SEYFARTH SHAW LLP
ATTORNEYS

Trading Secrets

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

2012 – Year in Review

Trading Secrets

Dear Clients and Friends,

2012 was another fabulous 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, Corporate Counsel, Bloomberg News, BNA, 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 2012 Year in Review which compiles our significant blog posts from 2012 and highlights our blog's authors. For a general overview of 2012, we direct you to our Top-10 2012 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2012 Trade Secrets Webinar Series - Year in Review blog entry, which provide a summary of 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. We incorporated several new features, including video interviews, an informative resources page, special guest authors, and cutting edge infographics, and provided access to our well-received Trade Secret Webinar Series from 2011 to the present. In 2013, we plan to incorporate video blog posts, audio podcasts, more special guest authors, and provide a more enhanced resources page on the blog. We also plan to incorporate the developments in privacy, social media, and technology into our blog coverage.

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 2012, we hosted eight webinars which are listed in the program listing contained in this Review . For those who missed any of the programs in 2012'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 2012 webinars, please e-mail CLE@seyfarth.com to request a username and password.

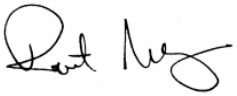
We are kicking off the 2013 webinar series with a program entitled, "2012 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law." More information on our upcoming 2013 webinars is available in the program listing contained 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 preeminent 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

Table of Contents

Trading Secrets

2012 Trade Secrets Webinar Series

- Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff
  January 2012
- Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing
  March 2012
- Pleading, Providing and Protecting Trade Secrets in Litigation
  April 2012
- Protecting Your Trade Secrets in the Financial Services Industry
  May 2012
- When Trade Secrets Cross International Borders
  July 2012
- Trade Secrets and Non-Compete Legislative Update
  September 2012
- Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours
  November 2012
- 2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law
  December 2012

Trading Secrets

2013 Trade Secrets Webinar Series

- Latest Cases/Developments in Trade Secret/Non-Compete/Computer Fraud Law - 2012 National Year In Review
- Legislative Update: Massachusetts, Illinois, and Federal Legislation Review
- Trade Secrets in the Pharmaceuticals Industry
- Trade Secrets in the Telecommunications Industry
- Trade Secrets in Financial Services Industry
- How Big Data Impacts Trade Secret and Computer Fraud Law
- Are Trade Secrets More Important Under the America Invents Act?
- When Trade Secrets Collide With The Latest Developments In Social Media and Privacy Law
- Trade Secret and Non-Compete Considerations In Asia
- How and Why California Is Different When It Comes To Trade Secrets and Non-Competes
- My Company's Trade Secrets And Confidential Information Were Posted On The Internet, What Can I Do?

Trading Secrets

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.

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.

Robert Milligan is the editor of the blog and a partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP. His practice encompasses a wide variety of commercial litigation and employment matters, including general business and contract disputes, unfair competition, trade secret misappropriation and other intellectual property theft, franchise litigation, real estate litigation, insurance bad faith, invasion of privacy, consumer and employee class actions, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower and SOX cases, bankruptcy, and other business torts. He specializes in trade secret, non-compete, social media, privacy, and data protection litigation and transactional work on a state, national, and international platform.

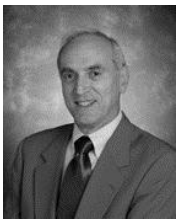
Justin Beyer is an associate in the Chicago office of Seyfarth Shaw LLP and a member of the firm's Commercial Litigation Practice Group. Mr. Beyer focuses his practice in the areas of product liability, complex commercial litigation, and trade secrets, including seeking and defending against injunctive relief based on claims of misappropriation of trade secrets and breaches of non-competition agreements.

Michael Baniak is a partner in the Chicago office and a member of the firm's Intellectual Property Practice Group. As a trial attorney, he has been involved in upwards of 300 intellectual property litigations over the course of his career, with more than half of those being patent litigations. Mr. Baniak has a broad-based practice, and expertise that spans all facets of IP transactions, counseling, and litigation and appellate work, in patent, trademark, copyright and trade secret law. He is a true "hybrid," working in every aspect of IP virtually daily.

Trading Secrets

Misty Blair is an associate in the Intellectual Property and Commercial Litigation Practice Groups of Seyfarth Shaw LLP. She practices in the areas of complex civil litigation, patent litigation, and a variety of intellectual property matters, including patent and trademark prosecution. She has represented and advised clients in a variety of litigation contexts, including biological, pharmaceutical, chemical, and medical devices. Ms. Blair has provided litigation support in complex patent litigation matters and has experience analyzing patent claims, prosecution histories and developing infringement and non-infringement positions.

Randy Bruchmiller is a senior associate in the Commercial Litigation and Trade Secrets practice groups of Seyfarth Shaw LLP. Mr. Bruchmiller was a principal at a medium-size litigation firm in Houston prior to joining Seyfarth Shaw in 2010. He has handled a variety of cases while representing both plaintiffs and defendants. He has obtained numerous favorable outcomes for those clients through summary judgments, settlements and trial.



Paul Freehling is a partner with the Chicago office. 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.

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.

Daniel Hargis is an associate in the Los Angeles office of Seyfarth Shaw LLP. His practice focuses on business litigation, with an emphasis on consumer class actions. He has litigated numerous consumer class actions on behalf of corporate defendants in federal and state courts, including class actions brought under California's Unfair Competition Law, False Advertising Law, the Consumer Legal Remedies Act, and the Song-Beverly Credit Card Act. In these class actions, Mr. Hargis has represented several *Fortune* 500 companies and other businesses with a national presence.

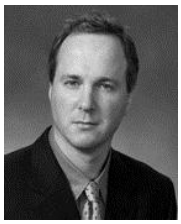
Trading Secrets

Daniel Hart is an associate in the Atlanta office of Seyfarth Shaw LLP. A member of the Labor & Employment department, he focuses his practice in all aspects of labor and employment litigation, including race, gender, national origin, age, and disability discrimination claims, wage and hour disputes, and common law tort claims, before various state and federal courts and administrative agencies.

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.

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.

Jessica Mendelson is an associate in the Litigation practice group of Seyfarth Shaw LLP. She has counseled and represented a variety of clients in the litigation process. Her practice focuses on commercial litigation, including trade secrets, the defense and prosecution of claims for breach of contract and business torts, as well as construction law and government contracts.

Trading Secrets

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.

Eddy Salcedo is an experienced first-chair trial lawyer based in New York. 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.

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 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.

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.

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.

Trading Secrets

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 Whistleblower and Fraud & Abuse, False Claims and Internal Investigations Teams.

Matthew Werber is an associate in the firm's litigation practice group. His practice focuses primarily on areas of intellectual property litigation and counseling. Mr. Werber has represented some of the world's largest manufacturers and retailers in federal courts, state courts and the U.S. International Trade Commission in litigation matters involving semiconductors, smart phone mobile devices, e-commerce, information systems, software, mechanical devices, water treatment systems and computerized modeling, among other technologies.

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.

James Yu is a partner in the Litigation and Labor & Employment Departments. He has defended several class action lawsuits, including wage and hour class and collective actions, and is experienced in handling multi-district litigations.

Trading Secrets

2012 Summary Posts

- 2012 Trade Secrets, Computer Fraud, and Non-Competes Webinar Series – Year in Review
  By Robert Milligan (December 20, 2012)

- Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2012
  By Robert Milligan and Joshua Salinas (December 31, 2012)

Trade Secrets

- US Companies Have Options Against Chinese Companies For Trade Secret Misappropriation
  By Eddy Salcedo (January 9, 2012)

- After Ohio Jury Finds Trade Secret Misappropriation But Awards Zero Damages, Trial Judge Enters Injunction Order But Sets Royalty Payment As Alternative
  By Paul E. Freehling (January 10, 2012)

- 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
  By Paul E. Freehling (January 12, 2012)

- Does A Trade Secret Plaintiff Have To Disclose Its Trade Secrets Prior To The Commencement Of Discovery In California Federal Court?
  By Joshua Salinas (January 13, 2012)

- Court Rules Pennsylvania Trade Secrets Act Entitles Defendants To Attorneys' Fees For Bad Faith Misappropriation Claim
  By Justin Beyer (January 24, 2012)

- Court Allows Employer's Interference With Prospective Economic Advantage Claims To Survive In Lawsuit Claiming Employee's Theft of Twitter Account
  By Robert Milligan and Gary Glasser (February 1, 2012)

- New Jersey Adopts Variation of Uniform Trade Secrets Act
  By Robert Milligan (February 3, 2012)

- Filing A Patent Application Covering A Misappropriated Trade Secret Held To Constitute A "Use" Which Justifies $600,000 In Compensatory Damages
  By Paul E. Freehling (February 6, 2012)

- California Federal Court Finds That Plaintiff's Claims Are Not Preempted By The California Uniform Trade Secrets Act In Farmville Spat
  By Scott Schaefers (February 9, 2012)

Trading Secrets

- Protecting Trade Secrets and Confidential Information In The Social Media Generation
  By Robert Milligan (February 12, 2012)

- Click Wrap? Forget It: Federal Court Finds That Violation of Online Clickwrap Agreement Not Enough to Constitute Trade Secret Misappropriation Under California Law
  By Scott Schaefers (February 17, 2012)

- Solar Panel Rivals In Trade Secret and Data Theft Spat In California Federal Court
  By Jessica Mendelson (February 18, 2012)

- California Federal Court Hammers Defendant For Destroying Evidence In Trade Secret Rift
  By Vincent Smolczynski (March 2, 2012)

- Virginia Supreme Court Issues Important Trade Secret Decision and Raises Bar for Proving Damages
  By Rebecca Woods (March 7, 2012)

- What Happens in Vegas May Stay in Vegas, But Misappropriation of Trade Secrets and Unauthorized Disclosure of Confidential Information Will Still Land You in Hot Water According To Recent Supreme Court of Nevada Decision
  By James D. McNairy (March 10, 2012)

- Mattel Appeals $310 Million Award in Bratz Case, Argues Trade Secret Counterclaim Was Untimely
  By Joshua Salinas (March 12, 2012)

- UConn is Dancin' for a Third Reason: Its Donor List is a Trade Secret and Exempt from Freedom of Information Act
  By Scott A. Schaefers (March 15, 2012)

- Keep Your Pot of Gold Hidden, Ohio Court Rules Information Posted Online Not Trade Secret
  By Joshua Salinas (March 16, 2012)

- Utah Appellate Court Holds That "Confidential" Price List Is Not A Trade Secret But A Contract Bid Could Be, And Uniform Trade Secrets Act Preempts Common Law Claims Based On Misusing Confidential Information Not A "Trade Secret"
  By Paul E. Freehling (March 21, 2012)

- Denver Club Owner Fails to Bounce His Partner's Trade Secrets Lawsuit for Alleged MySpace Friends Theft
  By Scott A. Schaefers (March 23, 2012)

- Got Forensics? The Use of Digital Forensics in Trade Secret Matters
  By Jim Vaughn (April 2, 2012)

Trading Secrets

- Seventh Circuit Rejects Pool Technology Company's Trade Secrets Claim
  By Scott A. Schaefers (April 4, 2012)

- Massachusetts Appeals Court Affirms Judgment in Breach of Confidentiality Agreement and Unfair Business Practices Action Involving Weapon Designer
  By Erik Weibust (April 5, 2012)

- Law School Exam-Type Trade Secret Complaint Survives a Specific Pleading Challenge in Colorado Federal Court
  By David Monachino (April 24, 2012)

- No Cause of Action Under Georgia's or Utah's Trade Secrets Statutes for Misappropriation of Confidential and Proprietary Information Not Qualifying as Trade Secret
  By Paul D. Freehling (April 25, 2012)

- Parties In High Profile Sports Agent Dispute In California Involving Trade Secret and Non-Compete Issues Throw Off The Gloves
  By Jessica Mendelson (April 26, 2012)

- Illinois Federal Court Limits Discovery of IP Address Identification Information from ISPs in John Doe Actions: Highlights Continuing Challenge of Identifying Anonymous Posters Of Trade Secrets and Other Intellectual Property On Internet
  By Robert Milligan (April 27, 2012)

- In a Case of First Impression, a New York State Court Requires Specific Pleading of a Trade Secret Cause of Action Before Proceeding with Discovery
  By David Monachino (May 3, 2012)

- April Fools' Day Prank Leads To Trade Secrets Litigation
  By Paul E. Freehling (May 7, 2012)

- California Federal Court Transfers Trade Secret Dispute Involving High-Tech Gloves To New York
  By Robert Milligan (May 9, 2012)

- North Carolina Federal District Court Confirms Importance of Alleging Actual Harm in Pleadings
  By Jessica Mendelson (May 10, 2012)

- Trade Secret Theft Prosecution Cases In The News
  By Justin K. Beyer (May 16, 2012)

- Another Federal Court Holds That A Compilation Of Non-Trade Secret Data Can Be A Trade Secret; Court Also Holds That An Unambiguous Written Contract With A Provision Precluding

Unwritten Amendments Nonetheless Can Be Modified By Conduct
By Paul E. Freehling (May 17, 2012)

- The Use of Digital Forensics in Trade Secret Matters (Part 2 of 3)
  By Jim Vaughn (May 23, 2012)

- California Federal District Court Examines Personal Jurisdiction Issue in International Trade Secret Misappropriation and Breach of Contract Dispute and Maintains Suit Brought Against Irish Company and Owner
  By Robert Milligan (May 27, 2012)

- Federal Judge In California Holds That Unauthorized Use Of Copyrighted Password-Protected Computer Diagnostic Software Can Be The Basis Of A Copyright Infringement Suit and Trade Secret Misappropriation Claim
  By Paul E. Freehling (May 31, 2012)

- You Think Trade Secrets Are Important? So Does the FBI
  By James D. McNairy (June 1, 2012)

- New Hampshire Federal District Court Broadly Interprets Preemption Provision In State's Uniform Trade Secrets Act
  By Ryan Malloy (June 7, 2012)

- Virginia Supreme Court Muddies Damages Valuation of Lost Goodwill In Trade Secret Matter
  By Rebecca Woods (June 18, 2012)

- California Federal District Court Issues Decision On Reasonable Secrecy Measures, Trade Secret Identification, and Preemption
  By James D. McNairy (June 19, 2012)

- Five Practical Guidelines on PROTECTING YOUR GREAT BUSINESS IDEA
  By Joren De Wachter (June 20, 2012)

- Massachusetts Federal Court Rejects Expansive View of Inevitable Disclosure Doctrine and Denies Preliminary Injunction
  By Ryan Malloy (June 22, 2012)

- California Federal District Court Finds That Plaintiffs May Assert A Claim For Alleged Misleading Actions of Agent and Misuse of Confidential Information Not Rising To Level Of A Trade Secret In Youth Hostel Dispute
  By Robert Milligan (June 26, 2012)

- NLRB Continues To Crack Down On Employer Social Media Policies and Continues to Leave Doubt On What Provisions Designed To Protect Trade Secrets and Confidential Information

Will Withstand Its Scrutiny
By Jessica Mendelson (June 28, 2012)

- Missouri Federal Court Denies Summary Judgment Motion Finding Disputed Issue On Whether Trade Secret Exists Notwithstanding Lack of Confidentiality Agreements and Partial Disclosure to Copyright Office
  By Paul E. Freehling (July 17, 2012)

- Legal Standards For Evaluating A Petition To Award Attorneys' Fees To A Defendant In A Trade Secret Misappropriation Case
  By Paul E. Freehling (July 18, 2012)

- Nevada Federal Court Rules That Plaintiff Must Identify Trade Secrets With Specificity Before Serving Discovery
  By Jessica Mendelson (July 25, 2012)

- Considerations In Determining Whether To Grant To A Prevailing Trade Secret Misappropriation Plaintiff A Permanent Injunction In Addition To Substantial Damages
  By Paul E. Freehling (August 7, 2012)

- Indiana Federal Court Holds That A Confidentiality Agreement Without Any Limitations Violates Indiana Law And That A Suit For Misappropriation Cannot Be Brought By A Plaintiff Who Uses A Trade Secret With Permission But Does Not Own It
  By Paul E. Freehling (August 8, 2012)

- Ninth Circuit Issues Opinion Vacating Arizona Jury's Misappropriation Damages Award Because Plaintiff Failed To Apportion Between Confidential Profit Margin And Expense Rate Information And Other Non-Trade Secret Information
  By Paul E. Freehling (August 17, 2012)

- Manhattan District Attorney Considers Formal Charges Against Computer Programmer For Alleged Theft of Confidential Trading Codes
  By Jessica Mendelson (August 18, 2012)

- Indiana Appellate Court Finds That Indiana Uniform Trade Secrets Act Preempts Common Law Misappropriation and Civil Conversion Claims In Mixed Martial Arts Broadcasting Dispute
  By Ryan Malloy (August 20, 2012)

- Facebook Fans For Piggy Paint Not A Business Expectancy, Michigan Federal Court Dismisses Tortious Interference Claims for Facebook Page Takedown
  By Joshua Salinas (August 22, 2012)

- Alabama Federal Court Issues Decision Regarding Measuring The "Amount In Controversy" When The Plaintiff's State Court Trade Secret Misappropriation Complaint Is Silent As To The

Amount Of Damages And The Defendant Removes The Case To Federal Court
By Paul E. Freehling (August 23, 2012)

- Using the International Trade Commission to Address Trade Secret Misappropriation Occurring Abroad
  By Matthew Werber (August 24, 2012)

- Protecting Disclosure Of Trade Secrets Included In A Bid Responsive To A Government Request For Proposal
  By Paul E. Freehling (August 25, 2012)

- Alleged Breach of Non-Disclosure Agreement Related To 3-D Technology At Issue In New California Suit Involving Hollywood Heavyweights
  By Jessica Mendelson (August 26, 2012)

- When the Government Wants Trade Secrets: Presenting a Shield-or-Disclose Framework
  By Elizabeth Rowe (August 29, 2012)

- Extraordinary 20-Year Global Injunction For "Bulletproof" Trade Secrets Theft
  By Joshua Salinas (August 31, 2012)

- "Prior Restraint" Doctrine May Preclude Enjoining A Newspaper From Publishing Misappropriated Trade Secrets
  By Paul E. Freehling (September 3, 2012)

- The Use of Digital Forensics in Trade Secret Matters (Part 3 of 3)
  By Jim Vaughn (September 5, 2012)

- When Everything Becomes Software, How Does That Affect IP Strategy?
  By Joren De Wachter (September 8, 2012)

- Religious Organization's Trade Secret Misappropriation Claim Against Anonymous Blogger Survives Anti-SLAPP Motion to Strike In California Federal Court
  By Robert Milligan and Joshua Salinas (September 9, 2012)

- Despite Allegations That Something Fishy Was Occurring, Kentucky Federal District Court Rules That Texas Corporate Defendant Was Not Subject To Personal Jurisdiction In Trade Secret Misappropriation Suit
  By Paul E. Freehling (September 21, 2012)

- If Confidential Information Constituted A Trade Secret On The Date It Was Misappropriated, The Misappropriation Is Actionable
  By Paul E. Freehling (October 4, 2012)

Trading Secrets

- The Trade Secret Is In the Swirl Cupcake: Bakery Sues To Protect Its Signature Icing Topping
  By James Yu (October 5, 2012)

- Florida Court Rejects Argument That Plaintiff Must Make "Threshold Finding" of Trade Secret Before Proceeding With Discovery
  By Joshua Salinas (October 10, 2012)

- Trade Secret Lawsuit Filed Against Heavy Metal Band Regarding "Drum Set Loop Coaster"
  By Joshua Salinas (October 17, 2012)

- Sports Agent Non-Compete and Trade Secrets Dispute Heats Up in California
  By Robert Milligan and Jessica Mendelson (October 19, 2012)

- Zynga Sues Former Employee For Trade Secret Theft While Defending Its Acquisition Of Other Alleged Proprietary Information
  By Jason Stiehl (October 29, 2012)

- Royalties Awarded for Theft of Skycam Trade Secrets
  By Joshua Salinas (October 30, 2012)

- Mobile Game Rivals Clash In California Trade Secret and Unfair Competition Suit
  By Jason Stiehl (November 14, 2012)

- Breach of Fiduciary Duty and Trade Secret Misappropriation Alleged In "Preppy Clothing Dispute" Involving Fashion Designer Tory Burch
  By Jessica Mendelson (November 23, 2012)

- California Federal Court Finds Arbitration Agreement's Exclusion of Injunctive Relief for Trade Secrets and Unfair Competition Claims Is Not Unconscionable
  By Joshua Salinas and Grace Chuchla (November 29, 2012)

- Former PhoneDog Employee Off the Hook in Closely Watched Trade Secrets Spat
  By Jessica Mendelson and Joshua Salinas (December 5, 2012)

- NBA Sports Agent Slams Non-Compete and Trade Secret Claims and Scores 85K Jury Verdict Against Former Agency For Privacy Violation
  By Robert B. Milligan and Jessica Mendelson (December 7, 2012)

- $4.38 Million Verdict In Utah Federal Court For Malicious Trade Secrets Misappropriation
  By Paul E. Freehling (December 11, 2012)

- Ninth Circuit Hears Oral Argument in Rival Toy Makers' Trade Secrets Dispute
  By Joshua Salinas (December 12, 2012)

Trading Secrets

- Wisconsin Federal Court Finds That Common Law Claims Are Preempted by the California Uniform Trade Secrets Act
  By Daniel Hargis (December 13, 2012)

- Tidings of Data Theft and Coal: California Federal Court Holds That Trade Secret Misappropriation Statute Preempts Claim for Misappropriation of Confidential Non-Trade Secret Data
  By Paul E. Freehling (December 24, 2012)

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
  By Scott Schaefers (January 5, 2012)

- Waiting On Nosal...Combating Data Theft Under The Computer Fraud and Abuse Act In The Ninth Circuit
  By Robert Milligan (February 20, 2012)

- California Federal Court Grants Summary Judgment For Facebook On Its CAN-SPAM Act, Computer Fraud and Abuse Act, And Penal Code Section 502 Claims Against Social Media Aggregator
  By Robert Milligan (February 29, 2012)

- Colorado Federal Court Rules That Former Employer Stated A Claim Against Former Executive and His New Employer Under The Computer Fraud Abuse and Act Regardless Of Differing Circuit Interpretations Of The Act
  By Robert Milligan (March 9, 2012)

- Minnesota District Court Dismisses Computer Fraud and Abuse Act Claim Brought Against Former Employee Based Upon Narrow Interpretation Of Act
  By Robert Milligan and Joshua Salinas (March 21, 2012)

- Ninth Circuit En Banc Panel Tells Employers That Computer Fraud and Abuse Act Is Only To Combat Hacking, Not Employee Trade Secret Misappropriation: United States Supreme Court May Need To Resolve Circuit Split
  By Robert Milligan (April 20, 2012)

- New York Federal District Court Strikes Down Application of the Computer Fraud and Abuse Act to ISP Throttling Case
  By Robert Milligan (April 26, 2012)

Trading Secrets

- *US v. Nosal* Update: Solicitor General and DOJ Still Deciding Whether To File Writ Of Certiorari With United States Supreme Court
  By Robert Milligan (May 9, 2012)

- Michigan Federal Court Adopts Narrow Interpretation of Civil Liability Under Computer Fraud and Abuse Act
  By Robert Milligan (May 30, 2012)

- *U.S. v. Nosal* Update: Solicitor General Still Deciding Whether To Seek Supreme Court Review of Important Ninth Circuit Computer Fraud and Abuse Act Decision
  By Robert Milligan (July 12, 2012)

- Another Michigan Federal Court Adopts Narrow Interpretation of Civil Liability Under Computer Fraud and Abuse Act
  By Paul E. Freehling (July 24, 2012)

- Solicitor General Decides Not To File Petition For Review In *United States v. Nosal*: Circuit Split On Computer Fraud And Abuse Act Remains
  By Robert Milligan and Joshua Salinas (August 3, 2012)

- Employers Beware: Fourth Circuit Adopts Narrow Interpretation of Computer Fraud and Abuse Act
  By Jessica Mendelson (August 6, 2012)

- California Federal District Court Distinguishes Ninth Circuit's Nosal Decision and Finds that Computer Fraud and Abuse Act Claims Are Available for Violations of Employers' "Access" Restrictions
  By Joshua Salinas (August 14, 2012)

