House Bill 4040 attempted to limit non-compete enforcement to employees or independent contractors who:

- have substantial involvement in the executive management of the employer's business;
- have direct and substantial contact with the employer's customers;
- possess knowledge of the employer's trade secrets and/or proprietary information;
- possess such unique skills that they have achieved "a high degree of public or industry notoriety, fame, or reputation as a representative of the employer;" or
- are among the highest paid 5% of the employer's work force for the year immediately preceding the separation.

House Bill 4040 also attempted to change Illinois law by:

- eliminating an employer's ability to enforce a non-competition covenant if the employer failed to notify the new employee two weeks prior to the first day of his employment that a covenant not to compete is required, or if the covenant is not accompanied by a "material" advancement, promotion, bonus or compensation increase;
- creating a rebuttable presumption that a non-competition covenant is invalid if the covenant exceeds one year, the geographic restrictions in the covenant cover areas beyond which the former employee provided services "*during the one year preceding his termination*;" or if the covenant concerns personal services activities that the employee did not perform during the "*one year preceding termination of their employment*;"
- forbidding a court, if it chooses to modify an existing covenant, from imposing a damages award for the employee's original breach of the covenant;
- instructing a court to interpret any attorneys' fees provision found in a non-competition covenant to allow either the employer or the employee to recover their attorneys' fees

- empowering the court to award attorneys' fees to the employee if, through a declaratory judgment action brought by the employee, the court declares the non-competition covenant unenforceable.

House Bill 4040 was introduced by Representative Rosemary Mulligan (Republican - 65th District) and never made it out of committee. Hence, the Bill terminated when the Illinois House of Representatives concluded its session. However, Representative Jil Tracy (Republican - 93rd District) introduced a bill identical to House Bill 4040 on January 12, 2011. Representative Mulligan became a co-sponsor of Representative Tracy's bill, House Bill 0016, on February 4th. So far, House Bill 0016 has not attracted significant public attention or traction in the Illinois House. Nevertheless, we will continue to monitor House Bill 0016 and any other actions the Illinois House or Senate may undertake with respect to non-competition agreements or trade secrets.

Georgia Legislature to Consider Re-enacting Restrictive Covenant Act

January 7, 2011 by Seyfarth Shaw LLP

As we have noted in an earlier blog posting, many have raised questions about the effective date of Georgia's new Restrictive Covenant Act. The questions derive from inconsistencies in the effective dates between the amendment that gave life to the statute and the statute itself. To cure this potential issue, Rep. Wendell Willard, Vice Chairman of the Rules Committee and Chairman of the Judiciary Committee, has introduced HB 30 to re-enact the statute. In Section 1 of the Bill, the purpose of introducing HB 30 is set forth:

> During the 2009 legislative session the General Assembly enacted HB 173 (Act No. 64, Ga. L. 2009, p. 231), which was a bill that dealt with the issue of restrictive covenants in contracts and which was contingently effective on the passage of a constitutional amendment. During the 2010 legislative session the General Assembly enacted HR 178 (Ga. L. 2010, p. 1260), the constitutional amendment necessary for the statutory language of HB 173 (Act No. 64, Ga. L. 2009, p. 231), and the voters ratified the constitutional amendment on November 2, 2010. It has been suggested by certain parties that because of the effective date provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), there may be some question about the validity of that legislation. It is the intention of this Act to remove any such uncertainty by substantially reenacting the substantive provisions of HB 173 (Act No. 64, Ga. L. 2009, p. 231), but the enactment of this Act should not be taken as evidence of a legislative determination that HB 173 (Act No. 64, Ga. L. 2009, p. 231) was in fact invalid.

The speed with which this may pass through the legislature when it reconvenes on January 10 is unknown. As of today, it is not yet on the legislative calendar.

SEYFARTH SHAW LLP
ATTORNEYS

Atlanta	Los Angeles	Washington, D.C.
Boston	New York	London
Chicago	Sacramento	
Houston	San Francisco	www.seyfarth.com

Breadth. Depth. Results.