- Federal Court Clerk Arrested For Allegedly Sharing Confidential Information With Gangs
  By Jessica Mendelson (August 28, 2012)

- Update: California Federal District Court Reaffirms that Computer Fraud and Abuse Act Claims are Available for Violations of Employers' "Access Restrictions" Despite Ninth Circuit's Nosal Decision
  By Joshua Salinas (September 13, 2012)

- "Click Fraud" Allegations Found Insufficient Under Computer Fraud and Abuse Act, But Personal Jurisdiction Found Where Defendant Company's Website Deliberately Targeted Consumers Within the Forum State
  By Joshua Salinas and Jessica Mendelson (September 19, 2012)

- New Federal Legislation Proposed To Amend Computer Fraud and Abuse Act To Address Unauthorized Cloud Computing Activities
  By Jessica Mendelson (October 9, 2012)

Trading Secrets

- Pennsylvania Federal Court Dismisses Employee's Computer Fraud and Abuse Act Claim Based Upon Employer's Alleged Improprer Access of LinkedIn Account: No Cognizable Damages
  By Jessica Mendelson and Robert Milligan (October 12, 2012)

- Hacking Into Personal E-Mail Account Not a Violation of the Stored Communications Act According to South Carolina Supreme Court
  By Molly Joyce (October 23, 2012)

- Employer Petitions U.S. Supreme Court to Resolve Computer Fraud and Abuse Act Circuit Split
  By Robert Milligan and Joshua Salinas (November 2, 2012)

- Plaintiffs Retain Home Field Advantage in Email Hacking Action But Nebraska Federal Court Dismisses Computer Fraud and Abuse Act Claim
  By Marcus Mintz (November 13, 2012)

- Arizona Federal Court Issues Significant Computer Fraud and Abuse Act and Trade Secret Preemption Decision
  By Paul E. Freehling (November 26th, 2012)

- Mississippi Federal District Court Allows Computer Fraud and Abuse Act Claim to Proceed Against Former Employee
  By Jessica Mendelson (December 18, 2012)

- Virginia Federal Court Finds For Employer on Fidicuary Duty Claim Against Former Employee
  By Michael Baniak (December 19, 2012)

Non-Competes & Restrictive Covenants

- Pennsylvania Federal Court Salvages Customer Lists as Basis for UTSA Claim, But Shreds Liquidated Damages Provision and Rejects Fiduciary Claim
  By Rebecca Woods (February 3, 2012)

- New York Federal Court Finds That Anti-Raiding Clause Is Subject to Rule of Reasonableness Under New York Law
  By David Monachino (February 7, 2012)

- Illinois Appellate Court Holds That Illinois Supreme Court Non-Compete Decision In Reliable Fire Applies Retroactively
  By Jessica Mendelson (February 11, 2012)

Trading Secrets

- Oregon Federal Court Permits Declaratory Relief Suit To Proceed In Race To Judgment Non-Compete Dispute
  By Robert Milligan and Joshua Salinas (February 13, 2012)

- Former Pharmacy Benefit Management Executives Sued For Alleged Violations Of Customer Non-Solicitation Agreements In Wisconsin Federal Court
  By Justin Beyer (February 15, 2012)

- A New York Court Holds that Employee Choice Doctrine Does Not Apply to Equitable Relief in a Non-Compete Matter
  By David Monachino (March 2, 2012)

- New Ninth Circuit Case Aids Departing Employees In Non-Compete and Non-Solicit Disputes Involving Race To Judgment
  By James D. McNairy (March 5, 2012)

- Massachusetts Court Finds IT Consultant's Non-Compete Agreement Unenforceable Due to "Material Change" in Employment Relationship
  By Kate Perrelli, Erik Weibust, and Ryan Malloy (March 6, 2012)

- California Federal Court Ships California Employee's Declaratory Relief Action Seeking To Invalidate His Non-Compete To Pennsylvania
  By Jessica Mendelson (March 8, 2012)

- Texas Appellate Court Voids, As Contrary to Fundamental Texas Law, Incentive Compensation Contract Imposing A Substantial Penalty For Post-Employment Competition With The Ex-Employer
  By Paul Freehling (March 13, 2012)

- Fireworks Fly, California District Court Enjoins Former Pyrotechnics Company Employee From Soliciting Former Employer's Customers
  By James D. McNairy (March 30, 2012)

- For Whom the Employment Agreement Tolls: New York State Appellate Court Applies Equitable Tolling Doctrine In Non-Compete Dispute
  For David Monachino (March 31, 2012)

- Employer Who Sued Former Employees to Enforce Non-Competition Clauses Did Not Violate Indiana's Blacklisting Statute
  By Paul Freehling (April 3, 2012)

- Colorado Federal Court Decision In Non-Compete Dispute Demonstrates Importance Of Drafting Enforceable Forum Selection Provisions In Business Transactions
  By Robert Milligan (April 6, 2012)

Trading Secrets

- Sale of Business "Good Will" and Subsequent Competition with Purchaser May Subject Seller to Perpetual Restrictions on Contacting Former Customers and Clients
  By Paul Freehling (April 12, 2012)

- Washington Appellate Court Finds That Employer's Threatening Letter, Relying In Part On Inevitable Disclosure Doctrine, to Former Employee's Prospective Employer Is Not Actionable
  By Jessica Mendelson (June 16, 2012)

- New Hampshire Enacts New Law Requiring Disclosure of Non-Compete and Non-Piracy Agreements Prior To Job Offer And Change In Job Classification
  By Ryan Malloy and Robert Milligan (June 17, 2012)

- A Business Entity That Changes Its Corporate Structure Risks Expiration Of Its Employees' Covenants-Not-To-Compete And Confidentiality Agreements
  By Paul E. Freehling (June 25, 2012)

- Delaware Chancery Court Rules That Former Employees Are Not Indispensable Parties in Non-Compete Case
  By Ryan Malloy (July 22, 2012)

- Nevada Attorney General and FTC Scrutinize Nevada Healthcare Company's Alleged Anti-Competitive Behavior Concerning Use of Non-Compete Agreements
  By Jessica Mendelson (August 15, 2012)

- Texas Federal Courts Reach Differing Conclusions On Granting Injunctive Relief On Close To Expiring Or Expired Non-Competes: Some Courts Elect To Equitably Extend Covenants
  By Paul E. Freehling (August 19, 2012)

- Missouri Supreme Court Reaffirms That Missouri Is A Pro Non-Compete Jurisdiction, Enforcing Non-Competition and Modified Non-Solicitation Agreements Against Non-Resident Former Security Company Employees
  By Robert Milligan and Grace Chuchla (August 21, 2012)

- California Court Of Appeal Finds That Non-Competition Agreement Contained In Employment Agreement Is Unenforceable Against Former Seller/Employee Even Though It Was Executed In Connection With The Sale Of A Business
  By Robert Milligan and Joshua Salinas (August 27, 2012)

- Kentucky Appellate Court Affirms Authority of Kentucky Courts to Modify Overly Broad Non-Competition Agreements in the Employment Context and Sets Forth "Guiding Principles" for Future Non-Compete Cases
  By Robert Milligan and Grace Chuchla (September 6, 2012)

Trading Secrets

- Connecticut Federal Court Finds That Non-Competition Covenant Which Is Silent Regarding Assignability May Be Enforceable Depending Upon the Parties' Intent Under New York Law
  By Paul E. Freehling (September 7, 2012)

- California Federal Court Boots Employee's Challenge Of His Non-Compete Because Of Pennsylvania Forum Selection Provision
  By Robert Milligan and Grace Chuchla (September 27, 2012)

- Ignorance Isn't Always Bliss: What to Do When Your Job Candidate Isn't Sure if She Is Bound By A Non-Compete
  By Molly Joyce (September 28, 2012)

- Can an Employer Enforce a Non-Compete Agreement That It Forgot to Sign? Perhaps Not In Texas
  By Randy Bruchmiller (October 3, 2012)

- California Appellate Court Holds That Non-Compete Restriction in Stipulated Injunction Is Enforceable Because There Was No Showing That It Was Not Necessary to Protect Trade Secrets
  By Joshua Salinas and Robert Milligan (October 11, 2012)

- Are Non-Competition And Non-Solicitation Provisions In An Employment Agreement Enforceable Despite The Absence Of Compensable Damages?
  By Paul E. Freehling (October, 15, 2012)

- "Gist Of The Action" Doctrine May Require Dismissal Of Tort Claims Based On Breach Of Restrictive Covenants In Employment Agreement
  By Paul E. Freehling (October 18, 2012)

- Paramedics Defeat Noncompete and Customer Nonsolicit Preliminary Injunction on Grounds of Potential Harm to Public and Paramedics
  By Paul E. Freehling (October 24, 2012)

- Speculative Fears Insufficient for Non-Compete Temporary Restraining Order Against Former Employee
  By Paul E. Freehling (October 31, 2012)

- Illinois Supreme Court Affirms Liability Against Former Employer For Unlawful Investigation Methods Used By Private Investigators In Non-Competition Investigation Into Activities By Ex-Sales Agent
  By Marcus Mintz (November 21, 2012)

- Employers Thanful for New Second Circuit Non-Compete Decision
  By Jessica Mendelson (November 22, 2012)

- Massachusetts Court Rules That Facebook Posting of New Job Does Not Violate Non-Competition Covenant
  By Paul E. Freehling (November 30, 2012)

- New York Federal Court Rejects Heightened Specificity Pleading Standard for Breach of Confidentiality and Non-Disclosure Claim
  By Joshua Salinas and Jessica Mendelson (December 4, 2012)

- US Supreme Court Strikes Down Oklahoma Supreme Court Decision And Holds That Arbitrator, Rather Than Court, Must Determine the Enforceability of Non-Compete Agreements Containing Arbitration Provisions
  By Robert B. Milligan and Grace Chuchla (December 5, 2012)

Legislation

- At Long Last, New Jersey Passes Trade Secrets Act
  By David Monachino (January 9, 2012)

- Virginia Bill Proposes to Ban Most Non-Competes
  By Rebecca Woods (January 30, 2012)

- New Jersey Adopts New Jersey Adopts Variation of Uniform Trade Secrets Act
  By Robert Milligan (February 3, 2012)

- Idaho and New Hampshire Propose Significant Trade Secret and Non-Compete Legislation
  By Jessica Mendelson (March 22, 2012)

- Access To Social Media Accounts In The Hiring Process And Employer Ownership Of Trade Secrets Or Confidential Information Contained In Social Media Accounts: Legislation On Horizon?
  By Jessica Mendelson (April 4, 2012)

- Hey Lumbergh, You Don't Own My Facebook Account: Maryland Passes Legislation To Protect Employee's Social Media Accounts
  By Jessica Mendelson (April 18, 2012)

- Massachusetts Legislature Considers New Social Media Bill
  By Ryan Malloy and Erik Weibust (May 1, 2012)

- Georgia's New Restrictive Covenant Act Turns One Year Old
  By Daniel Hart and Bob Stevens (May 14, 2012)

- New Federal Trade Secrets Legislation Proposed
  By Jessica Mendelson and Robert Milligan (July 19, 2012)

Trading Secrets

- Illinois Becomes Second State In Nation To Bar Employers From Obtaining Access To Employee Social Networking Pages
  By Ronald Kramer (August 16, 2012)

- Proposed Social Media Legislation On California Governor's Desk
  By Jessica Mendelson and Grace Chuchla (September 26, 2012)

- California Governor Jerry Brown Signs New Social Media Legislation
  By Robert B. Milligan (September 27, 2012)

- Failed Federal Cybersecurity Act May Emerge In Executive Order
  By Misty Blair (October 1, 2012)

- What Employers Need to Know About California's New Social Media Law
  By Robert Milligan, Jessica Mendelson, and Joshua Salinas (October 2, 2012)

- Update on Proposed Massachusetts Non-Compete and Trade Secret "Reform" Legislation
  By Ryan Malloy and Erik Weibust (November 5, 2012)

- On Election Day, Cybersecurity Is A Part Of Candidates' Platforms
  By Misty Blair (November 6, 2012)

- Cybersecurity Act of 2012 Dies Again in the Senate
  By Misty Blair (November 16, 2012)

- United States Senate Unanimously Approves the Theft of Trade Secrets Clarification Act
  By Jessica Mendelson (December 3, 2012)

- Big Brother Can't Ask For Access To Your "Personal" Social Media Accounts Either….More Social Media Legislation Proposed In California
  By Robert B. Milligan and Jessica Mendelson (December 11, 2012)

- US House of Representatives Passes Theft of Trade Secrets Clarification Act
  By Robert Milligan and Jessica Mendelson (December 18, 2012)

- President Obama Signs Trade Secrets Clarification Act and House of Representatives Considers Enhancing Economic Espionage Act Penalties
  By Robert Milligan (December 31, 2012)

2012 Summary Posts

2012 Trade Secrets, Computer Fraud, and Non-Competes Webinar Series – Year in Review

By Robert B. Milligan (December 20, 2012)

Throughout 2012, 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 eight webinars:

1) Employee Privacy, Social Networking at Work, and the Computer Fraud and Abuse Act Standoff;
2) Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing;
3) Pleading, Providing and Protecting Trade Secrets in Litigation;
4) Protecting Your Trade Secrets in the Financial Services Industry;
5) When Trade Secrets Cross International Borders;
6) Trade Secrets and Non-Compete Legislative Update;
7) Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours; and
8) 2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law.

As a conclusion to this well-received 2012 webinar series, we 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 CD upon request or you may click on the title below of each webinar for the online recording. CLE credit is available as discussed below. We are also pleased to announce that Seyfarth will continue its trade secrets webinar programming in 2013 and has several exciting topics lined up. We will release the 2013 trade secrets webinar series in the coming weeks.

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

The first webinar of the year, led by Seyfarth partners Gary Glaser and Scott Schaefers, addressed the issue of employees' privacy rights on their work computers; unauthorized use or disclosure of company intellectual property while using social media; and the Computer Fraud and Abuse Act (CFAA).

- To have the best chance of seeking remedies under the federal CFAA, only give employees access to company networks on a need-to-know basis. Require all employees with access to confidential company information to sign confidentiality and restricted access and use agreements. Have clear written policies in place that leave no doubt that any access and use of company information, for purposes other than company business, is strictly prohibited, and have employees acknowledge receiving copies of such policies. Send out periodic reminders of those policies, each of which should require acknowledgement of receipt by the employees.

- Do NOT attempt to access an employee's personal e-mails, files or Internet accounts without advice of counsel. Under both federal and many state laws, employees often have privacy rights in their personal information, even if they store it or access it on company computers.

- For social networking sites (e.g., LinkedIn), have clear written policies that spell out what company information may/may not be posted on such sites, and identify what information belongs to the company (e.g., contact lists, company photos or graphics, etc.), as well as a process for purging the company-owned information from their contact lists posted on social networking sites such as LinkedIn at the time the employee departs. An exit interview should also be conducted at the time any employee separates, and as part of that exit interview process, each exiting employee should be given a written reminder of their ongoing trade secret, confidentiality and social networking obligations. If an employee leaves the company without such clear written direction, the company risks waiving any proprietary interest in the information in his/her LinkedIn profile. Also consider using ownership agreements that specify that the company owns the particular social media accounts that the employee may work on and remember to obtain the password from the employee to the company owned social media account before the employee leaves.

Employee Theft of Trade Secrets or Confidential Information in The Name of Protected Whistleblowing

In our second webinar of the series, Seyfarth partner Robert Milligan answered the question, "Can employees steal trade secrets and confidential information to support their whistleblower claims?" This program covered recent decisions addressing the interplay between maintaining employer confidentiality and protection of trade secrets and protected activity under whistleblower statutes and "self-help" discovery, as well as the provisions in whistleblower bounty programs that preclude enforcement of confidentiality agreements in certain instances.

- A central goal of Sarbanes-Oxley is the accurate valuation and protection of a company's assets. But what does this mean for trade secrets, which have traditionally been thought of as an undefined intellectual property right? Sarbanes-Oxley has mandated duties of disclosure and internal controls that have transformed trade secrets into an asset that must be valued and reported.

- At a minimum, companies should create a trade-secret protection committee or have a corporate officer whose job it is to identify, value, and protect trade secrets. However, doing so requires an understanding of 1) what a trade secret is, 2) where one finds a trade secret, and 3) how to

appropriately protect a trade secret. The key is to identify, inventory and value as well as institute internal controls to protect trade secrets. Seyfarth has extensive experience assisting companies with this process and offers an effective and well-received trade secret audit program.

- Section 922 of the Dodd-Frank Act prevents any person from interfering with a whistleblower's report, including by threatening to enforce confidentiality agreements. Whistleblower thieves may seek revenge by making confidential information public in addition to bringing it before the SEC. Companies must act swiftly to have genuine confidential or trade secret information removed from public mediums, such as the Internet, to attempt to preserve its secrecy. New whistleblower rules may decrease incentives to follow internal reporting procedures and instead provide a perverse incentive for sham employees to work for bounties rather than fulfill their employment obligations. Careful planning should be done to make good hiring decisions as well as employing effective performance management of existing hires to attempt to manage the risk of the retention of rogue and disloyal servants.

- Consider these strategies to protect trade secrets and confidential information when faced with a whistleblower thief:

    - Make sure you have a clear anti-retaliation policy and document investigation. Follow your corporate compliance programs and ethics policies and procedures.
    - Be careful in all communications with the whistleblower. Do not make him or her feel threatened. Try to find an employee that the whistleblower thief trusts to get back company documents.
    - Consider engaging a third-party neutral to maintain confidential documents and information if the whistleblower has not yet gone to the SEC.
    - Consider amnesty negotiations. Remind the whistleblower of the serious legal consequences of stealing trade secret and confidential information.
    - Offer to study the problem internally and report to the SEC.
    - Move swiftly to attempt to obtain the removal of any confidential or trade secret documents from the Internet by working with Internet service providers to obtain the immediate takedown and involve the court as needed.

Pleading, Proving and Protecting Trade Secrets in Litigation

The third installment in the 2012 Trade Secrets Webinar Series was presented by trade secrets practice leader Michael Wexler. Many courts require that claims for trade secret misappropriation be pled specifically as to the nature of the trade secret or suffer the consequences of challenges to the pleadings. The challenge is to plead with reasonable particularity without actually disclosing the secrets in a public document. From a defense stand point, the identity of the trade secret is paramount to prepare defenses, determine the value of the secrets, and determine if they were actually

misappropriated. This webinar covered the ethical, technical and practical aspects of initial pleadings that are fundamental to the filing and defending of trade secret claims.

- In any trade secrets litigation in which you represent the plaintiff, you must have a frank discussion with your client prior to the inception of the litigation concerning its duties to identify the alleged misappropriated trade secrets with specificity and the resulting discovery disclosure that will be required in the litigation. Simply put, the client needs to know that counsel for the defendant(s) (at a minimum) will be provided access to the allegedly purloined trade secret as well as others. Depending upon the state and occasionally the individual judge, the defendants may also be able to obtain access to the stolen trade secrets subject to a protective order so that they can defend themselves against the claim. A plaintiff must be mindful that their secrets may be further disclosed to a competitor during trade secret litigation subject to non-disclosure obligations and that plaintiff must vigorously defend and protect the confidentiality of said information throughout the litigation.

- A majority of states either by statute or case law require that a plaintiff disclose their trade secrets with specificity as part of the discovery process. Failure by the plaintiff to provide sufficient specificity regarding the stolen trade secret in discovery may result in a defendant obtaining summary judgment on the claim. Some states require the plaintiff to provide a specific trade secret disclosure document before discovery commences. See California Code of Civil Procedure section 2019.210.

- Protective orders in trade secret litigation must be carefully tailored to protect confidential information disclosed in discovery and limit the disclosure of such information to those who need to know for purposes of the litigation. A protective order should have appropriate measures concerning how documents containing confidential information will be provided to the court, witnesses, and experts. Careful consideration should also be made on whose burden it is to justify the protection level assigned to particular documents.

- Plaintiffs should use contention interrogatories to flesh out any allegations made by the defendant(s) that particular alleged trade secrets are in the public domain. Written discovery should probe the basis of such allegations, including when and where such disclosure occurred.

Protecting Your Trade Secrets in the Financial Services Industry

The fourth webinar in the series, presented by partners Scott Humphrey and James McNairy, focused on trade secret considerations in the banking and finance industry, including prosecuting claims against former employees who are FINRA members.

- When seeking injunctive relief in a trade secrets dispute involving parties that are subject to FINRA regulation, be sure to first consult FINRA (NASD) Rule 13804 governing injunctive relief—while the moving party may first seek injunctive relief from a court of competent jurisdiction, the party must also make specified filings with FINRA.

- When litigating a trade secret dispute before FINRA, keep in mind that the FINRA process is often less formal than in court, and the arbitration panel may include persons who are not lawyers. Thus,

it behooves both parties to keep their legal arguments concise and, where complex trading algorithms or other complex trade secrets are at issue, the trade secret should be described as simply as possible.

- When the FINRA trade secret dispute arises out of facts involving broker recruitment, the parties should be aware of the 2004 "Protocol for Broker Recruiting," which currently has well over 400 signatories and allows brokers to take to their new employer certain account information. Other limitations within the protocol should also be carefully considered before filing suit.

When Trade Secrets Cross International Borders

Our fifth webinar in the 2012 series was presented by Robert Milligan, Marjorie Culver and Matthew Werber and provided a high-level discussion of recent non-compete and trade secret issues that impact foreign companies conducting business in the United States and companies operating internationally. This program provided an overview of the key considerations that foreign companies should appreciate in order to effectively navigate trade secret and non-compete law in the U.S. and highlighting the issues facing U.S. trade secret owners attempting to address the theft of stolen trade secrets abroad. This webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these jurisdictions to ensure they are adequately protecting their trade secrets.

- In many U.S. states, initial employment and continued employment can be sufficient consideration for non-compete, non-solicitation and non-disclosure agreements, whereas in several European countries, the employer must pay for any post-termination non-compete. In contrast to the law in some foreign countries, employers can still enforce the non-compete even if the employer terminates the employment relationship in some U.S. states. Injunctive relief is typically the top litigation goal in most U.S. trade secret/non-compete matters. There are significant differences in U.S. states concerning the interpretation of the Uniform Trade Secrets Act (which has been adopted in 46 U.S. States). For example, there are significant differences regarding the application of the inevitable disclosure doctrine, trade secret preemption and recoverable damages.

- Cross-border considerations: employers must be vigilant and think critically about the most likely venue that a non-compete/trade secret battle will occur should an employee later leave the company as forum and choice of law can be outcome determinative. Employers should carefully select employees for cross-border coverage, taking into consideration where the work will likely be performed, where the employee will likely reside, what jurisdiction/choice of law is most favorable, and the likely chance of successful enforcement. The employer should draft to the highest standard based upon the likely locale of any dispute concerning the non-compete.

- Trade secret holders seeking to remedy misappropriation occurring abroad should consider the United States International Trade Commission (ITC) as a potential forum for seeking relief. In TianRui Group Co., Ltd. v. ITC, 661 F.3d 1322 (Fed. Cir. 2011), the Federal Circuit ruled that the

ITC can exercise its jurisdiction over acts of misappropriation occurring entirely in China so long as the dispute concerns products being imported into the United States.

Trade Secrets and Non-Compete Legislative Update

The sixth webinar of the year, led by Robert Stevens, Erik Weibust, and Daniel Hart, focused on new and pending legislative changes to non-compete and trade secrets statutes, including a review of Georgia's Revised Restrictive Covenant Act one year after its enactment, recent and pending legislative changes to non-compete statutes in New Hampshire and Massachusetts, adoption of the New Jersey Uniform Trade Secrets Act, and pending legislative changes to trade secrets statutes in Idaho and at the federal level.

- To the extent that they have not already done so, employers operating in Georgia should have their non-compete agreements evaluated by counsel to ensure that they are taking full advantage of the change in Georgia public policy toward enforcement of restrictive covenant agreements, which permits courts to blue pencil overbroad agreements and which only applies to agreements signed after May 11, 2011.

- Employers operating in New Hampshire should ensure compliance with the new statutory requirement of disclosing non-compete and non-piracy agreements to employees prior to making an offer of employment or an offer of change in job classification, while employers operating in Massachusetts should stay abreast of proposed legislation that, if enacted, could make enforcement of restrictive covenants more difficult in Massachusetts. Please see our chart that summarizes the various iterations of the proposed legislation.

- In light of New Jersey's adoption of the Uniform Trade Secrets Act and proposed legislation in Idaho and at the federal level, trade secrets law is slowly moving toward greater uniformity. In light of the continually developing statutory landscape, employers operating anywhere in the United States should continue to ensure that they have taken reasonable measures to protect their trade secrets, by, among other steps, limiting access to trade secrets to employees with a need for such access, providing password protections on documents, encrypting data, limiting the ability of employees to remotely print highly sensitive documents, and enacting vigorous restrictive covenant agreements in jurisdictions where such agreements are permitted.

Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours

The seventh webinar in our series, presented by Michael Wexler, Robert Milligan and Joshua Salinas, discussed best practices when dealing with newly hired or departing employees and the incumbent trade secret, non-competition and information protection issues.

- During the job interview of a competitor's employee, remember to 1) discuss general skills and talents, not the former employer's customers or trade secrets; 2) control the interview and put the employee at ease; 3) make clear that the employee should not, under any circumstances, use or

bring any of his employer's information or solicit any former co-workers; 4) focus on making the transition as smooth as possible for the former employer; and 5) check if the employee has any existing agreements with former employers before making an offer.

- Key agreements/provisions/policies that companies should have with their employees: 1) non-disclosure and trade secret protection agreements; 2) non-solicitation of employee agreements/provisions; as permitted by law 3) agreements/provisions relating to former employer's trade secrets (don't use or disclose and do not bring to premises); 4) computer use and access provisions/agreements; 5) social media ownership agreements and policies; and 6) invention assignment agreements.

- The exit interview process with departing employees is key. Employers should:

    - Prepare for the interview, identify the trade secret and confidential information the employee accessed/used, consider having in-house counsel or HR and employee's manager present
    - Question the departing employee in detail.
    - Ask the employee why he/she is leaving.
    - Ask the employee what his/her new position will be.
    - Check the employee's computer activities and work activities in advance of the meeting.
    - Ensure that all Company property, hardware, and devices have been returned, including e-mail and cloud data, and social media accounts; consider using an inventory list.
    - Ensure that arrangements are made to have all company data removed from any personal devices, accounts, storage areas.
    - Disable access to company computer networks.
    - Make sure you obtain user names and passwords for all company social media accounts.
    - Inform the employee of his continuing obligations under agreements with the Company.
    - Consider letter to new employer and employee with reminder of continuing obligations.
    - Consider having departing employee's emails preserved and electronic devices forensically imaged.
    - Consider using an exit interview certification.

Trading Secrets

2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law

In Seyfarth's final installment of its 2012 Trade Secret Webinar series, Seyfarth attorneys James McNairy, Joshua Salinas and Jessica Mendelson reviewed noteworthy California cases and other legal developments in the increasingly hot areas of trade secret protection, the preemptive effect of the California Uniform Trade Secrets Act, California's hostility to non-competition and non-solicitation agreements, the continued erosion of the Computer Fraud and Abuse Act as a tool for California employers to curb data theft, and social media's influence on how organizations identify and protect confidential information.

- Clearly define company social media policies before problems arise. Avoid restricting employees' abilities to discuss the terms and conditions of their employment, wages, and other activities protected under Section 7 of the National Labor Relations Act. Employers who make use of social media accounts should consider using contracts to state clearly that the employer owns the accounts, which are to be used only for authorized purposes, but that do not overreach into areas that violate employee rights to privacy.

- Companies should ensure their computer and network policies cover "access," not merely "use," to comply with the Ninth Circuit's narrow interpretation of the CFAA. Access should be defined clearly to delineate functionally what computer resources and information employees permissibly may and may not access, with data repositories containing sensitive information requiring enhanced access restrictions.

- To fall under California Business and Professions Code section 16601′s "sale of business" exception, non-competition covenants executed pursuant to the sale of a business should be incorporated into the terms of the purchase agreements and reflect a clear purpose to protect business goodwill.

- Because preemption under California's Uniform Trade Secrets act is increasingly invoked by defendants as a basis to dismiss claims related to the taking of trade secret information, it is imperative that potential plaintiffs carefully plead non-trade secret claims as distinct from the trade secret allegations within the complaint. Failure to do so can cause related claims to be preempted and, if the trade secret claim itself is faulty, significantly reduce the number of at issue claims.

- Create a culture of confidentiality within your company so that at every turn employees are aware of the importance of protecting confidential, proprietary, and trade secret information and the steps required of all employees to protect the company's information assets. Doing so may enable your organization to invoke the trade secrets exception to California Business and Professions Code section 16600, which may help protect company information assets and moderate high employee mobility in California.

Trading Secrets

2013 Trade Secrets Webinar Series

Beginning in January 2013, we will begin another series of trade secret webinars. The first webinar of 2013 will be a national year in review on the most important cases and developments throughout the country concerning trade secrets, non-competes, and computer fraud. 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 attorneys licensed in Illinois, New York or California, who are interested in receiving CLE credit for viewing recorded versions of the 2012 webinars, please e-mail CLE@seyfarth.com to request a username and password. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are also happy to discuss with you presenting similar presentations to your groups for CLE credit.

Trading Secrets

Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2012

By Robert Milligan and Joshua Salinas (January 3, 2013)

As part of our annual tradition, here is our list of the top 10 developments/headlines in trade secret, computer fraud, and non-compete law for 2012.

Last year we predicted that in 2012 we would see a significant increase in social media cases and this year did not disappoint. In fact, we saw several disputes involving the ownership of social media accounts and account "followers" on Twitter, LinkedIn, Facebook and Myspace. We also saw several states enacting legislation to protect employees' "personal" social media accounts and we expect more states to follow next year. In 2013, we expect to see social media continue to generate disputes in trade secret, computer fraud, and non-compete law, as well as in privacy law.

The circuit split regarding the interpretation of what is unlawful access under the Computer Fraud and Abuse Act ("CFAA") continued to widen with the Fourth Circuit and federal district courts in Minnesota and Michigan adopting the Ninth Circuit's narrow interpretation, which significantly limits employers' ability to use the CFAA in typical employee data theft scenarios. A resolution may be soon approaching, however, as a petition for writ of certiorari has been filed with the US Supreme Court on "whether the CFAA applies to employees who violate employer-imposed computer access and data use restrictions to steal company data."

There have also been significant legislative efforts to modify trade secret, computer fraud, and non-compete law in various jurisdictions. In fact, New Jersey adopted a version of the Uniform Trade Secrets Act. President Obama signed into law an amendment to the criminal Economic Espionage Act which closes a loophole in the Act and expands trade secret protections for companies. New Hampshire also adopted notification requirements on the use of non-compete agreements. Massachusetts, Virginia, and Idaho have considered legislation that would provide certain limitations on non-compete agreements or modifications to their trade secret laws. We expect more legislative activity in 2013, particularly regarding social media, privacy, and trade secret legislation to curb foreign trade secret theft.

Finally, government agencies have become more active, such as the FBI's recent initiative to curb the growing rise of trade secret and other intellectual property theft and some high profile prosecutions under the Economic Espionage Act and the National Labor Relations Board's increased scrutiny of employers' social media policies. We expect more government activity in 2013.

Trading Secrets

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 enforceability of non-compete agreements or other significant trade secret/data theft issues. In a rare procedural move, the Ohio Supreme Court reconsidered and reversed its prior decision in a post-merger non-compete case and held that non-competes are like any other agreement and automatically transfer to the surviving entity after a merger. The Nevada Supreme Court recognized for the first time (although implicitly) that restrictive covenants may be enforceable against independent contractors. The Indiana Supreme Court rejected one of its century-old decisions and held that filing a lawsuit to enforce a non-compete agreement does not violate the state's blacklisting statute. The Missouri Supreme Court reaffirmed that Missouri is a pro-non-compete jurisdiction when it enforced non-compete and modified non-solicit agreements against non-resident former security company employees. Recognizing the trend across Illinois appellate courts in recent years, the Illinois Supreme Court joined the "vast majority of other jurisdictions" in recognizing the tort of intrusion upon seclusion in a case involving a former employer's unlawful investigation methods into the activities of an ex-sales agent bound by a non-compete.

The South Carolina Supreme Court found that a defendant who allegedly hacked into a plaintiff's personal e-mail account to retrieve messages that were already read by the plaintiff was not liable under the Stored Communications Act. The South Carolina Supreme Court also held that holdover clauses in invention assignment agreements were not restraints of trade subject to the traditional three-part "rule of reason" standard analyzing the enforceability of non-competes. The Virginia Supreme Court issued two important trade secret decisions: one that raised the bar for proving damages and another that complicated the valuation of lost goodwill damages. The Ohio Supreme Court also affirmed in large part an Ohio jury's award of $26.5 million for unfair competition claims that arose from the alleged malicious litigation of a trade secret case brought to disrupt and/or destroy a small business. Thanks to a recent decision of the Georgia Supreme Court, the assignee of confidential and proprietary information has found itself in a Catch 22 dilemma – precluded from suing under the state's trade secrets statute because the information did not qualify as trade secrets but prohibited by that statute from bringing related common law claims.

2. Widening Federal Circuit Split on the Computer Fraud and Abuse Act

This year the circuit split regarding the interpretation of unlawful access under the CFAA continued to widen. On one side, the Ninth Circuit has adopted a narrow interpretation of the CFAA, while on the other side, the Fifth, Seventh, and Eleventh Circuits have adopted a broader interpretation of the CFAA based on either common-law agency principles or computer usage policies. Similarly, a Mississippi federal district court adopted the common-law agency theory of liability espoused by Judge Posner in the Seventh Circuit and found that a plaintiff had stated a claim under the CFAA. Earlier this spring, a Ninth Circuit en banc panel in *U.S. v. Nosal* adopted a narrow interpretation of the CFAA and found that an employee's violation of his/her employer's computer usage policies was not a violation of the CFAA; the Solicitor General declined to file a petition for writ of certiorari in that case. The Ninth

Circuit's narrow interpretation was followed by federal district courts in Minnesota and Michigan. Perhaps more important was the Fourth Circuit's adoption of the Ninth Circuit's narrow interpretation, which resulted in a petition for writ of certiorari before the Supreme Court on "whether the CFAA applies to employees who violate employer-imposed computer access and data use restrictions to steal company data." Should the Supreme Court grant the petition, it will undoubtedly be the hottest and most closely watched CFAA case in 2013. Should the petition be denied and Congress not intervene, the protection of employers' data under the CFAA will vary depending upon the circuit's interpretation of the CFAA.

3. The Social Media Cases and Ownership Issues

Social media was one of the hottest topics in 2012 because it raised novel issues in many areas of law, including trade secrets, computer fraud, and non-competes. We saw disputes over the ownership of company social media accounts and account "followers" in cases involving Twitter *(PhoneDog v. Noah Kravitz)*, LinkedIn (*Eagle v. Morgan*), Facebook *(Lown Companies, LLC v. Piggy Paint)* and Myspace *(Christou v. Beatport)*. One significant takeaway from 2012 is the necessity for employers to have social media ownership agreements with their employees when utilizing company social media accounts to conduct business. Moreover, at least one court found that suggestive Facebook posts may not violate non-solicitation covenants. We also saw the difficulty in employees proving cognizable losses or damages under the CFAA when their social media accounts, such as LinkedIn, are taken over by their employers. We expect social media cases to continue to be hot in 2013 and for companies to continue to seek to capitalize on "Big Data" and for related disputes over the ownership of such data to increase. We will offer a special webinar this year on the trade secret and privacy issues involved in the Big Data movement.

4. Continuing Developments in Legislation

Some of the biggest developments involved legislation that was never enacted. Specifically, the SOPA, PIPA, and CISPA anti-piracy and cybersecurity measures failed to pass after immense public backlash and widespread protests. The last attempt by Congress, the Cybersecurity Act of 2012, failed in November 2012. Additionally, there were failed attempts to amend the CFAA and limit its applicability.

In late December 2012, the President signed the Theft of Trade Secrets Clarification Act, which strengthens the scope of the Economic Espionage Act to ensure it addresses the theft of trade secrets related to a product or service used *or intended to be used* in interstate or foreign commerce, and to prevent results like the Second Circuit's decision in *U.S. v. Aleynikov*.

Additionally, the America Invents Act went into effect. The Invents Act 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. We believe that the full extent of this "defense" will begin to be fleshed out this year and more companies may begin to rely upon trade secret, rather than patent, protections as

result. The United States Patent and Trademark Office submitted a report to Congress earlier this year affirming the "prior commercial use" defense, which allows companies that commercially use a trade secret to avoid patent infringement liability if a patent is later issued on that trade secret.

There was also proposed federal trade secret legislation, which provided for a federal civil cause of action for trade secret theft, seizure orders to keep infringing goods from entering the US, as well as for monetary damages, attorneys' fees, and other injunctive relief. We expect that similar legislation will be reintroduced to Congress in 2013.

There has also been some new state legislation. New Jersey became the 47th state to adopt the Uniform Trade Secrets Act. New Hampshire enacted a notice period requirement for presenting employees or prospective employees with non-competes. Massachusetts also considered a statute that would limit non-competes, like California. There was also similar legislation proposed in Virginia. There was legislation proposed in Idaho to modify its trade secrets law. None of the bills, however, passed.

An emerging trend that may carry over into 2013 involves social media legislation. California, Maryland, Illinois, Michigan, and New Jersey enacted laws regulating employers' abilities to demand access to employees and prospective employees' personal social media accounts. We expect that more states will consider similar legislation in 2013.

5. Significant Jury Trials Verdicts, Criminal Sentences, and Other Notable Decisions Regarding Trade Secret Identification, Sealing, and Bad Faith Attorney Awards

In *U.S. v. Aleynikov*, the Second Circuit Court of Appeals in surprise decision overturned convictions against a former employee accused of steal computer source code for trade secret theft under the Economic Espionage Act and transporting stolen property in interstate commerce under the National Stolen Property Act (NSPA), holding the stolen computer source code was not a good or product intended for interstate commerce, and thus, Aleynikov had not violated either law. As a result, Congress recently passed the Trade Secrets Clarification Act which closes this loophole and expands the Economic Espionage Act to cover trade secrets "related to a product or service used in or intended for use in interstate or foreign commerce." This means that the amended Economic Espionage Act, which was signed by President Obama, will now protect a broader range of trade secrets.

There were also some significant prosecutions under the Economic Espionage Act and related statutes. A former Motorola engineer was convicted of stealing his former employer's trade secrets. A former General Motors engineer and her husband were convicted of stealing trade secrets on hybrid-car technology from the automaker to help develop such vehicles in China. Additionally, a former software engineer for CME Group Inc., the world's largest derivatives exchange, pleaded guilty to charges of downloading more than 10,000 files containing source code from his employer to support trading activities in an exchange in China. A New Jersey federal jury convicted a former employee of L-3 Communications Holdings Inc's. space and navigation division for transporting stolen property and possessing trade secrets related to precision navigation devices. The Department of Justice has prepared a report listing some of its most significant cases.

As for significant civil cases, American chemical company DuPont was awarded almost a billion dollars and an extraordinary 20-year global manufacturing injunction against rival Kolon Industries for the alleged theft of trade secrets regarding a proprietary fiber used to make "bulletproof" police and riot gear. Hallmark Cards won a jury verdict of $31.3 million in November in a trade secrets case in Kansas City federal court. A California pharmaceutical company secured a 10-month sale injunction in a California federal court against a competitor for the alleged misappropriation of protected customer lists and contact information.

A Ninth Circuit panel recently heard oral argument in the long running and closely-watched Mattel and MGA dispute, which may result in the reversal of a more than $310 million award in damages and attorneys' fees against Mattel in whole or part.

A California Court of Appeal held that parties may be liable for attorneys' fees and costs under its Uniform Trade Secrets Act for trade secret claims brought in bad faith if the claims are brought on suspicions alone and without any evidence of misappropriation to support the claims. A Pennsylvania federal court also held in a case of first impression that a defendant may recover attorneys' fees against a plaintiff where the plaintiff filed an objectively specious trade secret misappropriation claim and subsequently engaged in subjective misconduct during the course of discovery.

The widely followed *Apple v. Samsung* case illustrated the difficulties and challenges in protecting trade secrets filed in the public record or discussed in open court, especially when courts are unwilling or refuse to seal records in trade secret cases.

Courts continue to require identification of trade secrets with particularity in pleadings and discovery.

We also saw the Internal Revenue Service award a record $104 million to a whistleblower that helped the IRS collect hundreds of millions of dollars in U.S. taxes owed on money stored overseas. This underscores the importance of handling purported whistleblowers with access to your company's confidential information and trade secrets with extreme care and caution. Please see our previously recorded webinar on this important topic.

6. Increased Involvement of Government Agencies

This year we also saw increased involvement of government agencies in the areas of trade secrets and non-compete law. The FBI recently launched an initiative to curb the growing rise of trade secret and other intellectual property theft, in part because it sees state-sponsored espionage as a growing national security threat. As mentioned above, we saw additional prosecutions under the Economic Espionage Act. Both the FTC and Nevada Attorney General scrutinized a Nevada healthcare company's alleged anti-competitive behavior concerning the use of non-competes. The Department of Justice continued to scrutinize alleged no-hire agreements between companies and a proposed civil class action pending in federal court in California concerning the alleged unlawful use of anti-poaching agreements continues to proceed. Finally, the National Labor Relations Board has increasingly scrutinized employer's social media policies and issued several reports and memorandum concerning

such policies. Employers should make sure that their policies comply with the NLRB's recent "guidance" and also utilize social media ownership agreements with their employees.

7. Significant Non-Compete Enforcement and Defense Cases

An Illinois Appellate Court of Illinois in a significant unpublished non-compete decision held that the Illinois Supreme Court's *Reliable Fire Equipment v. Arredondo* opinion should apply both retroactively and proactively. *Reliable Fire* clarified the standard for determining the enforceability of non-compete agreements in Illinois. According to the Illinois Supreme Court, for an agreement to be enforceable, it must be analyzed under a three-pronged rule of reason test. The covenant would only be enforced if doing so was (1) not greater than necessary to protect a legitimate business interest of the promisee, (2) would not be "injurious to the public," and (3) would not cause "undue hardship to the promisor." *Reliable Fire*, 2011 IL 111871 at ¶ 17. Additionally, the court found that whether an interest was considered a "legitimate business interest" needed to be determined based on the totality of the circumstances. *Id.*

In a race to judgment non-compete dispute, an Oregon federal court found the amount in controversy for federal diversity jurisdiction satisfied, even though the plaintiff sought only declaratory relief and did not claim damages exceeding $75,000, based on the plaintiff's potential liability for defendant's allegations in a separate out-of-state lawsuit. A New York court held that the employee choice doctrine does not apply to equitable relief in a non-compete matter. The Kentucky Court of Appeals both affirmed the ability of Kentucky courts to modify overly broad non-competition agreements in the employment context and laid out a six-part framework that trial courts may follow when analyzing the reasonableness and enforceability of non-competition agreements. A Texas appellate court reminded employers of the importance in signing employment agreements when it held that a non-compete was unenforceable because the employment contract it was contained within was not signed by the employer.

Despite California's general prohibition on non-competes, the limited sale of business exception and so-called trade secret exception continue to remain viable mechanisms for certain non-compete enforcement in California when correctly utilized.

As predicated in last year's review, choice of law provisions and forum selection clauses cases contained to be significant in 2012. Such provisions are often included in non-compete agreements to apply the law and forum of the state that will most likely result in a favorable enforcement of the non-compete by the employer. The Ninth Circuit held that a contractual choice of law provision calling for the application of Georgia law was unenforceable because California had a materially greater interest than Georgia did in the outcome of the case. A California federal court for the Northern District of California, however, found that the alleged illegality of a non-compete clause in an employment agreement involving a California employee has no bearing on a legal forum selection clause and, accordingly, transferred the employee's declaratory relief action seeking to invalidate his non-compete to a Pennsylvania federal court. Another Northern District of California federal court similarly held that it did not matter to the court whether the ultimate effect of enforcing the forum selection clause may

result in the enforcement of the non-compete provision which "was purportedly contrary to California law," and dismissed the employee's case.

Further, a Colorado federal court decision in a non-compete dispute demonstrated the importance of drafting enforceable forum selection provisions in business transactions.

8. Trade Secret Preemption Gains Steam

Trade secret preemption continues to remain a significant issue in many jurisdictions. In a well-researched and articulate opinion, the federal court for the Northern District of California recently dismissed, as preempted by the California Uniform Trade Secrets Act, claims for misappropriation of non-trade secret proprietary information. This decision is at odds with a case earlier this year from the Northern District of California involving two social media app gaming companies and other state and federal authority. A federal court in Wisconsin (applying California law) illustrated that claimants who merely assert, in the alternative to their trade secret claim or otherwise, misappropriation of information not qualifying as a trade secret risk dismissal of those claims on preemption grounds. According to a puzzling Arizona federal court decision, employers must choose whether to sue for an Arizona Uniform Trade Secrets Act violation or for pre-empted claims. The Utah Court of Appeals also held that the Utah Uniform Trade Secrets Act preempts many common law claims relating to allegations of misuse of confidential information not qualifying as a trade secret. The Indiana Court of Appeals in a mixed martial arts broadcasting dispute held that the Indiana Uniform Trade Secrets Act preempts common law misappropriation and civil conversion claims. A New Hampshire federal court also broadly interpreted preemption under the New Hampshire Uniform Trade Secrets Act. We predict further unsettling trade secret preemption decisions in 2013 as courts grapple with whether the theft of non-trade secret information is actionable in tort.

9. Bring Your Own Device? Create Your Own Headache.

More companies are allowing employees to use their own computer devices in the work place. This reduces costs for the companies and the employees' familiarity with the devices can lead to increased productivity. Employing effective BYOD policies are important to protect valuable company trade secrets and information. In fact, the federal government recently developed a BYOD Working Group to study and analyze effective BYOD implementation, procedures, and policies. Some legal commentators, however, predict that BYOD may disappear in 2013 with an increased prevalence of corporate-owned devices. Some companies feel greater security over the control of their information through the use of corporate-owned devices. Employers must be vigilant not to invade the privacy of their employees' personal information and accounts in light of recent cases and legislation.

10. Increase in Arbitration?

The U.S. Supreme Court reaffirmed the Federal Arbitration Act's national policy in favor of arbitration and emphatically shot down an attempt by the Oklahoma Supreme Court to exert judicial review over the enforceability of a non-compete agreement that contained a mandatory arbitration provision. This opinion is yet another clear affirmation of the Court's 2011 *AT&T Mobility v. Concepcion* opinion and its desire to bolster the power of the FAA. Employers in jurisdictions hostile to non-compete agreements

may consider employing arbitration agreements with company-friendly mandated venues and choice of law provisions in light of the new decision. Employers, however, typically like to have courts handle requests for injunctive relief, so the ultimate impact of this decision may be mixed.

Some courts have pointed to carve outs for employers to pursue non-compete and trade secret claims in court in arbitration agreements as purported evidence of unconscionability to invalidate arbitration agreements. Notwithstanding those decisions, a California federal court recently ruled that an arbitration agreement's exclusion for injunctive relief for trade secrets and unfair competition claims is not unconscionable and does not invalidate the agreement.

Please continue following our blog this year. We incorporated several new features in our blog in 2012, including video interviews, an informative resources page, special guest authors, cutting edge infographics, and access to our well-received Trade Secret Webinar Series from 2011 to the present.

In 2013, we plan to incorporate video blog posts, audio podcasts, more guest authors, and provide a more enhanced resources page on the blog. We also plan to incorporate the latest developments in privacy, social media, big data, and technology into our blog coverage. Additionally, we plan to increase the accessibility to our blog by joining additional social media networks. Thank you for your continued support of the blog. You can also follow us on Twitter at @tradesecretslaw.

Trade Secrets

US Companies Have Options Against Chinese Companies For Trade Secret Misappropriation

By Eddy Salcedo (January 9, 2012)

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 to 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 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.

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

By Paul E. Freehling (January 10, 2012)

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.*, 2012 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 Columbia'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.

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

By Paul E. Freehling (January 12, 2012)

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.

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

By Joshua Salinas (January 13, 2012)

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 applies 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 Southern 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.

Court Rules Pennsylvania Trade Secrets Act Entitles Defendants To Attorneys' Fees For Bad Faith Misappropriation Claim

By Justin Beyer (January 24, 2012)

In a matter of first impression, Judge William Standish of the Western District of Pennsylvania ruled in *Best Medical Int'l, Inc. v. Spellman*, 07-cv-01709-WLS, 2011 U.S. Dist. LEXIS 147853 (W.D. Pa. Dec. 22, 2011), that, pursuant to the Pennsylvania Uniform Trade Secrets Act ("PUTSA"), a defendant may recover attorneys' fees against a plaintiff where the plaintiff filed an objectively specious misappropriation of trade secrets claim and subsequently engaged in subjective misconduct during the course of discovery.

At issue in this case was Best Medical's claims that four of its former employees (Hill, Spellman, Scherch, and Bittman) misappropriated Best Medical's trade secrets and provided those trade secrets to Accuray, Inc. Accuray and Best Medical are competitors in the radiation treatment planning and image guided therapy systems industry.

In December 2007, Robert Hill filed suit against Best Medical claiming Best Medical denied him severance benefits after his job responsibilities were reduced due to corporate downsizing. Following what Hill claimed was his constructive discharge, Hill went to work for Accuray, Inc.

Best Medical counterclaimed, alleging, among other claims, that Hill misappropriated Best Medical's confidential and trade secret information. In March 2008, Hill and Best Medical agreed to a stipulated motion for permanent injunction. Included amongst the terms of the permanent injunction, Hill agreed to return all Best Medical documents in hard copy form and submit his electronic storage devices to forensic examination, permit an image of his computer to be taken, and permit the alleged trade secrets and confidential information to be deleted from his computer. At no point during the remainder of the litigation did Best Medical claim that Hill violated the stipulated permanent injunction in any way.

In October 2008, Best Medical filed suit against Spellman, Scherch, and Bittman (the "Spellman Defendants"), all former Best Medical employees, and Accuray, alleging breaches of contract, tortious interference, and violations of PUTSA. Like Hill, the Spellman Defendants and Best Medical entered into a stipulated permanent injunction, also requiring the Spellman Defendants to turn over their electronic devices for review, imaging, and deletion of Best Medical's documents found on the computers.

The parties then engaged in nearly a year of settlement negotiations, which eventually culminated in Best Medical filing another complaint against Hill, the Spellman Defendants, and Accuray. In May 2010, Accuray filed a series of motions to compel seeking a definitive answer from Best Medical as to the trade secrets Best Medical claimed had been misappropriated and which Best Medical further claimed Accuray was using to Best Medical's detriment.

Over the course of another year, Best Medical stonewalled on answering that question, until two 30(b)(6) deponents, presented by Best Medical, conceded that Best Medical: (a) could not identify the trade secrets that Accuray allegedly misappropriated; (b) had not investigated its misappropriation claim prior to filing suit; and (c) did not have any evidence of Accuray misappropriating and improperly using Best Medical's trade secrets.

Following the court's grant of summary judgment in October 2011, Accuray and the Spellman Defendants sought recovery of attorneys' fees spent defending the misappropriation claims based on three theories:

(1) Best Medical violated PUTSA, 12 Pa. C.S. § 5305(1), which requires that "attorneys fees, expenses and costs [may be recovered by] the prevailing party: (1) if a claim of misappropriation is made in bad faith;"

(2) Best Medical violated 28 U.S.C. § 1927, which requires that: "Any attorney or other person admitted to conduct cases in any court of the United States ... who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct;" and

(3) that the court possessed the inherent power to sanction Best Medical and award attorneys fees to Accuray and the Spellman Defendants due to Best Medical's litigation conduct.

Finding no Pennsylvania case interpreting 12 Pa. C.S. § 5305(1), the court relied heavily on other states' interpretation of their own versions of the Uniform Trade Secrets Act. The court decided to follow and apply a two-part test rendered by the California Court of Appeal in *Gemini Aluminum Corp. v. Cal. Custom Shapes, Inc.*, 95 Cal. App. 4th 1249, 1262 (Ct. App. 2002). In *Gemini*, the California Court of Appeals ruled that, to merit an attorneys fee sanction against the plaintiff, the defendant must prove: (1) the "objective speciousness of the plaintiff's claim;" and (2) "subjective bad faith in brining or maintaining the claim." 2011 U.S. Dist. 147853, at * 10, *citing Gemini*, 95 Cal. App. 4th at 1262.

Defining "objective speciousness," the *Best Medical* court cited to decisions from the District of Maryland and the Southern District of California, in which those courts held that "objective speciousness exists where there is a complete lack of evidence supporting plaintiff's claims."

The *Best Medical* court also defined what constituted "subjective misconduct" finding it "exists where a plaintiff knows or is reckless in not knowing that its claim for trade secret misappropriation has no merit." 2011 U.S. Dist. LEXIS 147853, at *12.

After also considering a defendant's burden of proof to show that attorneys' fees should be awarded under 28 U.S.C. § 1927 or the court's inherent power, the court analyzed why an award was appropriate pursuant to PUTSA. The court found that Best Medical acted in bad faith, and relied heavily on three salient facts; namely:

(1) that Best Medical possessed images of the Spellman Defendants' computers since November 2008, but failed to analyze those computers;

(2) that an affidavit from Best Medical's president, which indicated that Best Medical was: (a) always ready, willing and able to assist counsel in the prosecution of this matter; (b) monitored its counsel's activities throughout the litigation; and (c) identified to counsel at the outset of the litigation the trade secrets at issue; was essentially unreliable and not supported by the facts of the case; and

(3) that Best Medical's 30(b)(6) witness admitted in May 2011 that Best Medical did not investigate its misappropriation claims thoroughly before it filed its complaint against Accuray and the Spellman Defendants.

The court concluded that Accuray and the Spellman Defendants were entitled to all of their attorneys' fees incurred as a result of defending the PUTSA claims. The court did not reach the other arguments based on 28 U.S.C. § 1927 or the inherent powers of the court.

While the reach of this decision is not yet apparent, it is important to note that Pennsylvania now joins other states, including, California, Maryland, Minnesota, and Michigan, in finding that a defendant may recover attorneys' fees where a plaintiff brings or maintains a misappropriation claim in bad faith. See 2011 U.S. Dist. LEXIS 147853, at * 10-12. As seen from the above factual recitation, however, it also appears that a plaintiff must act quite egregiously and lack any evidence of misappropriation before a Pennsylvania court will award attorneys' fees.

Court Allows Employer's Interference With Prospective Economic Advantage Claims To Survive In Lawsuit Claiming Employee's Theft of Twitter Account

By Robert Milligan and Gary Glaser (February 1, 2012)

A California federal district court denied a former employee's motion to dismiss his former employer's claims for tortious interference with prospective economic advantage and negligent inteference with prospective economic advantage Monday in a closely watched lawsuit concerning the interplay between social media, trade secrets, and employee mobility.

We previously wrote about this case from the United States District Court for the Northern District of California after the Court 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.) (November 8, 2011)

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. According to the complaint, the employee refused to turnover the Twitter account after he left and instead changed the name handle and continued to use the account with the built-in following.

Kravitz had moved to dismiss the entire suit on the grounds, among other things, that a Twitter account's followers are not "secret" and that Kravitz's followers were not property.

As part of its November ruling, the Court granted the employee's motion to dismiss PhoneDog's tortious interference and negligent interference with prospective economic advantage claims, subject to PhoneDog's right to file an amended complaint. PhoneDog subsequently filed an amended complaint and then Kravitz filed a motion to dismiss PhoneDog's claims for tortious interference with prospective economic advantage and negligent inteference with prospective economic advantage.

In its most recent January ruling denying Kravitz's motion to dismiss, the Court found that "the court is able to draw the reasonable inference that PhoneDog had an economic relationship with at least one third-party advertiser that was disrupted by Kravitz's alleged conduct, causing it economic harm."

The Court stated that it initially dismissed PhoneDog's tortious interference claim because PhoneDog failed to sufficiently allege which economic relationships were actually disrupted by Kravitz's alleged conduct. Dkt. No. 28 at 11-12. To cure this deficiency, according to the Court, PhoneDog's first amended complaint clarified that it had economic relationships with (1) the approximately 17,000 followers of the Twitter account at issue; (2) its current and prospective advertisers; and (3) CNBC and Fox News, and that each of these economic relationships were actually disrupted by Kravitz's conduct. FAC ¶¶ 19, 33-36.

Kravitz's motion attacked each of these three alleged economic relationships as insufficient to sustain the intentional interference claim. The Court reasoned that for PhoneDog to have properly alleged its tortious inteference claim, only one of the above economic relationships has to meet the elements of the tort. The Court found that the alleged relationship between PhoneDog and its current and prospective advertisers suffices.

The Court rejected Kravitz's argument that the allegations supporting this relationship are speculative because they only assert that PhoneDog's advertising revenue "might have" decreased. According to the Court, PhoneDog explicitly alleges in its first amended complaint that a significant amount of its income is derived from advertisements on its website, and "advertisers pay for ad inventory on PhoneDog's website for every 1000 pageviews generated from users visiting PhoneDog's website." FAC ¶ 10. According to the complaint, due to Kravitz's alleged conduct, "there is decreased traffic to [the] website through the Account, which in turn decreases the number of website page views and discourages advertisers from paying for ad inventory on PhoneDog's website." FAC ¶ 36. "As a direct and proximate result of Defendant's wrongful acts, PhoneDog has suffered damage to is business by way of lost advertising revenue. . . ." FAC ¶ 38. Based on these factual allegations, the Court concluded that it is able to draw the reasonable inference that PhoneDog had an economic relationship with at least one third-party advertiser that was disrupted by Kravitz's alleged conduct, causing it economic harm.

The Court also found that PhoneDog's first amended complaint also sufficiently alleges its third claim for negligent interference with prospective economic advantage. The Court previously dismissed this claim on the same grounds as it dismissed the second claim for intentional interference: PhoneDog had not sufficiently alleged which economic relationships were actually disrupted by Kravitz's alleged conduct. Dkt. No. 28 at 13. The Court found based upon the amendments discussed above that the previous deficiencies have been corrected by PhoneDog's amended allegations in the first amended complaint. The Court also noted that the other reason the Court previously dismissed the third claim was because PhoneDog had failed to allege that Kravitz owed it a duty of care, which is a necessary element of the negligent interference claim. To rectify this missing allegation, PhoneDog's first amended complaint now asserts that "Defendant owed a duty of care to PhoneDog as an agent of PhoneDog." FAC ¶ 42. Accordingly, the Court concluded that PhoneDog had complied with the Court's previous order and provided Kravitz with the reason why it believes he was negligent (as an employee, he owed his company a duty of care).

Trading Secrets

The next milestone in this closely watched case appears to be Kravitz's not yet filed summary judgment motion which will likely challenge PhoneDog's claims that the Twitter followers constitute trade secrets and its ownership interest in the Twitter account.

Filing A Patent Application Covering A Misappropriated Trade Secret Held To Constitute A "Use" Which Justifies $600,000 In Compensatory Damages

By Paul E. Freehling (February 6, 2012)

Quoting Section 40, comment c, of the Restatement (Third) of Unfair Competition, the Fifth Circuit Court of Appeals held recently that "*Any exploitation* of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant" constitutes a "use" giving rise to liability for misappropriation (emphasis added). So, when Varco, LLP filed its own patent application with respect to another person's invention which had been disclosed to Varco in confidence, Varco "used" the trade secret. Although no patent ever was issued, the jury's compensatory damages award of $600,000 against Varco and in favor of the inventor was warranted. *Bohnsack v. Varco, LLP*, No. 10-20741 (5th Cir., Jan. 23, 2012).

After Varco executed a confidentiality agreement, Bohnsack disclosed his invention of a machine to clean tanks used in oil drilling. Negotiations ensued regarding Varco's payment for use of the invention, but ultimately they were abandoned. During the course of the negotiations, Varco asked its attorney, McClure, to prepare a patent application. He did so, but he included a declaration that he and Bohnsack were co-inventors. At McClure's request, Bohnsack executed the declaration. After signing, however, he had second thoughts which he communicated to McClure who assured him that the declaration would not be filed until the matter was "sorted out." Nevertheless, McClure proceeded to file the application and declaration.

McClure assigned to Varco his rights in the invention. But Varco already had a product that performed the cleaning task cheaper, and so it decided not to use the invention, withdrew the patent application, and relinquished all rights to Bohnsack. He then developed the invention without patent protection.

Varco sued Bohnsack in a Texas federal district court, seeking a declaration that it had done nothing wrong. It stressed that McClure was not a Varco employee, and so respondeat superior did not apply to his misconduct. Bohnsack counterclaimed for trade secret misappropriation and for the fraud McClure had committed. Varco's motions for judgment were denied, and the case was submitted to the jury. It rendered a verdict for Bohnsack and against Varco, awarding him compensatory damages of $600,000 on both counts and punitive damages on the fraud claim.

The appellate court affirmed the trade secret misappropriation compensatory damages verdict but held that Bohnsack was entitled to a "take-nothing" judgment for fraud and to no punitive damages. Rejecting Varco's argument that Bohnsack had not proved an injury caused by the misappropriation, the Fifth Circuit reasoned that Varco knew about McClure's misconduct, and that a $600,000 award was proper because it approximated the minimum fair market value of the trade secret since Varco had offered to buy the invention for that much and more.

This case teaches, first, that filing a patent application covering someone else's invention may constitute a "use" of the invention and, therefore, an applicant who fails to obtain the inventor's unequivocal consent may be found guilty of trade secret misappropriation. The second lesson is that juries and judges are not sympathetic to miscreants.

California Federal Court Finds That Plaintiff's Claims Are Not Preempted By The California Uniform Trade Secrets Act In Farmville Spat

By Scott Schaefers (February 9, 2012)

On February 6, 2012, a federal court in Oakland, California denied the popular Facebook application "Farmville" operator's (Zynga, Inc.) motion to dismiss several claims brought by the inventor of "myFarm" (SocialApps, LLC, or "SA")) for alleged theft of the source code, game images, and "concepts and features" used in the myFarm app. The court allowed SocialApps to proceed with its claims that Zynga took SA's trade secrets, and breached implied contracts, "covenants of good faith and fair dealing," and SA's "confidences" in connection with a pre-acquisition non-disclosure agreement. In doing so, the court paved the way for SA to hold Zynga liable for allegedly betraying SA's unwritten, but clearly implied, trust and confidence it placed in Zynga while the two discussed Zynga's buyout of myFarm.

SA alleged that it launched myFarm the first-ever virtual farming game, in November 2008 on Facebook. The application thereafter attracted millions of users. In May 2009, in anticipation of Zynga's acquisition of myFarm, Zynga and SA entered into a written confidentiality agreement to protect SA's assets while Zynga conducted its due diligence. Within a month, however, Zynga used SA's source code, game images, and other "concepts and features" to launch FarmVille, all without buying the rights or obtaining SA's consent. Using the ruse of "due diligence," Zynga allegedly had SA produce its confidential source code and other information for 'myFarm,'" which Zynga allegedly use in "FarmVille," the complaint said.

In June 2011, SA sued Zynga, making six claims for copyright infringement, statutory trade secrets theft, breach of contract, breach of "implied contract," breach of confidence, and breach of implied covenant of good faith and fair dealing, and later adding a seventh claim for "unjust enrichment." In October 2011, Zynga asked the court to dismiss SA's claims for trade secrets theft, breach of implied contract, breach of confidence, and implied covenant of good faith. Zynga argued that SA's alleged trade secrets were on the internet, and thus not secret; that the claims breach of implied contract, confidence, and implied covenant of good faith were duplicative of the written contract claim, and that the California Trade Secrets Act preempted the breach of confidence claim.

The court largely rejected Zynga's arguments, at least at the preliminary stages of the case. The court did strike SA's trade secrets theft claim, but only insofar as it based the claim on any of myFarm's publicly available images and features.

"As [SocialApps] has alleged, the 'myFarm' game was publicly released in November 2008, and therefore the images and features were visible to the public several months before the May 2009 letter agreement or June 2009 release of 'FarmVille,'" the Court wrote. The "images and features"

component of SocialApps' trade secrets claim will therefore be stricken, leaving the "proprietary source code" component alive, the judge ruled.

The court upheld the trade secrets theft claim to the extent it was based on SA's source code, and upheld the other implied contract, confidence, and implied covenant of good faith confidence claims. In essence, the court held that SA could be held liable for violating not only the letter of the May 2009 non-disclosure agreement, but also its spirit.

Also of note is the court's holding that, at least at this stage, that SA's breach of confidence claim was *not* preempted by the Trade Secrets Act. The court held that to the extent SA based its confidence claim on Zynga's unauthorized use or disclosure of myFarm's "concepts and/or game features" that did not involve SA's proprietary source code underlying its trade secrets theft claim, SA stated a valid information-theft claim separate from a trade secrets violation. The decision is consistent with other courts' recent decisions that a plaintiff may maintain an independent common law claim for information theft, at least at the pleading stage. (i.e. *Amron Int'l Diving Supply, Inc. v. Hydrolink Diving Comm., Inc.*, No. 11-cv-1890-H (JMA), 2011 U.S. Dist. LEXIS 122420, at * 25-27 (S.D. Cal. Oct. 21, 2011).

We will continue to monitor this interesting new case.

Protecting Trade Secrets and Confidential Information In The Social Media Generation

By Robert Milligan (February 12, 2012)

Over the past decade, no avenue has had a bigger impact on society and the ways in which people interact than social media. Websites like Facebook, Twitter, LinkedIn, which traffic in information shared on its servers, encourage users to publish every detail of their lives. For employers, the reality of social media's pervasiveness (and benefits) presents unique challenges in maintaining the integrity of trade secrets and confidential information accessible to employees. While it is always important to err on the side of caution in crafting effective social media policies for the workplace, employers must be aware of their legal limitations in setting parameters for appropriate use. To avoid the ire of the National Labor Relations Board (NLRB), companies must align their policies with the National Labor Relations Act (NLRA). In connection with the same, the Office of the General Counsel for the NLRB has recently issued its interpretation of how the Act applies to social media. Companies that rely on trade secrets and confidential information need to listen and make sure that their social media policies are compliant with the NLRA or risk that their valuable information is exposed and liability under the NLRA.

Passed in 1935, the NLRA is a federal law designed to protect employees' rights to organize unions, labor strikes, or engage in collective bargaining. In practice, the Act allows workers to freely discuss issues ranging from the terms and conditions of employment to complaints of unfair treatment. Relating to social media, this protection allows employees to author public posts about a company or their workplace so long as it can be construed as a discussion with fellow employees and a potential first step towards self-organizing. With respect to this protection, it does not matter whether the employer is a union shop as these protections apply to non-union employers as well.

In a recent operations management memo issued by Lafe Solomon, the Acting General Counsel for the NLRB, an analysis of recent cases related to social networking in the workplace found that a majority of employers had applied overly broad policies that did not adhere to the provisions of the NLRA. These cases were largely related to the terminations of employees who had authored some sort of work-related post on Facebook. Although employers have both a duty and the right to take action against employees who misappropriate company information online, in light of the NLRB's interpretation of these cases, companies should revisit their social media policies and ensure that they offer maximum protection without opening themselves up to future litigation. In particular, employers should be aware of *what sorts of topics* are protected by the NLRA - even on a very public forum such as Facebook.

According to the NLRB, the report underscores two main points made in an earlier compilation of cases:

1. Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.

2. An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

The report provides several examples of social media policies that run afoul of the NLRA and those that do not. The NLRB report concluded that the policy described below was not overly broad and, therefore, was lawful:

> "The employer's social media policy provided that the employer could request employees to confine their social networking to matters unrelated to the company if necessary to ensure compliance with securities regulations and other laws. It prohibited employees from using or disclosing confidential and/or proprietary information, including personal health information about customers or patients, and it also prohibited employees from discussing in any form of social media 'embargoed information,' such as launch and release dates and pending reorganizations."

According to the NLRB's interpretation of recent cases, the potential scope of protected employee-discussion is fairly large. Examples of speech protected by the NLRA include accusations of sexism in the workplace, departmental complaints, complaints about orders or instructions perceived to be unfair and other labor disputes. In each of these cases, the NLRB found location (a forum including fellow employees) and context (relating to terms and conditions of employment) to be the standard for what is, and is not permissible.

For companies worried about trade secret protection and keeping sensitive information confidential, the broad nature of the NLRA can seem like a severe handicap in their efforts to prevent all forms of misappropriation. Dealing with the possibility that an employee could, for example, complain online about having to travel to a distant location for an upcoming project, only to inadvertently disclose a business strategy the company had otherwise gone to great lengths to keep confidential, is a nightmare scenario that is all too likely in the information age. Fortunately, the NLRB has clarified what it views as permissible social media policy in regards to this issue. Recently, a company expanded a policy asking employees to abide by securities regulations in relation to discussing the company on social networking sites to include "embargoed information" that it deemed confidential. Although this policy could be seen as trying to restrict actions protected under the NLRA, the NLRB ruled that the employees would reasonably interpret to the policy to apply only to communications that might implicate security regulations.

In addition, they ruled that since employees do not have a protected right to disclose embargoed information such as trade secrets or confidential information, the employees would not reasonably interpret the rule to disallow communications about the terms and conditions of their employment.

While this may not be the clearest, bright-line rule, it at least acknowledges that the NLRB acknowledges an employer's right to protect its trade secrets and confidential information.

Maintaining an up-to-date social media policy should be a high priority for any company. As social media continues to evolve in its effects on society and modern communication, it is critical that employers educate their employees on what is, and is not permissible social media use with regards to company information. Actual meaningful training is essential rather than hiding the social media policy in a stack of new hire paperwork. Eliminating any ambiguities that may remain from outdated policies can serve to offer future protection against the misappropriation of trade secrets or confidential information online, no matter what the social media service of choice may be for the particular company. Employers should focus on legitimate business interests in articulating their written policies and conveying their policies to employees. Clearly defining the parameters of what is off limits or embargoed for discussion in social media is the most effective way to protect a company from misappropriation while steering clear of overly broad policy applications that may be deemed unlawful by the NLRB. Depending upon the industry, social media policies may also want to address the ownership of content in social media accounts used to generate business for the employer. Competent legal counsel should be consulted to create and/or update appropriate social media policies.

Click Wrap? Forget It: Federal Court Finds That Violation of Online Clickwrap Agreement Not Enough to Constitute Trade Secret Misappropriation Under California Law

By Scott Schaefers (February 17, 2012)

On February 13, 2012, a federal judge in Los Angeles, California dismissed a remote-access software company's claim that one of its customers violated the California Trade Secrets Act, Cal. Civ. Code § 3426.1 *et seq*., by downloading a trial version of plaintiff's Mac-environment remote-access software and "reverse engineering" its own program. *Aqua Connect, Inc. v. Code Rebel LLC*, No. 2:11-cv-05764-RSWL-MAN (C.D. Cal. Feb. 15, 2012) (Doc. No. 30). This decision clarifies, to an extent, when competitors may be liable under the Trade Secrets Act for using free trial versions of a commercial product or program as a starting-off point for their own research and development of a competing product.

Aqua Connects' allegations were fairly straightforward. Aqua Connect alleged that its "ACTS" software, by which users can remotely access a Mac-based environment, was a trade secret under California's Trade Secrets Act. Aqua Connect alleged that Code Rebel downloaded a free trial version of ACTS after agreeing to all the terms and conditions of Aqua Connect's clickwrap End User Licensing Agreement. The Agreement prohibited users from reverse engineering the ACTS software and any subsequent sales of such infringing programs. That is exactly what Code Rebel did, according to Aqua Connect. Code Rebel allegedly used its free trial ACTS package to develop a competing remote-access program Aqua Connects alleged, in relevant part, that such reverse engineering in breach of the Agreement constituted acquisition of trade secret information by "improper means," and thus "misappropriation," under the Trade Secrets Act.

Code Rebel, and the federal court, disagreed. The court held that the Act's definition of "improper means" and the accompanying committee comments made clear that mere reverse engineering of a trade secret, without any further evidence of improper access or acquisition, was not enough to prove misappropriation under the Act. Thus, Aqua Connect's online offering of free 14-day trials of its ACTS program, even though accompanied by a license agreement not to reverse engineer and subsequently sell such programs, precluded Aqua Connect's claim of improper acquisition. Essentially, the court focused on Code Rebel's access, and not use, of the ACTS program, and there was nothing wrong with the access.

The court also rejected Aqua Connect's alternative argument that Code Rebel is liable under the Act because misappropriation also occurs when someone acquires a secret "under circumstances giving rise to a duty to maintain its secrecy, but nevertheless uses the secret without authorization. That theory of misappropriation, the court held, was reserved for fiduciary or employment relationships where agents or employees owe automatic legal duties to their clients or employers, which circumstances were not present here. And because Aqua Connect had twice tried and failed to allege

trade secret misappropriation based on Code Rebel's misuse of the online trial program, the court dismissed Aqua Connect's claim with prejudice and without permission to try again.

This decision is noteworthy because it refused to hold liable under the Trade Secrets Act a company which agreed not to reverse engineer a competitor's product for its own benefit, but then turned around and did just that. One might question why Aqua Connect's clickwrap agreement's express prohibition against reverse engineering was not enough to impose on Code Rebel a duty under the Trade Secrets Act not to misuse the ACTS software. If agents and employees can be held liable under the "circumstances giving rise" theory of trade secrets misappropriation, and agents and employees voluntarily take on their legal duties of loyalty and confidence, then why cannot a customer which voluntarily takes on a contractual duty of secrecy be held to the same standard? After all, holding Code Rebel to the same standard would seemingly not contradict the Act's provision that reverse engineering alone is insufficient. Code Rebel breached an express promise of secrecy, a promise that Aqua Connect probably insisted on to prevent the very acts of which it accused Code Rebel. But, the logic and fairness of this result are broader topics that are outside the scope of this post.

And in the end, Aqua Connect is not without recourse. Still alive are its claims for breach of agreement, false promise, statutory unfair competition, and unjust enrichment. So Aqua Connect still may be able to recover similar compensatory damages as it would under a trade secret misappropriation claim, and it can potentially recover punitive damages under its false promise claim. We will continue to follow this case and update you on any significant developments.

Solar Panel Rivals In Trade Secret and Data Theft Spat In California Federal Court

By Jessica Mendelson (February 18, 2012)

On February 13, SunPower Corporation, a manufacturer of solar panels, sued five former employees, as well as its rival, SolarCity Corporation in federal court in San Francisco, California and sought a temporary restraining order against the defendants. SunPower asserted claims of unfair competition, trade secret misappropriation, and violations of the Computer Fraud and Abuse Act ("CFAA"), as well as a number of other claims, in its complaint.

In its complaint, SunPower alleges that five former employees copied thousands of electronic files containing confidential information on to external hard drives and USB devices. The individual defendant employees all signed non-disclosure and non-solicitation agreements with SunPower.

One of the individual defendants allegedly left SunPower in August 2011, and began working at SolarCity. In the days leading up to his departure, SunPower alleges the individual defendant used portable storage devices to steal proposals, contracts, quotes, deals and market analysis from SunPower. This data also included information about SunPower's major customers, as well as the names of the employees responsible for the sales. SunPower alleges this former employee then used this information to recruit other SunPower employees to SolarCity. These employees included the other individual defendants, each of whom allegedly copied additional confidential information on to a personal USB device prior to leaving SunPower. One of the individual defendants also allegedly accessed his SunPower email immediately after leaving and forwarded several confidential documents to his personal email account. SunPower used forensic analysis to confirm the alleged theft of these files after the fact.

SunPower's complaint alleges the stolen files were then transferred to computers or devices at SolarCity, which knowingly accepted them, and used the information to conduct business. In doing so, SunPower alleges SolarCity and its employees violated the CFAA and misappropriated trade secrets. Based on SolarCity's actions, SunPower requested the judge grant a temporary restraining order, which would include allowing a forensic expert to copy data from the employees' computers and computer media to preserve evidence of stolen information.

SunPower alleges the stolen information "will greatly damage [their] global sales by allowing SolarCity to predict SunPower's every movement for years to come. . . it is highly likely defendants will conceal the stolen computer files unless this court grants this motion and allows SunPower to copy data from the former employees' computers."

The Ninth Circuit has previously addressed the issue of liability under the CFAA in cases where employees steal or remove electronic data in violation of employer computer use policies. In *US v. Nosal* (9th Cir. No. 10-10038), the court held that a former employee "exceeds authorized access" to

data on an employer's computer system when the employee takes actions on the computer which are prohibited by written policies and procedures concerning acceptable use. Under the policy articulated in *Nosal*, employees must strictly adhere to a company's computer use restrictions in order to comply with the CFAA. However, the Ninth Circuit granted en banc review of the previous Ninth Circuit *Nosal* decision. Oral argument before the en banc panel was held in December and a decision has yet to be released. Accordingly, it is unclear whether Sunpower will be able to maintain its CFAA claim.

As of February 17, it appears unlikely that the court will rule on Sunpower's motion for temporary restraining order. The parties have filed a joint stipulation withdrawing the motion for a temporary restraining order without prejudice, and seem to think it is likely that an agreement can be reached. However, SunPower has reserved the right to refile for injunctive relief. We will continue to follow this case closely as it progresses.

California Federal Court Hammers Defendant For Destroying Evidence In Trade Secret Rift

By Vincent Smolczynski (March 2, 2012)

A California federal district court judge recently issued a contempt citation and sanction award of $73,000 against a defendant in a trade secret misappropriation dispute for violating a court order to preserve evidence pending a hearing on a temporary restraining order. The case is *Amron International Diving Supply, Inc. v. Hydrolinx Diving Communication, Inc.,* No. 11-CV-1890-H (S.D. Cal. Feb. 22, 2012) (Dkt. No. 76). The court's decision illustrates both the need for employers to conduct early forensic investigations of employees' computer hardware when suspected of stealing trade secrets, and the hefty sanctions that can be imposed on defendants for the failure to preserve data stored on computer hardware.

Amron brought its trade secrets suit against defendants Saad Sadik and Hydrolinx, a newly-formed, competing company established by Sadik shortly after he was terminated by Amron in 2010. Based upon information Amron obtained indicating Sadik allegedly stole trade secrets, destroyed electronic data and then attempted to "cover [his] tracks," Amron sought an ex parte temporary restraining order on August 23, 2011. The court scheduled a hearing and ordered the parties to preserve all evidence in its possession. At the hearing on August 31, 2011, the court granted the TRO, ordering defendants to produce all computers and media in their possession for forensic inspection and further ordering defendants to provide a written declaration attesting that, among other things, Sadik had not deleted any data since being served the order to preserve evidence.

Forensic analysis of the three produced computers established that days after being served the preservation order, defendant installed a Digital Document Shredder ("DDS") software program on two computers, permanently destroying all data on both. Defendant had also purchased a brand new hard drive two days after the preservation order and installed the hard drive in a third computer sometime thereafter. Amron's forensic inspection indicated Sadik manipulated the computer's system clock to make the newly-installed hard drive appear to have been installed a month before the order.

Amron sought sanctions against defendants for the use of the DDS software to wipe the computer, the destruction or hiding of another hard drive, and the manipulation of the computer system clock. Amron also filed a motion for contempt because of defendants' refusal to produce additional computer

hardware, including a portable hard drive, an additional computer, and several USB devices, which the court had ordered the defendant to produce. Though defendant offered "some excuses" to justify his actions, the court concluded monetary sanctions and contempt were appropriate for the defendants' willful violations of the order to preserve evidence. The calculation of the $73,000 award was based upon the attorney's fees associated with investigating the defendant's violations, the attorney's fees for bringing the motion for contempt, and the costs incurred to retain a computer forensic consulting firm.

The *Amron* decision serves as an important reminder of the extent to which parties to trade secret litigation may be liable for failing to preserve and protect electronic data. The case also illustrates the need for early forensic analysis to determine the extent of data preservation or lack thereof.

Virginia Supreme Court Issues Important Trade Secret Decision and Raises Bar for Proving Damages

By Rebecca Woods (March 7, 2012)

In its latest opinion dealing with trade secret issues, the Virginia Supreme Court ruled that the Virginia Uniform Trade Secrets Act, Va. Code §§ 59.1-336 through 343 ("VUTSA") protects trade secrets even if they are used by an entity that is not demonstrably "in competition with" the plaintiff. *Collelo v. Geographic Services, Inc.*, 721 S.E.2d 508 (2012) (283 Va. 56). The Court also apparently concluded that a plaintiff must demonstrate different damages flowing from a violation of the VUTSA, on the one hand, and claims for breaches of contract and tortious interference of contract, on the other hand. Further, the trial court's original ruling and the *Collelo* dissent suggest that hostility to trade secret protection for employers in Virginia is not waning.

Anthony Collelo worked for Geographic Services, Inc. ("GSI") for two years on GSI's "geonames" work, in which GSI sold information to its clients that populated maps. As part of his training and work, Collelo had access to and utilized tools and methods developed by GSI with respect to its geonames work. Collelo had an employment agreement with GSI that included non-disloclosure and non-solicitation provisions with GSI, preventing him from disclosing GSI's confidential information or performing "conflicting services" for a customer or contractor of GSI's for a period of one year after his employment with GSI ended.

Collelo resigned from GSI in 2008 and began working for a new employer, a customer of GSI's for whom GSI had done geonames work. Collelo's work for his new employer appeared to be substantially identical to the work he had done for GSI on geonames, including development of tools for the new employer that were substantially similar to those used at GSI. Notably, after Collelo joined his new employer, the new employer demanded from GSI a reduction in rates and hours for certain geonames work by GSI.

GSI filed suit against Collelo and the new employer alleging, among other things, that Collelo had breached his employment agreement with GSI and violated the VUTSA, and that the new employer had violated the VUTSA and had tortiously interfered with GSI's employment contract with Collelo. Among the relief sought was damages, reasonable royalty, and an injunction. GSI lost at trial, however, when the trial judge granted the defendants' motion to strike after GSI's case in chief and dismissed the case with prejudice.

The trial court had ruled that GSI established the existence of proprietary information under VUSTA. However, it concluded that even if Mr. Collelo had taken something from GSI, because the new employer was not doing the same work as GSI, GSI could establish no loss of business or damages. The court reasoned that the purpose of protections for proprietary information was to keep competitors from using them to take business away from the owner of that proprietary information. In the trial court's view, there must be loss of business by plaintiff, or a gain in income by the defendant, in order for there to be compensable damage.

On appeal, the Virginia Supreme Court analyzed the VUTSA and concluded that it does not require that "one who is accused of misappropriating a trade secret use [it] to compete with the holder of the trade secret." Instead, the law requires only proof of a trade secret, its misappropriation or use of the trade secret by someone knowing or having reason to know it was acquired by improper means, and damages. The Court then declined to rule as a matter of law on the sufficiency of the VUSTA damages demonstrated by GSI.

The Court then upheld the trial court's dismissal of the breach of contract and tortious interference claims because GSI's two damages experts stated on cross-examination that they were offering opinions as to the VUSTA claims only. This testimony led the Court to conclude there was no evidence supporting damages for the breach of contract or tortious interference claims. Apparently GSI's counsel did not argue that the experts' testimony regarding unjust enrichment, devaluation of the trade secrets, and devaluation of GSI supported the damages claim for the contract and tort claims.

The dissent took GSI's damages evidence to task and argued that the majority's failure to rule on the merits of GSI's damages was in error. While not precedential, the dissent's analysis of the damages is the most detailed such analysis in a recent Virginia Supreme Court trade secret case and thus deserves attention. The dissent demanded evidence of lost profits to support actual damages, rejecting as being legally baseless GSI's claim for diminished value and cost to develop the trade secret. The dissent found GSI's expert calculation of unjust enrichment to be insufficient because it did not provide a one-for-one analysis of the use of GSI's trade secret and profits obtained thereby by the new employer. Because the royalty analysis was dependent on the unjust enrichment analysis, the dissent rejected that claim out of hand.

Lessons

- The Virginia Supreme Court likely got it right in interpreting the VUSTA to apply even in instances when a misappropriated trade secret is used by an entity that is not technically in competition with the trade secret's owner.

- The Court probably got it wrong, however, in apparently requiring different damages to flow from a VUSTA violation and claims for breach of contract and tortious interference. While the damages may, in fact, be separate among the claims, they need not be. For example, GSI proffered evidence of a diminution in value of its trade secrets, and of its company, as a result of the new employer's alleged use of those trade secrets. Nothing in the Court's analysis explains why these

kinds of damages could flow from all of GSI's claims against the new employer – except for the testimony of GSI's experts limiting the scope of their damages analysis to a single claim. The lesson here is for employers (and their trial counsel) to prep your experts better. Leave it to the lawyers to argue which damages proofs support which claims.

- Finally, the dissent's opinion is cautionary and indicates that Virginia courts may have a high bar for proof of damages flowing from actionable misuse or disclosure of a trade secret. Make sure your experts provide rigorous opinions supporting the damages claim, and be armed with legal support for the kinds of damages to which a plaintiff is entitled in trade secrets cases.

Trading Secrets

What Happens in Vegas May Stay in Vegas, But Misappropriation of Trade Secrets and Unauthorized Disclosure of Confidential Information Will Still Land You in Hot Water According To Recent Supreme Court of Nevada Decision

By James D. McNairy (March 10, 2012)

In *Finkel v. Cashman Professional, Inc., et al*., Case Nos. 54520, 55377, 2012 WL 669897 (Nev. March 1, 2012), the Supreme Court of Nevada addressed the validity of non-solicitation, non-competition, and non-disclosure covenants and the proper duration of a preliminary injunction prohibiting disclosure or use of trade secrets. The Nevada Supreme Court received the case after it consolidated two appeals from Marc Finkel: one challenging the original preliminary injunction entered against him and the second challenging the lower court's denial of Finkel's motion to dissolve the injunction after Finkel terminated a consulting contract containing the restrictive covenants.

Finkel is a former executive with Cashman Professional, Inc. ("Cashman"). While employed by Cashman, Finkel was responsible for expanding and streamlining Cashman's Las Vegas-based wedding photography business. Among other things, Cashman designed business software, negotiated sales contracts with customers, developed new strategies, created training programs, and implemented new management techniques. Cashman went to "great lengths" to keep these aspects of its business confidential.

When Finkel left Cashman in 2008, Cashman and Finkel entered into a consulting agreement ("Agreement") providing that Finkel would abide by restrictive covenants prohibiting Finkel from, among other things, engaging in a business competitive with Cashman, soliciting Cashman's employees, and disclosing Cashman's confidential information.

In 2009, Finkel purchased a printing company which was the only printing company in Las Vegas that could provide overnight printing of wedding photo books ("PrintCo"). Prior to and after Finkel's purchase of PrintCo, Cashman relied on PrintCo when overnight printing services were required. Finkel enlisted several Cashman employees to help establish PrintCo, solicited several Cashman customers to move their business to PrintCo, and in the process disclosed Cashman's confidential information and misappropriated its trade secrets.

Cashman then obtained a preliminary injunction ("PI") against Finkel enforcing the Agreement's restrictive covenants and concluding that Finkel had misappropriated trade secrets in violation of Nevada's Uniform Trade Secrets Act. Finkel appealed the PI order and then exercised his right to terminate the Agreement. Finkel then moved to dissolve the PI upon termination of the Agreement. The lower court denied Finkel's motion to dissolve and Finkel appealed.

The District Court Did Not Err in Granting the Preliminary Injunction

The Nevada Supreme Court found that substantial evidence supported the district court's conclusions that Finkel likely competed with Cashman, solicited Cashman's employees, disclosed Cashman's confidential information, and misappropriated Cashman's trade secrets. The court rejected Finkel's argument that the information used by him were not Cashman trade secrets. Specifically, in rejecting Finkel's argument, the court noted Finkel's admission that costs, discounts, future plans, business processes, technical matters, and product designs are confidential trade secrets to hold that the Cashman information used by Finkel likely constituted trade secrets and that Cashman had taken reasonable measures to maintain the confidentiality of its information.

After Finkel Terminated the Agreement, the District Court Should Have Dissolved the Aspect of the PI Applying to the Restrictive Covenants

The Nevada Supreme Court held that the district court erred by refusing to dissolve the aspect of the injunction enforcing the restrictive covenants. The court reasoned that, because the Agreement was no longer in effect, the restrictive covenants were no longer enforceable. Although this was an issue of "first impression" in Nevada, the court cited the Ninth Circuit decision of *Economics Laboratory, Inc. v. Donnolo*, 612 F.2d 405, 408 (9th Cir. 1979) in support. Ultimately, the court reasoned that it was an abuse of discretion to restrict Finkel's business activities based restrictive covenants within a terminated agreement.

Finally, the Supreme Court held that, under Nevada's adoption of the Uniform Trade Secrets Act, the district court had not made findings as to (1) whether the information alleged by Cashman to be trade secret remained trade secret at the time of Finkel's appeal; and (2) the proper duration of the injunction. The court remanded this issue to the district court for reconsideration.

Takeaways

In Nevada, confidential information that does not rise to the level of a trade secret may nonetheless be protected from disclosure by contract. Breach of such contracts may serve an independent basis to obtain injunctive relief.

Employers should carefully consider how to best structure termination clauses in non-disclosure agreements in order to help ensure that the duration of restrictive covenants within such agreements cannot be prematurely and unilaterally terminated.

Mattel Appeals $310 Million Award in Bratz Case, Argues Trade Secret Counterclaim Was Untimely

By Joshua Salinas (March 12, 2012)

Mattel recently appealed a $310 million award for its alleged misappropriation of MGA's trade secrets and MGA's attorney's fees and costs in defense of Mattel's copyright claim. In its opening brief, Mattel requests the Ninth Circuit to vacate or reverse the award on grounds that MGA's trade secret counterclaim was untimely and barred by the statute of limitations. Mattel also requests that the Court reverse or vacate the trade secret damages award on grounds of insufficient evidence, and reverse or vacate the attorneys' fees and costs award on grounds that Mattel's pursuit of its copyright claim was objectively reasonable.

Statute of Limitations

The statute of limitations for trade secret misappropriation under the California Uniform Trade Secret Act (Cal. Civ. Code § 3426.7) is three years after the plaintiff discovers, or should have discovered, the misappropriation.

MGA filed a trade secret counterclaim against Mattel in August 2010, on grounds that Mattel allegedly stole trade secret information about upcoming Bratz Doll lines during toy fairs. Mattel alleged that the statute of limitations accrued in 2004, when MGA had reason to suspect the alleged misappropriation after it hired two Mattel employees that were aware of Mattel's alleged "toy fair conduct." Thus, Mattel argues that more than three years had passed and MGA's trade secret counterclaim was untimely and barred.

In addition, Mattel argues that the district court erred when it found that MGA's trade secret counterclaim compulsory and related back to Mattel's own trade secret claim in 2006, because the two sets of claims involved different trade secrets that were allegedly stolen at different places and times; by different actors; and through different means.

Insufficient Evidence for Judgment of Trade Secret Liability and Damages

Mattel also requests that the Ninth Circuit reverse or vacate the judgment of Mattel's trade secret liability. Mattel writes in its brief that the "evidence was insufficient to support the jury's verdict that each of the 26 products on which it found liability and damages was a trade secret." Mattel acknowledges that MGA provided evidence that MGA generally made reasonable efforts to protect its trade secrets at toy fairs by protecting information from the press, locking products in separate rooms, and requesting

visitors to sign Non-Disclosure Agreements. Mattel argued that the evidence, however, failed to demonstrate that MGA took these reasonable efforts of protection for each of the 26 products the jury found liability and damages.

In addition, Mattel argues that the evidence is insufficient to support the $85 million for trade secret damages because there is no evidence of identical uniform damages of $3.4 million for each of the 26 products. Mattel requests that the Court vacate or remand the trade secret damages award for a new trial limited to determining damages on these 26 trade secrets.

Attorneys' Fees and Costs

Finally, Mattel argues that the $137.2 million in attorneys' fees and costs awarded to MGA under the Copyright Act for MGA's defense against Mattel's copyright claims should be reversed or vacated. Section 505 of the Copyright Act grants courts the discretion to award reasonable attorney's fees and costs to a prevailing party. The 9th Circuit requires that courts shifting copyright fees and costs to consider the objective unreasonableness, frivolousness, motivation and need for deterrence. Mattel argues that its copyright litigation against MGA was objectively reasonable considering Mattel prevailed before the first, jury, obtained substantial relief, and had the Appellate Court remand the case for a new trial.

MGA has yet to file its response brief. This appeal merits attention and we will keep you updated.

UConn is Dancin' for a Third Reason: Its Donor List is a Trade Secret and Exempt from Freedom of Information Act

By Scott A. Schaefers (March 15, 2012)

The University of Connecticut has a third well-publicized reason to celebrate, beyond its men's and women's basketball teams' berths in the NCAA Tournament. The Connecticut Supreme Court recently held that the University's databases of benefactors, season ticket holders, and others interested in University programs and departments were exempted from a FOIA request on the grounds that the databases were "trade secrets" under the state's FOIA disclosure exemption.

In *University of Connecticut v. Freedom of Information Commission*, 303 Conn. 724, A.3d (Feb. 21, 2012), the Supreme Court rejected the state Freedom of Information Commission's decision that the University's databases could not be "trade secrets" under the disclosure exemption because the University was a public entity that did not engage in "trade." Rather, the Supreme Court ruled that the FOIA trade-secret exemption said nothing about the alleged trade secret owner's status as a private or public entity, and so long as the public agency presented sufficient evidence that the databases met the exemption's definition of trade secrets, which the University did, the databases were exempted from disclosure. The Supreme Court further reasoned that the FOIA exemption's definition of "trade secrets" was identical to that term's definition under Connecticut's Trade Secrets Act, and because the Trade Secrets Act's definition of "person" specifically included government agencies, the FOIA exemption should likewise apply to the University, an undisputed government agency.

Interestingly, the Supreme Court effectively held, without expressly saying it, that the University *does* engage in trade. The Court noted that the trial court, which reversed the commission's decision, held that "a government entity that sells things would have customers, as that term is commonly understood." Thus, the University's "customer" lists (i.e. season ticket holders, donors, theatre subscribers, prospective continuing-education applicants, etc.), generated significant revenue for the University, and thus conferred "independent economic value." This value would be lost if the public could readily access the lists with a FOIA request. So, even though the Supreme Court did not come out and say the University engages in trade by selling tickets to its athletic, theatre, and cultural events, and by marketing its academic and vocational programs to potential applicants, that finding is quite clearly implied. In fact, the Supreme Court did say that:

> "it cannot reasonably be questioned that the university expends considerable resources of the state, on its own or in partnership with others, for the research and development of intellectual property. The state's ability to recoup the costs or *reap the financial benefits* of such efforts would be seriously undermined if any member of the public could obtain such information simply by filing a request under [FOIA]." (emphasis added).

"Reaping the financial benefits" apparently means that a public university should be able to profit from its investment in research and development, and not merely reimburse itself for its out-of-pocket costs. Turning a profit, and not just breaking even, is certainly at the core of engaging in "trade," and some might say inconsistent with the mission of not-for-profit universities.

The impact of this decision may be extensive, and perhaps unintended by the Connecticut Supreme Court. First, public agencies across the country may cite this decision in support of their claims for exemptions under their corresponding FOI Acts. Many states' FOI Acts have trade-secret exemptions from disclosure, and the Uniform Trade Secrets Act, which 46 states, the District of Columbia, and Puerto Rico have adopted, defines "person" in the same way as the Connecticut Trade Secrets Act – to include government agencies. Such agencies under these similar FOI and Trade Secrets statutes might now argue that the products or services they sell at a price (i.e. licenses, permits, utilities, tickets to municipal events, etc.) confer trade-secret disclosure exemption on buyer and subscriber information that otherwise would be subject to FOIA disclosure. Of course, public agencies would have to be prepared to prove that their lists or databases meet the requirements of trade secrecy (that is, that the information is valuable because it is secret, and was kept a secret). But assuming public agencies can jump that hurdle, we may see a spike in FOIA litigation across the country.

Second, will this decision provide ammo to the IRS or state taxing authorities to argue that certain public or quasi-public 501(c)(3) entities which sell products or services above cost should be stripped of their tax exempt status? Many state and local universities and other institutions are classified "charitable organizations" under 501(c)(3), and many of those same organizations have significant in-the-black earnings on ticket sales and merchandising. One may wonder if the IRS, which last year stripped the tax-exempt statuses of 275,000 501(c)(3) organizations for failure to properly renew or maintain their exemptions, will take a closer look at university operating statements in light of this decision.

Keep Your Pot of Gold Hidden, Ohio Court Rules Information Posted Online Not Trade Secret

By Joshua Salinas (March 16, 2012)

St. Patrick's Day calls to mind the traditional Irish folklore of leprechauns and their hidden pots of gold. These hidden pots of gold illustrate the fundamental and straightforward rule for protecting prized trade secret information – keep it secret. A recent Ohio District Court, the Honorable Judge Michael R. Barrett presiding, denied a Plaintiff's Motion for Temporary Restraining Order because the Plaintiff had publicly posted his alleged trade secret information online. (*Allure Jewelers, Inc. v. Ulu*, No. 1:12cv91, 2012 WL 367719 (S.D. Ohio Feb. 3, 2012).

Plaintiff Allure Jewelers, Inc. sells gold jewelry online through eBay, Amazon, and its own website. Allure's competitor, Defendants Mustafa Ulu and Goldia.com, similarly sells gold jewelry online through eBay, Amazon, and its own website. Since both sellers acquire their products from the same manufacturer and distributor, Quality Gold, they often sell the same products.

A dispute arose when Ulu and Goldia.com allegedly "scraped" or copied information about products from Allure's website for their own advertisements and product listings on Goldia.com, eBay, and Amazon. Allure claimed that it spent a considerable amount of time and expense developing its trade secrets, i.e. the details and descriptions of its marketed products.

Ulu and Goldia.com also allegedly used a computer program to automatically list and sell corresponding products calculated at 98% of Allure's advertised prices. Allure claimed that Ulu and Goldia.com were unfairly pricing products to compete with Allure.

Allure brought claims against Ulu and Goldia.com for, inter alia, misappropriation of trade secrets under the Ohio Trade Secrets Act ("OTSA") and unfair competition. Allure also moved for a Temporary Restraining Order to enjoin Ulu and Goldia.com from advertising or selling any products in which they had illegally acquired data from Allure.

The court denied Allure's Motion because Allure demonstrated "little to no likelihood of success on the merits of its claims." The court highlighted the fact that Allure's Complaint failed to provide any allegation that Allure took any efforts to guard the secrecy of the information about its products: "Instead ... [Allure] has published this information on the Internet."

The court also found Allure's unfair competition claim for Defendants' alleged unfair pricing was preempted by the OTSA to the extent it was based upon the misappropriation of trade secrets claim.

The court noted again that Allure's Complaint failed to show any reasonable efforts of secrecy regarding pricing information, which was also publicly available on Allure's website.

This case reiterates the essential secrecy element for maintaining information's trade secret status. Simply put, knowingly and intentionally posting information on the Internet is contrary to preserving or maintaining secrecy. While this decision appears clear-cut and not groundbreaking, the case involves underlying gold and secrecy themes that provide a nice St. Patrick's Day treat. Finally, if you happen to find a hidden pot of gold on St. Patrick's Day, make sure you keep its location a secret and do not post its whereabouts on the Internet.

Utah Appellate Court Holds That "Confidential" Price List Is Not A Trade Secret But A Contract Bid Could Be, And Uniform Trade Secrets Act Preempts Common Law Claims Based On Misusing Confidential Information Not A "Trade Secret"

By Paul E. Freehling (March 21, 2012)

In a recent, lengthy decision involving allegations of deceitful acts and unfair competition, the Utah Court of Appeals largely affirmed the lower court's grant of summary judgment to the defendants with respect to a complaint alleging misappropriation of proprietary data and related conduct. Particularly noteworthy, the appellate court held that the Utah Uniform Trade Secrets Act (UTSA) preempts many common law claims relating to allegations of misuse of confidential information not qualifying as a trade secret. *CDC Restoration & Constr., LC, v. Tradesmen Contractors, LLC*, 2012 UT App. 60 (Feb. 24, 2012).

Paul Carsey was a long-time employee of CDC, a company that repairs concrete and installs protective and decorative coatings. CDC and its customer Kennecott entered into a preferred provider agreement containing CDC's confidential labor and material costs. In January 2006, while Carsey was assisting CDC in the preparation of a Kennecott contract bid, he resigned from CDC and was elected vice president and project developer for Tradesmen Contractors, a CDC competitor.

At the same time, Kenneth Allen worked for an independent project manager hired by Kennecott to supervise projects such as the bidding. Previously, Allen had been a long-time Kennecott employee. Like Carsey, Allen had intimate knowledge of CDC's bid. Shortly before Carsey joined Tradesmen, Allen formalized his ownership interest in that company. According to CDC, both Carsey and Allen went to great lengths prior to CDC's bid submission to conceal their involvement with Tradesmen.

CDC, Tradesmen, and a third company all bid on the Kennecott contract. Tradesmen's bid was lower than CDC's, a fact CDC attributed to Tradesmen's knowledge of CDC's prospective bid. Although Tradesmen's bid was higher than the third company's, Tradesmen was awarded the contract. CDC sued Tradesmen, Carsey and Allen, alleging (among other wrongs) misappropriation of trade secrets – CDC's labor and equipment rates, and its bid – as well as the defendants' intentional interference with CDC's economic advantage.

CDC also accused Carsey of breach of fiduciary duty.

The trial court granted the defendants' motion for summary judgment. The appellate court agreed that CDC had failed to demonstrate that there was a genuine issue of material fact in dispute with respect to most of the counts of its complaint but reversed and remanded for trial the trade secret misappropriation claim relating to CDC's bid. There was no evidence that the pricing information was unobtainable by proper means, or that it required a substantial amount of time and money to develop. Making an argument similar to the basis for a number of court rulings in favor of trade secret claims, CDC maintained that "if Defendants could have easily developed pricing for their [bid] without using CDC's confidential information, why did they not do so?" The Court of Appeals was not persuaded and held that "mere use" of confidential information is neither "sufficient to maintain a finding of trade secret status, [nor] even a factor relevant to that inquiry." Moreover, because Carsey himself had provided input into development of CDC's pricing information, and Allen "lived and worked" this type of data, the court concluded that their general knowledge and experience defeated CDC's trade secret claim. Finally, the equipment rates, at least, were readily ascertainable simply by making an inquiry to equipment rental companies.

Both courts held that CDC's bid was a trade secret, but the trial court reasoned that there was no evidence that the bid was used by the defendants, or that they even knew the amount. CDC persuaded the appellate court that there was sufficient circumstantial evidence of the defendants' use and knowledge of CDC's bid to defeat a motion for summary judgment.

CDC struck out completely on its common law claims relating to misappropriation "of confidential, proprietary, or otherwise secret information falling short of trade-secret status (e.g., idea misappropriation, information piracy, theft of commercial information, etc." This was an issue of first impression in Utah appellate courts and one which has divided that state's federal district courts. Agreeing with a majority of decisions from other states and from Utah district courts, as well as a concern about a ruling that could "undermine the uniformity that motivated the creation and passage of the" uniform trade secrets statutes, the Court of Appeals held that CDC's common law causes of action were preempted by the UTSA because they "are dependent on the same facts as" CDC's trade secrets misappropriation claim. Well aware that this holding produces the harsh result that CDC's common law claims are "preempted by a statute that grants [CDC] no cause of action," the court observed that the UTSA expressly permits protection of "valuable commercial information contractually, regardless of whether such information meets the statutory definition" of a trade secret.

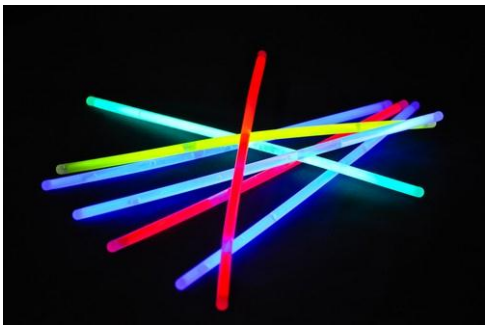
Although for different reasons, the Utah trial and appellate courts rejected CDC's claim that Carsey breached a fiduciary duty to the company arising because he was an employee. Without addressing preemption, the trial court held that there was no evidence of a fiduciary duty. The Court of Appeals observed that Utah law is unclear as to whether an employee owes a fiduciary duty to the employer. However, since the supposed breach of fiduciary duty was based on an alleged obligation not to disclose or use confidential business information, the claim was dependent on "misappropriation-of-trade-secret facts" and, therefore, preempted because those are precisely the facts with which the UTSA deals.

Lastly, neither court found a basis for a trial regarding CDC's averments of tortious interference. While "the evidence supports the allegation that Carsey and Allen did engage in deceptive and deceitful acts," those acts "all were done to facilitate Tradesmen's preparation of the winning bid using CDC's pricing information." Since CDC's claim for intentional interference with economic relations relies "on the misuse of confidential information," that claim also is preempted by the UTSA.

Not all courts would have reached the same result, or would have based the result on the same arguments, as the Utah court did. Other jurisdictions have stronger protections for confidential information that may not rise to the level of a trade secret. One lesson learned is that protecting confidential information by contract may be preferable to reliance solely on a trade secrets statute, at least in Utah.

Denver Club Owner Fails to Bounce His Partner's Trade Secrets Lawsuit for Alleged MySpace Friends Theft

By Scott A. Schaefers (March 23, 2012)



On March 14th, a federal court in Denver, Colorado kept alive an electronic dance club owner's trade secret theft and antitrust lawsuit against one of his former partners, alleging his partner stole his clubs' MySpace "friends" and tried to drive the owner out of the Denver electronic dance market. In *Christou v. Beatport, LLC*, No. 10-cv-02912-RBJ-KMT, 2012 WL 872574 (D. Colo. Mar. 14, 2012), the court ruled that plaintiff, Christou, who owned a group of dance clubs in the Denver area popularly referred as the "SOCO" clubs, could maintain a trade secrets misappropriation lawsuit against his former partner, Bradley Roulier, who owned a competing club ("Beta") and operated an electronic dance music e-commerce site ("Beatport"), for his alleged theft of Christou's compilation of MySpace friends' profiles and contact information. The court rejected Roulier's argument that Christou's MySpace friends were fair game because they were available on the internet.

Key to the court's decision was that Christou did not claim his online list of friends was a trade secret, but rather his relationships with those friends. That is, Christou's efforts and expense in "friending" thousands of potential dance club patrons, and thus having their contact information and permission to contact them, were enough to make his MySpace friendships trade secrets, at least at the early stages of the case. Roulier's use of those friendships to market his Beatport site and draw people to Beta, the court further held, could constitute theft of those secrets. Though the court noted that Roulier might be able, with enough time and effort, to duplicate Christou's friends list, this would involve making thousands of friend requests, and it was uncertain that those people would accept the requests as they did with Christou.

Christou also sufficiently protected its friend relationships, as required by the Colorado Trade Secrets Act, by securing SOCO's profile with a confidential login and password, and distributing that information only to a limited number of his employees (including Roulier) for the purpose of maintaining and updating SOCO's profile.

This decision is not unlike other court decisions allowing companies to sue its employees for alleged theft of online social networking profiles and related information. Seyfarth's trade secrets team also blogged about a December 2011 federal court decision in Philadelphia where the court allowed a former employee to maintain a claim for theft of its LinkedIn profiles, as well as a November 2011 Northern District of California decision allowing an employer to sue a former employee for his unauthorized, post-employment use of its Twitter account. I also recently gave a Skype interview to LexBlog regarding a February 2012 decision allowing a lawsuit to proceed against the operator of Facebook's Farmville app

for alleged theft of concepts and features. These decisions appear careful to protect a company's sweat equity in its online networking profiles, so long as the information is not readily available.

Got Forensics? The Use of Digital Forensics in Trade Secret Matters.

By Jim Vaughn (April 2, 2012)

As a new special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy the first part of a three part blog series by digital forensics expert Jim Vaughn, a Managing Director of Intelligent Discovery Solutions.

In today's world, the amount of communication is astronomical. BYOD (Bring Your Own Device) adds to the complexity layer when already faced with traditional data sources used by most corporations. This article is intended to be a helpful reminder, or for some, new information on things to consider when using digital forensics for investigating potential theft or improper usage of proprietary data.

Consideration of Electronic Storage Areas/Devices

Whether you are working for the Defendant, Plaintiff or as a Forensic Neutral, there are certain electronic data sources one should consider for the investigation. These may include laptops/desktops (aka workstations), email servers, file servers, external media, online repositories, personal email accounts, home computers, smart phones, and other portable computing devices. Some of these sources are self-explanatory, but others may not be. A couple examples include email servers and file servers. Email servers can be configured to keep the email on the server. This is important to understand so as not to assume the email will all be located on a desktop or laptop. One technique may be to synchronize the email to the desktop or laptop before creating a forensic image of that device. This may save you the need to collect the email from the email server.

For servers, it is important to understand the terminology being used. Take a file server for example: a server where individuals or members of certain groups can store loose documents or email archives. It is often referred to as a private network folder or home directory for individuals and as a group share for members of certain groups that have a common area for sharing documents. An example of a group share may be the accounting group share or an engineering group share.

Analysis Considerations

Email, workstations, external devices - where should I start? Data can leave a company in many different ways. Nowadays one way to exfiltrate "large" amounts of data is through the connection of an external device, but be aware it is certainly not the only way, nor should it be considered the most likely

method. With that said, It is very easy to connect an external device, mass copy files to the device, disconnect the device and leave with it. So what artifacts would one expect to see from that type of activity on your commonly used Windows type workstation?

Clients often ask me why I cannot give them a list of files that were copied to an external device. To get this on the record, Windows does not create a "log," "audit trail," or "record" of files that are simply copied to an external device via the drag and drop method. Absent having the actual device that the files were copied to, you must rely on other artifacts to show, or infer, that this activity occurred. One way is through the review of link files. A link file is a shortcut on a local drive that will open a target file on an attached drive or device.

For example, I have a document named tradesecret.doc (aka, the target file). If I save and close that document, then go back to my Windows Start Menu, allow the programs to display, and then move my mouse up to the Microsoft Word Program. This allows me the option to see a list of documents that I can choose from to click on. I choose the entry for tradesecret.doc and I open it.

This method of opening one of those documents creates a link file. A link file exists on the computer because a document was "opened." Link files contain metadata including the path of the target file. The path may be an external device that left the company with the departed employee. The link file will also contain dates and times that the link file itself was created, as well as the creation, modified and access dates of the actual target file. So, what can you do with this information? We may visit this in a future post, but for now let's move on to the next topic.

Online repositories are areas that are "in the cloud". Programs like Carbonite, DropBox, SugarSync, YouSendIt, Mozy, Sharefile, and FTP are but just a few of the hundreds if not thousands of online repositories. Although each may vary slightly in how they are used, in the end they all allow a user to store files. Looking for the installation and usage of these programs on a workstation may prove to be valuable. Visiting these sites may also create a record within the Internet History files. For example, if I were to visit www.sugarsync.com on a certain date and time, this may be in my Internet History file, and this may be information relevant to your matter.

Portable devices and smart phones are capable of storing files. With today's advancement of "apps" it is possible to retrieve, open, edit and resave a document back to a portable device, or to the cloud based area the document was retrieved from. SIM cards from cell phones can maintain contact lists and can be moved from one phone to another compatible phone with ease. Let's not overlook backup files made from Blackberry's, iPads and other portable devices. These may prove to be valuable to show ownership or usage of a particular device that has not been produced for inspection, especially in today's BYOD world where the device may be privately owned, but allowed usage at the company has resulted in corporate data on the device.

Protocols may play an important role in your matter. A well written and agreed upon protocol can save a lot of grief for all parties. This is not always appropriate, and may or may not be necessary for a particular matter, but is something to be considered.

Trading Secrets

This blog post touches on areas where digital/computer forensic analysis can play a vital role. If you find this post useful, feel free to send a note requesting future posts building on this, or other topics.

Mr. Vaughn is a digital forensics expert who has given testimony in nearly 65 cases involving topics such as evidence preservation, documentation of events, and computer forensic methodologies. In addition to being an EnCase Certified Examiner (EnCE), Mr. Vaughn is certified by the International Association of Computer Investigative Specialists (IACIS) as a Certified Forensic Computer Examiner (CFCE). Mr. Vaughn has extensive experience working on litigation and consulting matters involving computer forensics, e-discovery and other high technology issues. He serves his clients through the litigation or consulting lifecycle by assisting them with important issues like data scoping, preserving, gathering, processing, hosting, review and production, as well as deeper diving issues uncovered through the use of computer forensics. Mr. Vaughn can be contacted at jvaughn@idiscoverysolutions.com. Please note that each case may be unique and this single blog post is not intended to fully cover everything related to trade secret investigations or constitute advice, legal or otherwise. It is always best to consult a qualified person to assist with any investigation.

Seventh Circuit Rejects Pool Technology Company's Trade Secrets Claim

By Scott A. Schaefers (April 4, 2012)

On March 29, 2012, the Seventh Circuit upheld summary judgment in favor of a defendant on plaintiff's claims for trade secrets misappropriation and unjust enrichment, holding that plaintiff failed to take any measures, let alone reasonable measures, to protect its alleged trade secrets during joint marketing negotiations with defendant. *Fail-Safe LLC v. A.O. Smith Corp.*, No. 11-1354 (7th Cir. Mar. 29, 2012). The decision highlights the need for written confidentiality agreements signed, sealed, and delivered before people explore doing business with each other.

Fail-Safe developed an anti-entrapment pump which prevents pool drains from trapping swimmers. After A.O. Smith representatives learned of Fail-Safe's pump at a trade show and in a magazine ad, the two companies had several meetings and extensively negotiated A.O. Smith's possibly marketing and selling the pump for Fail-Safe. Never during the negotiations did Fail-Safe require A.O. Smith to sign a confidentiality agreement not to use or disclose the alleged secret technology, nor did Fail-Safe even raise confidentiality during any meeting or correspondence, even though it had done so in the past with other potential marketing partners. The only confidentiality obligation was on Fail-Safe, which signed a one-way confidentiality agreement without asking for a reciprocal obligation from A.O. Smith. The Seventh Circuit held that the failure to take any precaution to protect the technology precluded Fail-Safe's trade secrets claim as a matter of law, rejecting Fail-Safe's argument that whether its protective measures were sufficient was a question to be decided by the jury. The court went so far as to say "you can't steal free advice," and that "Fail-Safe courted its own disaster by failing to take any protective measures."

On the same grounds, the court upheld the district court's summary judgment on plaintiff's unjust enrichment claim, holding that defendant could not have been unjustly enriched if plaintiff did not seek to protect the information. Notably, the court did not address any preemption argument; that is, whether an unjust enrichment claim would be preempted by Section 7 of the Trade Secrets Act.

Missing from the court's opinion was any comment on A.O. Smith's ostensibly suspect conduct in bringing a competing pump to market after Fail-Safe provided A.O. Smith with the necessary know-how. A.O. Smith sought out Fail-Safe to market the pump, not vice versa, and the parties appeared to closely engage each other regarding joint marketing possibilities. Fail-Safe disclosed its alleged secret technology apparently in good faith, and with hopes for future mutual profit. After Fail-Safe sought to commit the parties' relationship to writing, A.O. Smith called everything off, and less than two years later (after a reportedly contentious letter-writing campaign with Fail-Safe regarding their alleged rights in the pump), began selling its own pump. Fail-Safe should have at least asked for a non-disclosure

agreement, to be sure, and the court noted that Fail-Safe waited nearly two years after A.O. Smith began selling its alleged copycat pump before bringing suit – perhaps an inexplicable lapse of time to enforce rights in alleged proprietary assets. Nevertheless, A.O. Smith's alleged betrayal of Fail-Safe's trust appeared to be irrelevant to the court, and the Seventh Circuit's decision may mean that district courts in the circuit can properly condone allegedly underhanded conduct in the absence of a confidentiality agreement or other demonstrable security measures.

Massachusetts Appeals Court Affirms Judgment in Breach of Confidentiality Agreement and Unfair Business Practices Action Involving Weapon Designer

By Erik Weibust and Ryan Malloy (April 5, 2012)

In *Troy Industries, Inc. v. Samson Manufacturing Corporation and Scott A. Samson*, 81 Mass. App. Ct. 1122 (March 21, 2012), the Massachusetts Appeals Court recently affirmed a jury verdict in the Superior Court that awarded damages to the plaintiff, Troy Industries, Inc., based on the defendants' violation of a confidentiality agreement and the Massachusetts unfair trade practices statute, Massachusetts General Laws, chapter 93A ("Chapter 93A").

Troy, a recognized U.S. Government Contractor and weapons designer, sued Samson Manufacturing Corporation and its owner (and former Troy employee), Scott Samson, for breach of a confidentiality agreement and misappropriation of trade secrets and confidential business information. Specifically, Troy sought to enjoin the defendants' unlawful use of its design for weapon accessories that retrofit and upgrade the M-16 rifle, including a firearm handguard for the rifle named the Modular Rail Forend ("M.R.F.") Troy alleged that, in April 2003, former employee and machine parts manufacturer Scott Samson signed a confidentiality agreement, agreeing to hold in trust and strict confidence Troy's confidential business information, and not to use Troy's confidential information for any purpose other than for Troy's own business purposes. During his employment with Troy, Samson gained access to trade secrets involving the design of the M.R.F. and other, complex weapons accessories. In December 2004, Samson allegedly began advertising and selling on his website the M.R.F. and other accessories designed by Troy, representing the products as his own designs.

The jury awarded Troy $499,500.00 in damages for Samson's use of trade secrets or confidential business information, plus $152,000.82 in attorney's fees and costs. The trial court also issued a permanent injunction, barring the defendants from, among other things, manufacturing, contracting to manufacture, or soliciting, advertising, or accepting orders for sale of the M.R.F. or accessories that are substantially similar in design to the M.R.F. and whose design is derived in significant part from confidential information or trade secrets provided to Samson under the confidentiality agreement.

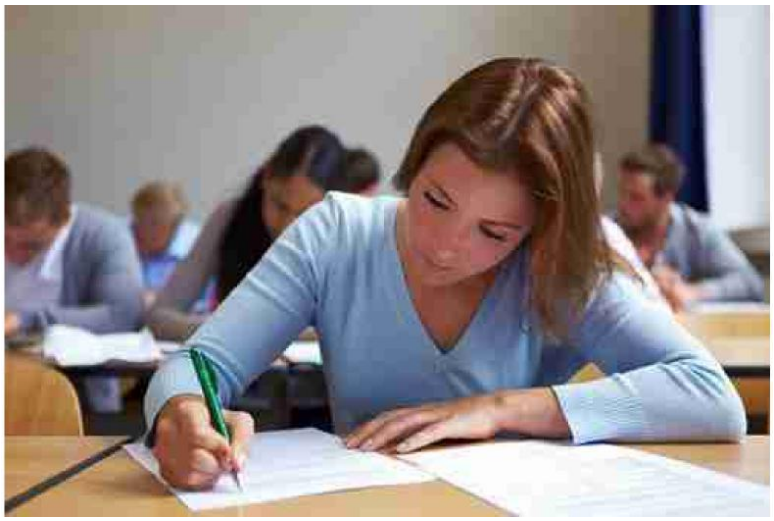
On appeal, the defendants argued primarily (1) that the confidentiality agreement did not create trade secret protection because it did not specify what was confidential, and (2) that Troy publicly disclosed the M.R.F. at a trade show in February, 2004, thereby losing any trade secret protection.

The Court disagreed, finding that Troy took reasonable precautions to protect its trade secrets, including entering into express agreements restricting disclosure, confining the revelation of its trade secrets to Samson so as to avoid their acquisition by unauthorized third parties, stressing confidentiality of the designs and work orally to Samson, and designating drawings as proprietary.

The Court concluded that Samson subsequently used the trade secrets and confidential business information, thereby breaching the agreement with Troy.

Law School Exam-Type Trade Secret Complaint Survives a Specific Pleading Challenge in Colorado Federal Court

By David Monachino (April 24, 2012)



As discussed in today's trade secrets webinar entitled "Pleading, Proving and Protecting Trade Secrets in Litigation," in an all to common theme, the plaintiff in *L–3 Communications Corporation v. Jaxon Engineering & Maintenance, Inc. et al.*, 2012 WL 1020516 (D.Colo. March 27, 2012) contended that several of its former employees devised a plan to leave L3 and create a competing business entity regarding specialty electronic equipment by using, among other things, misappropriated, customer lists and pricing data. In what the Court characterized as "the answer to a law school examination", L3's twenty-six claim Amended Complaint asserted a wide variety of legal theories for recovery, including theft of trade secrets.

Although the Amended Complaint contained some 400 allegations spread over 87 pages, the Defendants moved to dismiss, among other claims, the trade secret claim. The Defendants argued that L3's claim under the Colorado Uniform Trade Secrets Act should be dismissed, because the claim "fails to identify sufficiently any alleged trade secrets, and fails to plead which Defendants allegedly misappropriated such alleged trade secrets." The District Court disagreed and held that although the "Defendants would certainly prefer that L3 be even more specific in identifying each particular allegedly misappropriated trade secret, and that it be prohibited from referencing other alleged trade secrets in more general terms, the Court cannot say that the Amended Complaint is so bereft of specifics regarding any of the trade secrets at issue here that dismissal is warranted."

No Cause of Action Under Georgia's or Utah's Trade Secrets Statutes for Misappropriation of Confidential and Proprietary Information Not Qualifying as Trade Secret

By Paul E. Freehling (April 25, 2012)

Thanks to a recent decision of the Georgia Supreme Court, the assignee of confidential and proprietary information has found itself in a Catch 22 dilemma, precluded from suing under the state's trade secrets statute because the information did not qualify as trade secrets but prohibited by that statute from bringing related common law claims. *Robbins v. Supermarket Equipment Sales, LLC*, 290 Ga. 462, 722 S.E.2d 55 (Feb. 6, 2012). A similar ruling was issued by the Utah Court of Appeals a few days later. *CDC Restoration & Construc., LC v. Tradesmen Contractors, LLC,* 2012 Ut. App. 60 (Feb. 24, 2012). Other courts interpreting the preemption provision of the Uniform Trade Secrets Act are divided.

In the Georgia case, the final act of an insolvent company was to assign its confidential and proprietary library of drawings to an entity newly created for the purpose of conducting the same business, with the same employees, as the assignor. Former employees of the assignor made copies of the drawings and went to work for a competitor. The assignee sued them for misappropriation. The trial court held, and the Georgia Supreme Court agreed, that the assignee was basically engaged in a continuation of the assignor's business and, therefore, had standing to sue even though the misdeed took place before the assignment (indeed, before the assignee even was formed). But in light of the provision in the Georgia Trade Secrets Act stating that the statute supersedes all common law actions for trade secret misappropriation, and notwithstanding the conclusion that the confidential information did not qualify as a trade secret because it was not adequately protected, the supreme court held that the trial court abused its discretion by enjoining the miscreants from using the misappropriated property.

Section 10-1-767(a) of Georgia's trade secrets statute states that the law "shall supersede conflicting tort, restitutionary, and other laws of this state providing civil remedies for misappropriation of a trade secret." Even though the state Supreme Court held that assignee SES' proprietary information did not constitute a trade secret, the court interpreted the statute as precluding common law claims based on the same allegations that underlie the trade secret misappropriation cause of action. The court said: "For the [statute] to maintain its exclusiveness, a plaintiff cannot be allowed to plead a lesser and

alternate theory of restitution simply because the information does not qualify as a trade secret under the act."

The Utah opinion, which was the subject of a Seyfarth Shaw blog shortly after it was issued, emphasized that a uniform act is to "be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of the [trade secrets] chapter among states enacting it." The court cited decisions to a similar effect in state and federal courts of Hawaii, Kentucky, Michigan, New Hampshire (*Mortgage Specialists, Inc. v. Davey*, 904 A.2d 652, 663 (N.H. 2006) (collecting cases holding to the contrary but rejecting them), Ohio (*Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc.,* 649 F.Supp.2d 702, 720-22 (N.D. Ohio 2009) (collecting majority cases), Tennessee (*Hauck Mfg. Co. v. Astec Indus., Inc.,* 375 F.Supp.2d 649, 655 (E.D. Tenn. 2004) (same), and Virginia.

Thus, for plaintiffs in several states, such as Utah and Georgia, pleading misappropriation of proprietary information failing to qualify as a trade secret, the only way around those holdings may be by pleading some form of misconduct that is not based on theft of confidential data.

Parties In High Profile Sports Agent Dispute In California Involving Trade Secret and Non-Compete Issues Throw Off The Gloves

By Jessica Mendelson (April 26, 2012)

The case of *Mintz v. Mark Bartelstein & Associates d/b/a Priority Sports & Entertainment*, recently filed in the Central District of California, provides an interesting look at both non-compete and trade secret law, as seen through the world of a sports agent.

Aaron Mintz, a National Basketball Players Association (NBPA) certified player-agent, allegedly resigned from Priority Sports & Entertainment on March 23, 2012. Immediately following his alleged resignation, Mintz signed a contract with Creative Artists Agency (CAA), a competitor agency.

On the day of Mintz's resignation, he filed a complaint for declaratory relief against Mark Bartelstein & Associates, Inc., d/b/a Priority Sports & Entertainment. Mintz's claim for relief was based on the argument that non-compete agreements are illegal under California law. The terms of Mintz's contract with Priority Sports & Entertainment contained a two-year non-compete clause, which prohibits Mintz from representing any Priority Sports & Entertainment clients, either directly or indirectly. Under the terms of the contract, both parties consented to the jurisdiction of the Illinois State Courts. According to Mintz, however, the court should apply California law and the restrictive covenant should not be enforced because its enforcement would be contrary to public policy, since such provisions are prohibited under California Business and Professions Code Section 16600, restrictive covenants are prohibited in the employment context.

Although the parties' choice of law agreement generally governs which law is applied, in *Hughes Electronics Corp. v. Citibank Delaware,* the court held that if the chosen state's law is contrary to a fundamental public policy of the forum state, the parties' choice of law will not be enforced. Here, Mintz argues that the prohibition of non-compete agreements is a fundamental state policy, and as a result, the court must consider the effect of the non-compete clause, which would restrict him from competing in his trade within the state he lives in, and decide in his favor.

Since the initial complaint was filed, Priority Sports has filed an answer, along with a number of counterclaims against both Mintz and his new employer, Creative Artists Agency ("CAA"). Priority Sports alleges that Mintz and CAA are engaged in "a reckless and relentless claim to improperly solicit Priority Sports' clients by misappropriating and misusing Priority Sports' confidential, proprietary and trade secret information and by tarnishing Priority Sports' and Mark Bartelstein's good name."

According to Priority Sports' counterclaim, Mintz has been working for CAA for months, even though he was still under contract with Priority, a direct competitor.

Priority Sports asserts a variety of counterclaims, including breach of contract, breach of the covenant of good faith and fair dealing, breach of the duty of loyalty, intentional interference with contractual relations, intentional interference with present and prospective economic advantage and business relationships. Additionally, the company alleges misappropriation of trade secrets, conversion, and violation of California Penal Code section 502, stem from Mintz's removal of Priority Sports' property, including files, a laptop, cell phone and office keys, as well as business emails and customer lists sent to his Gmail Account.

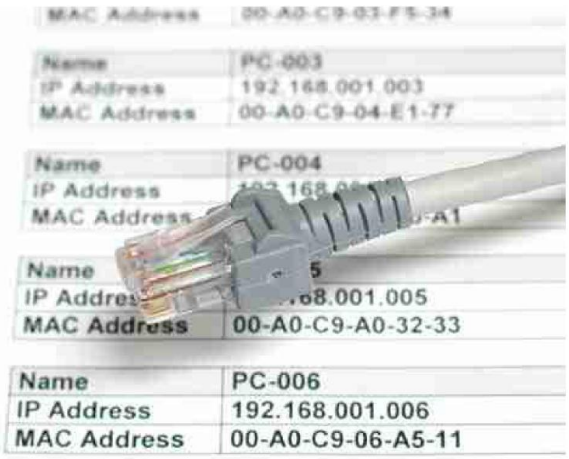
Priority further alleges defamation, trade libel, conspiracy, and unfair business practices under the California Unfair Business Practices Act. The company alleges Mintz made statements defaming both Bartelstein and Priority Sports, including suggesting that he had done "all the work" and that there was likely to be a "mass exodus" of players from Priority Sports' client roster. It is also alleged that Mintz was working for and soliciting clients for CAA, even while he was still employed by Priority Sports, and that Mintz disclosed confidential information to CAA regarding his former employer.

Following Priority Sports' answer and counterclaims, Mintz curiously initiated an additional lawsuit against both Priority and Mark Bartelstein individually in the Central District. Mintz's new lawsuit alleges Priority Sports has engaged in an "unrelenting campaign of illegal conduct," including, "impersonating Mintz in order to gain unauthorized access" to his internet account. Mintz also alleges Bartelstein has made false statements to third parties so as to interfere with Mintz' prospective economic relationships with clients. Mintz asserts seven causes of action: violation of the Computer Fraud and Abuse Act, violation of the Electronic Communications and Privacy Act, violation of the California Data Access and Fraud Act, defamation, invasion of privacy, interference with prospective economic advantage, and unfair business acts and practices.

The court's decision as to whether to apply California or Illinois law is likely to be a key factor in this case, as it plays a significant role in determining whether the non-compete agreement should be enforced. It will also be interesting to see if Priority Sports opens up a second front in Illinois to attempt to enforce the non-compete. Additionally, what the court chooses to consider a trade secret in the sports agency context will also likely play a role in the case's outcome. John Marsh has also blogged on this high profile case on his trade secret blog, Trade Secret Litigator. With all of the allegations each party is making, it is difficult to predict how this case will turn out, but we will continue to keep you posted as the case progresses.

Illinois Federal Court Limits Discovery of IP Address Identification Information from ISPs in John Doe Actions: Highlights Continuing Challenge of Identifying Anonymous Posters Of Trade Secrets and Other Intellectual Property On Internet

By Robert Milligan (April 27, 2012)



As highlighted in our recent webinar, The New Risk: Employee Theft Of Trade Secrets And Confidential Information In The Name Of Protected Whistleblowing, companies continue to struggle with anonymous whistleblowers in the Internet and social media age, including anonymous individuals who post trade secrets and other intellectual property on the Internet. Courts are often reluctant to require internet service providers ("ISPs") to disclose account holder information pursuant to a plaintiff's third party subpoena in a John Doe action against the alleged infringer/misappropriator without a strong showing on the merits by the plaintiff.

In a recent federal case from Illinois, *Pacific Century International, Ltd. v. John Does 1-37,* No. 12 C 1057, Chief Judge James F. Holderman of the U.S. District Court for the Northern District of Illinois granted in part and denied in part plaintiff's motion to compel ISPs' compliance with previously issued subpoenas.

Over the past decade, US courts have seen a marked rise in copyright lawsuits as media companies scramble to protect their intellectual property from digital infringement. Within this landscape, no industry has been more litigious than that of adult entertainment and pornography. To date, over 118 suits have been filed on behalf of producers of pornographic movies with over 15,000 defendants being named in just the last year and a half. Given the anonymity accorded to Internet users, copyright holders are often only able to identify alleged infringers by their IP addresses, requiring them to file against anonymous John Does. During the ensuing discovery, the plaintiffs in these suits often seek subpoenas from ISPs demanding information on the individuals associated with anonymous IP addresses. However, despite their frequency the validity of these subpoenas is often challenged by ISPs.

In *Pacific Century International, Ltd.*, the court held that the subpoenas for information linked to IP addresses specifically named in the suit with direct evidence of infringement should be enforced, but that subpoenas seeking information related to non-party IP addresses should not. The ruling

encompasses six cases, which were consolidated due to their similarities, stemming from four separate cases filed in varying Districts over the infringement of copyrighted pornographic videos shared online using the BitTorrent peer-to-peer ("P2P") file-sharing protocol.

In its analysis, the court outlined what it sees as the typical holding pattern for suits of this nature: (1) the plaintiffs sue large numbers of Doe defendants in a single suit; (2) they obtain through subpoena the identities linked to IP addresses; (3) they threaten the identified parties with legal action, often leveraging them into settlement due to the stigma associated with pornography. Once a subpoena is issued, ISPs are required to inform Doe defendants of the case prior to divulging their information in order to give them the opportunity to dispute the claim. The court noted two arguments used by previous Doe defendants that would compel the court to quash the subpoenas. First, if the Doe defendant does not reside in "the judicial district in which the action was brought" then they may argue that they are not subject to the personal jurisdiction of the court. Second, "the Doe defendants [can] contend that joinder of the defendants is improper under Federal Rule of Civil Procedure 20(a)(2)."

To skirt this judicial hurdle, the plaintiffs in three of the four underlying cases named a single defendant connected to an IP address located in the district where each respective suit was filed, but were seeking through discovery the identities of individuals linked to non-party IP addresses, or those that were not joined as defendants. The ISPs argued, and the courts agreed, that "the identity [sic] of individuals connected with non-party IP addresses is not relevant to the pending claims." Allowing the plaintiffs to justify the subpoena based on the identities' associated with non-party IP addresses relevance to "claims against future defendants who have not yet been sued" was not something the court was willing to accept. The plaintiffs' claim of civil conspiracy was also rejected in all of these cases due to the anonymous nature of the BitTorrent protocol in which users are blind to the identities of fellow users "and have no connection to them beyond the mere fact that they downloaded the same file." The court also struck down the civil conspiracy claim based on the plaintiffs' failure to plead "the existence of an agreement among the alleged conspirators." Based on this reasoning, the court denied the motion to compel the ISPs to comply with the five subpoenas where the identities of non-party ISPs were sought, quashing all five completely.

In the last of the four underlying cases, the plaintiffs named 37 specific defendants with IP addresses located within the jurisdiction of the U.S. District Court for the Southern District of Texas in which plaintiffs brought suit. The corresponding subpoena sought the identity of a single Doe defendant. In evaluating the motion to compel for this case, the court found that the subpoena would be a minimal burden on the ISP and was therefore not subject to rejection based on the court's obligation to protect non-party witnesses from "undue burden." Fed. R. Civ. P. 45(c)(3)(A)(iv). Similarly, questions of relevancy and personal jurisdiction were set aside given that the IP address in question was already a named defendant who resides within the district's jurisdiction. Although the joinder issue of whether the plaintiffs are justified in bringing the suit against these multiple defendants remains, the court reasoned that it was not relevant to the motion to compel the ISPs to comply with the subpoena. The court noted that ISPs have an obligation to notify their customers of the subpoena in order to give them an opportunity to object, which is when it argued that the joinder issue could be settled. For these reasons, the court granted plaintiffs' motion to compel for this case.

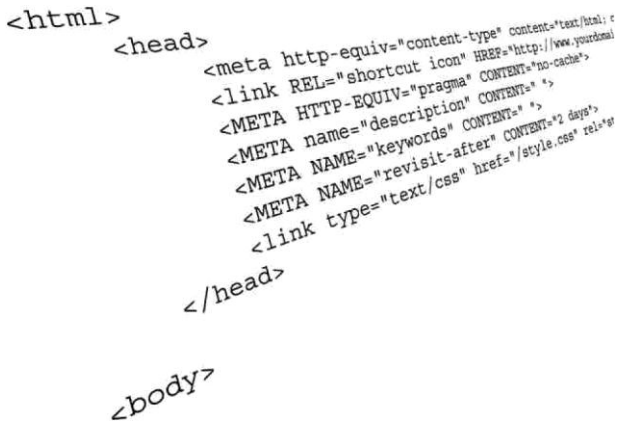
Trading Secrets

Litigating against a group of anonymous individuals can be extremely challenging. While the courts appear to be willing to support subpoenas aimed at bringing pirates hiding behind the cloak of anonymity to justice, they will only do so within the strict constructs of the law. Rather than allowing the wholesale indictment of thousands of alleged infringers in a single suit, many courts have begun demanding a higher standard of proof requiring copyright holders and other intellectual property holders to point to the specific individuals they are accusing of infringement or misappropriation. Moreover, using the process of discovery to unearth information on Internet users potentially subject to future claims is not a practice most judges will tolerate. In order to successfully bring suit against Internet users who have allegedly infringed on protected material, complaints must be carefully tailored to meet the requirements of relevancy, personal jurisdiction, and permissive joinder. Additionally, although the temptation to overreach in these suits can be great, it is imperative that a suit of this nature is not so broad in scope that it could be seen as an undue burden on non-parties, including ISPs. Actively protecting against infringement and misappropriation is critical for any owner of intellectual property, yet a large part of this proactive approach may require a great deal of patience in navigating the legal landscape.

Trading Secrets

In a Case of First Impression, a New York State Court Requires Specific Pleading of a Trade Secret Cause of Action Before Proceeding with Discovery

By David Monachino (May 3, 2012)



In what has been a growing trend across the country, on April 20, 2012, a New York state court has required that a plaintiff specifically plead its trade secrets in detail before proceeding with discovery. In *MSCI et al. v. Jacob and Axioma*, New York State Supreme Court, New York County, No. 651451/2011, the complaint alleged misappropriation of source code trade secrets by Axioma and Jacob, a former MSCI employee who now works for Axioma. Defendants argued that plaintiffs should be required to identify and describe their alleged trade secrets early in a litigation *before* the trade secret defendant produces its own confidential information and trade secrets.

At a conference held on November 21, 2011, the Court stated that, as a plaintiff, MSCI is required to identify its trade secrets; and, in response to MSCI's proposal, as a first step, ordered that MSCI identify with specificity the information that it is *not* claiming to be trade secret. Despite the Court's instruction, five months later defendant MSCI again sought judicial intervention because it claimed that Axioma was seeking to delay discovery in order to avoid having to submit its own source code for inspection.

The New York Court agreed with the defendants noting that "[m]erely providing defendants with plaintiffs' 'reference library' to establish what portions of their source code are in the public domain shifts the burden to defendants to clarify plaintiffs' claim." The Court went on to hold that: "[o]nly by distinguishing between the general knowledge in their field and their trade secrets, will the court be capable of setting the parameters of discovery and will defendants be able to prepare their defense."

April Fools' Day Prank Leads To Trade Secrets Litigation

By Paul E. Freehling (May 7, 2012)

A recent federal decision from Connecticut confirms the notion that information knowingly posted on the Internet by its owner cannot constitute a protectable trade secret.

On April 1, 2011, April Fools' Day, a human relations consulting firm SharedXpertise allegedly disseminated by email and on its website a false statement that it had acquired its competitor LRP Publications. Kutik, a consultant for LRP, was offended. He promptly sued SharedXpertise in the Connecticut federal court and alleged unfair competition, violation of the Connecticut Unfair Trade Practices Act, and other causes of action. He claimed that as a result of the press release, potential vendors and attendees signed up for SharedXpertise's May 2011 conference instead of LRP's competing event scheduled for October 2011.

Kutik served interrogatories and a request for production which would have had the effect of requiring SharedXpertise to identify the sponsors and providers for the May event. SharedXpertise objected and sought a protective order permitting the information to be produced for "attorneys eyes only" because, supposedly, it constituted confidential trade secrets. According to SharedXpertise, the only legitimate use of the information was to facilitate a comparison of the names on the list with the names of persons and entities expected to attend, but not attending, the October conference, and the attorneys could make this comparison. Kutek disputed the claim that SharedXpertise closely guarded its customer list, pointing out that the requested information was prominently displayed on SharedXpertise's website, and an attendance list was handed out at the conference. Further, he said that his own analysis of the information, based on 22 years in the industry, would be more efficient than his counsel's review alone.

Magistrate Judge Margolis issued a compromise ruling. She ordered SharedXpertise to produce without an "attorneys' eyes only" restriction information "readily available on defendant's website," but she permitted SharedXpertise to limit to Kutek's attorneys access to names "not openly identified through resort to defendant's website" *Kutik v. SharedXpertise Media, LLC*, 2012 WL 1435288 (D.Conn. 2012). The court's ruling confirms that although an entire list of customers may not constitute a trade secret, a portion or sub-set of the list that is not publicly available may qualify for trade secret protection.

California Federal Court Transfers Trade Secret Dispute Involving High-Tech Gloves To New York

By Robert Milligan (May 9, 2012)

In today's dynamic environment of interstate commerce, including internet transactions, deciding on the proper venue for a trade secret misappropriation dispute can be a complicated process involving a number of different factors particularly if the parties are domiciled and/or transact business in different states.

In the case of *GLT Technovations, LLC v. Fownes Brothers & Co*., 2012 WL 1380338 (N.D. Cal.), District Judge Ronald M. Whyte of the U.S. District Court for the Northern District of California granted the Defendant's Motion to Transfer pursuant to 28 U.S.C. § 1404(a) and sent the case to the Southern District of New York where a related case was already pending. Section 28 U.S.C. § 1404(a) provides that "[f]or the convenience of parties and witnesses, in the interest of justice, a district court may transfer any civil action to any other district or division where it might have been brought or to any district or division to which all parties have consented."

According to the pleadings, the Plaintiff, GLT Technovations, LLC ("GLT"), is a California based company registered in Nevada that has developed a "capacitive leather" technology called TouchTec. This technology allows TouchTec glove-wearers to control devices with capacitive touch screens, such as the iPhone, without having to expose their hands to the elements. According to the pleadings, while GLT developed the technology independently, it has partnered with Massachusetts based Broleco Worldwide, Inc. ("Broleco") to handle the exclusive manufacturing of TouchTec. Broleco is authorized by GLT to handle marketing of the technology to third party apparel manufacturers. In addition, GLT allows Broleco to share its trade secret information, including "capabilities, functionality, upcoming products and techniques related to the use of capacitive leather," with potential third party partners after said parties have signed non-disclosure agreements ("NDA").

According to the pleadings, in September 2009, the Defendant, Fownes Brothers & Co. ("Fownes"), expressed interest in licensing TouchTec after witnessing GLT's presentation of the technology at New York City's "Fashion Week." GLT and Fownes entered into an NDA, delivered to Fownes by Broleco, soon after in April 2010 while the two companies explored pursuing a business relationship. In the subsequent months, Broleco sales representatives visited Fownes' offices in New York to sell them on the idea of using the technology. In February 2011, Fownes purchased two orders of TouchTec leather from Broleco, and also visited Broleco's warehouse located in Johnstown, New York. Not long after,

Fownes announced the development of its own technology similar to TouchTec, and has not placed any additional orders for GLT's product since.

Reacting to what it believes is the misappropriation of its proprietary trade secret information, GLT distributed a letter to Fownes' potential retail partners in January 2012 informing them of its claims and the potential dangers of selling Fownes' products. In response, Fownes filed a complaint before the U.S. District Court for the Southern District of New York alleging "violations of the Lanham Act, unfair competition and tortious interference with business relations." Just four hours later, GLT filed a complaint before the U.S. District Court for the Northern District of California "seeking a declaratory judgment that it did non violate the Lanham Act," and alleging the misappropriation of its trade secrets, breach of the NDA and unfair competition. Fownes then filed a Motion to Transfer the suit to the U.S. District Court for the Southern District of New York, which Judge Whyte granted on April 20, 2012.

In consideration of transfer under 28 U.S.C. § 1404(a), Judge Whyte evaluated the eight factors "to determine whether transfer is appropriate" laid out in *Williams v. Bowman*, 157 F.Supp.2d 1103, 1106 (N.D.Cal.2001). They include: "(1) the plaintiff's choice of forum, (2) convenience of the parties, (3) convenience of the witnesses, (4) ease of access to the evidence, (5) familiarity of each forum with the applicable law, (6) feasibility of each forum with the applicable law, (7) any local interest in the controversy, and (8) the relative court congestion and time of trial in each forum."

For the first factor, Judge Whyte noted that "a plaintiff's choice of forum should be afforded substantial weight[,]" but that this should be given less consideration when the activities alleged in the complaint have little to no connection to the forum. Although GLT is based out of California, all of its interactions with Fownes - including those done through Broleco - occurred in New York. Given that the "center of gravity" of the dispute is in New York, the court weighed this factor in favor of the Defendant.

The second and third factors, or so-called "convenience factors," do not only take into account the number of witnesses who would be inconvenienced by hearing the suit in either forum, but also the potential quality and relevance of their testimony to the issues in the case. GLT's complaint is almost entirely based on Fownes' interactions with Broleco, which occurred in New York between companies based out of New York and Massachusetts, respectively. Since the Southern District of New York would undeniably be more convenient to the employees of these two entities, as well as to any non-party witnesses yet to be named, Judge Whyte weighed these two factors in favor of the Defendant.

For the same reasons used to weigh factors one through three in favor of the Defendant - namely the relevant interactions between Fownes and Broleco all taking place in New York - the court weighed factor four (ease of access to the evidence) in favor of the Defendant.

Arguing its case for weighing the fifth and sixth factors in its favor, GLT asserted that the case should be heard in a California court because its claims arise under California statutes and common law. In response, Judge Whyte cited multiple district court decisions where federal courts were deemed "fully capable of applying California law." Similarly, although the NDA contained a California choice-of-law provision, the court noted that the provision, unlike a forum selection clause, was not "determinative in

resolving a motion to transfer." With Fownes' own suit against GLT still pending in the Southern District of New York, the court stated its preference for both cases to be heard and decided by a single judge familiar with the facts and arguments of the case.

Evaluating the final two factors, Judge Whyte did not find a compelling reason to deny the Defendant's Motion to Transfer. Although Judge Whyte agreed with GLT that California has a distinct interest in protecting the intellectual property rights of local businesses, "the bi-coastal nature of the transactions...and the parties impacted by this case" make it so that neither forum has a greater interest or right to hear the case than the other. With regards to the final factor, since neither GLT nor Fownes argued for or against transfer based on the congestion of either court, the court considered "that factor to be neutral."

Taking all eight factors into account, Judge Whyte determined the overall weight of the facts to be overwhelmingly in favor of transfer to the U.S. District Court for the Southern District of New York. In particular, the court focused on "the convenience to the witnesses, the ease of access to evidence, and the possibility of consolidation with other litigation" in granting the Motion to Transfer.

The court's decision underscores the importance of including mandatory forum selection clauses in nondisclosure agreements to secure a party's desired forum and filing first in contentious trade secret disputes.

North Carolina Federal District Court Confirms Importance of Alleging Actual Harm in Pleadings

By Jessica Mendelson (May 10, 2012)

On April 25, 2012, a federal judge in North Carolina issued a ruling granting in part and denying in part motions to dismiss involving claims for trade secret misappropriation, breach of contract, and conversion in a dispute between two pharmaceutical companies in the case of *River's Edge Pharmaceuticals v. Gorbec Pharmaceutical Services, Inc*. This decision confirms, to an extent, the need to plead actual, rather than speculative harm to prevent dismissal for failure to state a claim.

River's Edge Pharmaceuticals ("River's Edge") is a company which distributes pharmaceutical products and aims to provide "reasonably priced alternatives to costly name brand pharmaceuticals." The company began marketing and developing certain alleged unapproved pharmaceutical products through an FDA approved process known as Drug Efficacy Study Implementation ("DESI").

In 2007, River's Edge began working with another pharmaceutical company, Gorbec, to manufacture DESI drugs and test and formulate generic drugs under the Abbreviated New Drug Application ("ANDA") process. According to the pleadings, the parties agreed to a contract, and agreed the terms would be memorialized in writing, however this was never actually done. River's Edge began submitting purchase orders to Gorbec, however, and Gorbec performed according to the agreed upon terms.

River's Edge alleges that beginning in 2010, Gorbec's executives began making statements about how they owned the "know-how, intellectual property, and regulatory approvals" which River's Edge had hired and paid them to develop. According to River's Edge, these statements were made despite the fact that River's Edge was the actual owner. In addition, Gorbec threatened to stop work on River's Edge's products, and made statements of intent to compete with the company. River's Edge alleges that all of these actions would harm the company and would worsen its chances of getting FDA approval. Gorbec, by contrast, alleged it had agreed to manufacture these drugs based on River's Edge's representations and proceeded to do so for three years. However, Gorbec alleges that during that time, River's Edge received a warning letter from the FDA asking the company to cease sales. River's Edge allegedly failed to tell Gorbec about it. Gorbec alleges River's Edge also failed to pay in full for the work they had performed.

River's Edge filed a complaint against Gorbec and its President, J. Michael Gorman, in the Middle District of North Carolina, requesting declaratory relief, and alleging breach of contract, breach of

fiduciary duty, constructive fraud, promissory estoppel, unjust enrichment, conversion, misappropriation of trade secrets, and punitive damages. Gorbec filed a counterclaim, alleging breach of contract, unjust enrichment, negligent misrepresentation, fraud, and unfair and deceptive trade practices.

Both parties recently filed motions to dismiss. Gorbec moved to dismiss all counts of the amended complaint, except for declaratory relief, while River's Edge moved to dismiss each and every one of Gorbec's counterclaims.

With regard to breach of contract claim, the court granted Gorbec's motion in part to the extent the claimed breach was based on Gorbec's statements of ownership or intent to compete, but denied the motion to the extent the breach alleged pertained to Gorbec's cessation of ANDA-related work.

Similarly, with respect to the breach of fiduciary duty claim, the court granted the motion to dismiss to the extent the claim was based on Gorbec's threatened or potential conduct, but denied the motion to the extent the claim was based on Gorbec's refusal to provide River's Edge with complete copies of communications with the FDA and info regarding pending ANDAs and said things suggesting ownership of River's Edge's intellectual property. The court also dismissed the claims for constructive fraud and unjust enrichment, holding the plaintiff's allegations failed to state a claim. The court however found that there were sufficient facts to state a claim for both conversion and misappropriation of trade secrets. On the misappropriation of trade secrets cause of action, however, the court held that while there was sufficient facts to state a claim, the burden would be on River's Edge to show Grobec had the opportunity to acquire, use and disclose such information without consent.

With respect to Gorbec's counterclaims, the court dismissed the claim for negligent misrepresentation and denied the motion to dismiss for unfair and deceptive trade practices and unjust enrichment, finding sufficient information to state a claim. Additionally, the court found Gorbec had sufficiently alleged a claim for breach of contract regarding the work Gorbec had done for the ANDA process, but dismissed the claim to the extent it was based on River's Edge's failure to enter into a marketing agreement. Similarly, the court denied the motion to dismiss the count of fraud to the extent it was based around River's Edge's fraudulent concealment of the warning letter, but dismissed the claim to the extent it was based on the idea that River's Edge formed its own manufacturing company in order to get around its contract.

The Court's ruling suggests the need to plead with specificity. Here, claims based on speculative damages, and threatened or potential conduct failed to survive dismissal. This confirms the importance of alleging clear harm in one's pleadings, and shows that to gain a more favorable result for a client, a pleading needs to be framed in such a way that it avoids speculation.

Trading Secrets

Trade Secret Theft Prosecution Cases In The News

By Justin K. Beyer (May 16, 2012)

During the past week, federal courts around the country have seen a handful of high profile pleas, convictions and sentencing in cases in which defendants are accused of stealing their former employer's trade secrets.

On May 7, 2012, Yuan Li, a former research scientist with Sanofi Aventis, who had pled guilty to one count of violating 18 U.S.C. § 1832 (the section of the Economic Espionage Act dealing with commercial economic espionage) in January 2012, was sentenced to 18 months in prison by the United States District Court for the District of New Jersey. In pleading guilty, Li, a Chinese national, admitted to stealing data on Sanofi's compounds, including their chemical structures, and sending that data via email or through use of a thumb drive to her home computer. Li was also ordered to pay $131,000 in restitution damages to Sanofi.

Later that same week, on May 9, 2012, the United States District Court for the Northern District of California convicted former Silicon Valley engineer, Suibin Zhang, of five counts; three counts for his theft and copying of trade secrets and downloading the trade secrets from a secure database, one count for duplication of trade secrets, and one count for possession of stolen trade secrets. This verdict followed a two-week bench trial before Judge Ronald M. Whyte, which concluded on November 9, 2011.

The evidence presented against Zhang during trial showed that, while employed as a project engineer for Netgear, Inc., he accessed the secure database of Marvell Semiconductor, Inc., downloading information with the intent of using that information after accepting a job at Marvell's chief competitor, Broadcom Corporation and later loading Marvell's trade secret information onto his Broadcom laptop. Zhang will be sentenced on August 27, 2012, and could face 10 years in prison, up to $250,000 in fines, plus restitution damages to Marvell if the court deemed such restitution damages appropriate.

Also last week, on May 11, 2012, former Frontier Scientist Inc. chemist, Prabhu Mohaptra, entered a guilty plea in the United States District Court for the District of Utah, pleading guilty to one count of unlawful access to a protected computer. Mohaptra's guilty plea was in exchange for the government dropping 25 other charges against him.

Mohaptra admitted to improperly accessing Frontier's chemical resource notebook and emailing certain chemical formulas to his brother-in-law in India. Mohaptra's case marks the first time that the Economic

Espionage Act was used to prosecute a case in Utah. Mohaptra is scheduled for sentencing on August 28, 2012, at which time he faces up to five years in prison.

Each of these cases highlight the need for companies to monitor the access of its employees to secure databases. Companies should consider using additional preventive means to prohibit employees from stealing trade secrets, such as configuring the operating system to restrict access to external devices, thus, restricting the ability to download information to an external device; blocking a user from uploading information to a web-based site; and/or utilizing software that blocks employees from sending emails to certain domain names. In situations like this, companies may also wish to consider placing blocks on the ability of its employees to email certain domain names that are known to be used for personal email accounts. In an era in which data is becoming increasingly portable, companies much increase their vigilance in monitoring use and exporting of its data and trade secrets.

Trading Secrets

Another Federal Court Holds That A Compilation Of Non-Trade Secret Data Can Be A Trade Secret; Court Also Holds That An Unambiguous Written Contract With A Provision Precluding Unwritten Amendments Nonetheless Can Be Modified By Conduct

By Paul E. Freehling (May 17, 2012)

A collaboration between Beacon Wireless Solutions and Garmin International to integrate Beacon's Global Positioning System fleet management vehicle tracking program into Garmin's personal navigation devices has gone awry. Allegedly without Beacon's knowledge or consent, in order to boost Garmin's sales, Garmin allegedly published to Beacon's competitors Beacon's confidential integration application specifications. Beacon sued, alleging trade secret misappropriation, breach of contract, and unjust enrichment. A few days ago, basing his decision on Kansas law, a U.S. District Court Judge in Virginia denied most of Garmin's motions for summary judgment. *Beacon Wireless Solutions, Inc. v. Garmin Int'l, Inc.*, Civ. Ac. No. 5:11-cv-0025 (May 9, 2012).

In its motion directed at the misappropriation count, Garmin asserted that, far from being kept confidential, Beacon's supposed design trade secrets are displayed to Beacon's customers and derive no value other than by public use. Beacon responded that it is not the individual features but their combination that is confidential, is not easily duplicated, and that enables Beacon's fleet management system to communicate with a Garmin device. In addition, Beacon maintained that it transferred technical information to Garmin which was a trade secret and did not, as Garmin insisted, constitute mere problem-solving support. The court determined that a jury trial is necessary because genuine issues of material fact exist with regard to whether the combination of design features, and the transferred technical information, constitute trade secrets under Kansas law. However, Garmin's summary judgment motion was granted as it related to Beacon's source code and other technical details of Beacon's software to which Garmin did not have access.

Beacon also avoided summary judgment on its breach of contract count. Under the parties' non-disclosure agreement, "Confidential information" was defined "to include, but is not limited to" data "relating to a party, its business or products which is marked as confidential or proprietary." Beacon claimed Garmin breached by disclosing data even though it was not marked "confidential or proprietary" because either (a) the agreement expressly prohibited such disclosure (by using the

phrase “includ[ing] but not limited to”), or (b) a question was raised, to be determined by the court, as to whether the agreement was ambiguous in this respect.

The court ruled that the agreement was unambiguous and clearly requires that information must be labeled as confidential or proprietary to qualify as “Confidential Information.” Surprisingly, however, the court went on to say that “this legal conclusion does not end the analysis” and that a material question of fact remains.

Beacon and Garmin exchanged unlabeled information and mutually promised to treat it as confidential. Despite a clause in the original contract stating that it could only be amended by a writing signed by both parties, “there is persuasive authority under Kansas law. . . supporting the proposition that an unambiguous written agreement . . . may be modified by a subsequent” unwritten accord. A “reasonable jury could determine that there was a meeting of the minds by the parties, evidenced by their course of conduct, to enter into an agreement to modify the Nondisclosure Agreement’s clause regarding how information exchanged by the parties could qualify as ‘Confidential Information’ under the contract.”

Finally, Beacon dodged a summary judgment bullet regarding the unjust enrichment count because Beacon gave Garmin more than simply trade secrets. In the court’s view, “a reasonable jury could find that [Beacon’s] provision of ancillary services to [Garmin], which falls outside the purview of the Nondisclosure Agreement, bestowed a benefit upon [Garmin] under circumstances that would render inequitable the retention of that benefit.”

Recent case law is consistent with the court’s conclusion that a unique combination of secret and non-secret information, that affords a competitive advantage and is not readily ascertainable, is a trade secret. *See, e.g., Avid Air Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 972 (8th Cir. 2011) (Indiana and Missouri law) (this case was the subject of a recent Seyfarth Shaw trade secrets blog); *Tewari De-Ox Syst. v. Mountain States/Rosen, L.L.C.*, 637 F.3d 604, 613 (5th Cir. 2011) (Texas law); and the dissent in a recent unreported Fourth Circuit decision, *Hill Holliday Connors Cosmopulos, Inc. v. Greenfield*,433 Fed. Appx. 207, 222-23 (2011 U.S. App. LEXIS 11241). The more unusual ruling in the *Beacon-Garmin* litigation is that a written contract can be deemed modified by the parties’ course of conduct despite a provision precluding unwritten-unsigned amendments. *Readers of this blog should take particular note of that risk.*

The Use of Digital Forensics in Trade Secret Matters (Part 2 of 3)

By Jim Vaughn (May 23, 2012)

As a special feature of our blog – special guest postings by experts, clients, and other professionals –please enjoy the second part of a three part blog series by digital forensics expert Jim Vaughn, a Managing Director of Intelligent Discovery Solutions.

This post is designed to build on Part 1 of this three part series on digital forensics. Part 1 addressed the subject of BYODs ("Bring Your Own Devices) in the workplace.

Staying on the subject of BYODs, what are the company policies and rules for these hybrid devices? Does your company have well-written policies, such as whether the employer can remotely "wipe" the entire device (business and personal data) if the device is lost, or if the employee and the company part ways? Have you considered how to deal with that issue before it happens?

IT departments originally focused on managing infrastructure, (tier 1 support), but this causes new challenges as employees use a greater variety of devices to access data in both the employer's network (or cloud) and from their own personal sources.

From a digital forensic perspective, this may have implications that counsel should address. If a company does not ban BYOD outright, they should try to manage the risk of security breaches, prepare for the worst, and manage employee expectations.

In addition to implementing and reinforcing a culture of security, and reserving the ability to "wipe" devices if they are lost or stolen; companies should also consider ongoing training, annual acknowledgements, and otherwise set and manage employee expectations about the privacy they will have to surrender in exchange for the convenience of using their personal devices for work.

Privacy? Aren't employees already mixing personal and business information? Yes, they are. But in a non-BYOD environment, this is typically an employee putting personal information on a portable work device.

This does not trouble privacy experts and judges as much as an employee putting work information on a portable personal device.

Should the need to examine portable devices arise, what are some of the artifacts one could look for to ensure confidential company data has not been taken, or no longer resides on a departed employee's device? In my Part 1 post I mentioned backup jobs created by portable computing devices, such as Blackerry's, iPhones/iPads or Android devices.

Let's assume you have reason to inspect a portable computing device (e.g. your forensic examiner found applicable backup jobs on the departed employee's work computer).

Examples of artifacts to look for may include; attachments that have been broken apart from an email and saved to the device, installed software that allows a direct connection to a company computer that may bypass a particular security protocol, names of file attachments that may exist within personal email accounts on the device, pictures that may have been taken of a trade secret document in lieu of the actual file being taken, Internet history and/or text messages, just to name a few. The data on the actual device may differ from the last backup, especially if the device is used more frequently and more recently than the last backup.

Similar to an official BYOD policy - what about the usage of personal or home computers for work? It is not uncommon for employers to allow employees to utilize home computers for work, whether they realize they are allowing it or not. Some of the ways this occurs is by enabling web access to company email; allowing a personal computer to connect to a company network through a virtual private network connection (aka VPN connection); by allowing access to personal email accounts while at work; by allowing access to personal cloud storage areas while at work; or by allowing un-controlled portable devices to be used on work computers with no controls in place.

Many of these access rights can be monitored, limited or excluded, according to your needs and situation. For example, USB ports can be configured as read-only, essentially preventing the exportation of data.

What if the user is actually someone who is granted certain administrative rights within the company because it is part of their job responsibility, but they have then allegedly abused those rights post-employment or prior to departure?

In a recent case, an employee is actually accused of setting up DropboxTM on the company server before leaving the company and having the software automatically backup (export) the company data on a near-real-time basis.

In my experience as a forensic expert (I am not an attorney), there has always been a delicate balance of interest by courts regarding the importance of preserving potentially relevant data from home computers while maintaining individual privacy concerns. Sometimes referred to as proportionality, sometimes referred to as the balance between relevancy and prejudice.

In *United Factory Furniture Corp. v. Alterwitz*, 2012 U.S. Dist. LEXIS 48795 (D. Nev. Apr. 6, 2012), the court approved of a mirror imaging protocol of the defendants' computers. The case generally involved an employee's alleged misuse of company information and improper access to a server. The court

concluded that the appointment of a third-party neutral expert to image and collect hard-drives was the appropriate way to satisfy the competing interests at stake. In some cases, the mere usage of a home computer may, whether intentional or not, destroy potentially relevant data. Some data is more transitory than other and in this case an important fact may be to show how this alleged improper access was occurring from the computer(s).

I will share some thoughts on what a forensic examiner may look for in this matter, but would like to note the following; I have no facts about this case other than reading the summary of the court's order, I am merely providing thoughts on what may be looked at without knowing the facts and therefore the analysis I refer to may or may not be relevant for this particular matter. Part of the allegation is that one of the defendants had IT expertise, and had used that expertise to access the plaintiff's server using a "back door" he created, and that he had "manipulated, copied, transferred, deleted and/or used" data, files, and other information.

The term "back door" as used here simply refers to a way for someone to access a particular computer while circumventing normal security protocols. In this case it sounds like the IT person has been accused of creating an unauthorized account. One of the recommendations made to companies is to perform an audit every so often for potentially rogue network accounts, especially if you have an IT person leave the company. Certain logs, if available may be used to show access dates and times, as well as where the access was made from. The varying methods of tracking such access may be through a user name and password and/or by capturing an IP address, which is essentially the equivalent of a street address.

The logs (or records) may be available from the firewall, VPN router, server(s) and/or the person's computer used to perform the access to the server. All of these sources are dependent on configuration, length of time, whether they were being stored to begin with, etc. Manipulation, copying or transferring of data can be examined from different angles. Aside from content analysis between an original document and an alleged manipulated document, an examiner can look at metadata. Generally, when a document gets manipulated (altered), the operating system metadata will reflect the date and time for such activity. When a document is deleted, you may be able to reference when, or at least within a window of time the deletion occurred. If a document was opened on a computer that was connected to the server, you may find text fragments on the computer in the area known as unallocated, or slack space.

The transferring of files is not always easy to detect. As mentioned in Part 1, there is no record that tells you the name of files that were, for example, copied to a connected USB device. However, the evidence may show that on a certain date and time a USB device was connected, and then hundreds of files (last access) dates were triggered. Assume the triggering of these last access dates were not from some automated process such as a virus scan, could you infer those files were copied to the connected device? These are but a few suggestions of things to look for. In my next post, Part 3, I will delve into protocols with greater detail.

Trading Secrets

Mr. Vaughn is a digital forensics expert who has given testimony in nearly 65 cases involving topics such as evidence preservation, documentation of events, and computer forensic methodologies. In addition to being an EnCase Certified Examiner (EnCE), Mr. Vaughn is certified by the International Association of Computer Investigative Specialists (IACIS) as a Certified Forensic Computer Examiner (CFCE). Mr. Vaughn has extensive experience working on litigation and consulting matters involving computer forensics, e-discovery and other high technology issues. He serves his clients through the litigation or consulting lifecycle by assisting them with important issues like data scoping, preserving, gathering, processing, hosting, review and production, as well as deeper diving issues uncovered through the use of computer forensics. Mr. Vaughn can be contacted at jvaughn@idiscoverysolutions.com. Please note that each case may be unique and this single blog post is not intended to fully cover everything related to trade secret investigations or constitute advice, legal or otherwise. It is always best to consult a qualified person to assist with any investigation.

Trading Secrets

California Federal District Court Examines Personal Jurisdiction Issue in International Trade Secret Misappropriation and Breach of Contract Dispute and Maintains Suit Brought Against Irish Company and Owner

By Robert Milligan (May 27, 2012)

In a recent federal case out of California, Judge Morrison C. England, Jr. of the U.S. District Court for the Eastern District of California examined the issue of personal jurisdiction in an international trade secret misappropriation and breach of contract dispute. The case, *Vance's Foods, Inc. v. Special Diets Europe Limited, et al.*, No. 2:11-cv-02943- MCE-GGH, centers around contracts governing the business relationship between an American company and a European distributor based out of Ireland. Using a three-prong test promulgated by the Ninth Circuit to determine the court's right to exercise specific jurisdiction over a defendant, Judge England granted in part and denied in part Defendants' Motion to Dismiss.

The Plaintiff, Vance's Foods, Inc. ("VF"), is an Alaskan corporation with its principal place of business in Sacramento, CA. VF produces and distributes a non-dairy milk substitute called DariFree™. According to the court's order, in October 2007, VF entered into two written agreements with the Defendants, Special Diets Europe Limited ("SDE"). The first contract, referred to as the "Distribution Agreement," made SDE the exclusive distributor for DariFree™ in a specified area of Europe. The second contract, known as the "Product Development Agreement" gave SDE permission to use VF's product formula, manufacturing process, and list of ingredient suppliers to develop and distribute a liquid stable version of DariFree™ in Europe. VF gave SDE this information with the caveat that they keep it confidential, use it only for the stated purpose of the contract (successful development of the liquid stable version within 8 months), and return the information upon VF's request or the termination of the agreement. In its initial complaint, VF claims that SDE, along with its owners and directors Eamon and Mariel Cotter, entered into this agreement with the sole intention of misappropriating and using VF's confidential information. In response, SDE and the Cotters filed a Motion to Dismiss for Lack of Personal Jurisdiction pursuant to Federal Rule of Procedure 12(b)(2). SDE is an Irish corporation with its offices located in Ireland. Individual defendants Eamon Cotter and Mariel Cotter are citizens and residents of Ireland. The Cotters are the sole owners and directors of SDE.

The Defendants did not challenge general jurisdiction over them, so the Court employed the "three prong test to determine whether a court can exercise specific jurisdiction over a defendant" first used by the Ninth Circuit in *Brayton Purcell LLP v. Recordon & Recordon*, 606 F.3d 1124, 1128 (9th Cir.2010). The first prong of this test requires that the non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws.

This first prong is primarily concerned with establishing a link between a defendant and the forum in which the case is being heard. This link is best established by either showing proof of direct activity related to the complaint within the forum, or by showing that the defendant has deliberately created an ongoing business relationship with forum residents and is therefore subject to "the burden of litigating in that state as well."

Defendants argued that SDE lacks the requisite "minimum contacts" with California because: 1) SDE does not have any offices, employees or agents, bank accounts, or real property in California; 2) SDE does not conduct any business in California, is not licensed to do business in California, and does not directly advertize or solicit business in California; 3) SDE's only purpose was to import and distribute Plaintiff's products in Europe; 4) both the Distribution Agreement and Product Development Agreement were negotiated and entered into in Ireland; and 5) any products that SDE received from Plaintiff were shipped from Plaintiff's plant in Utah, not from California.

Created with the primary purpose of developing a distributorship relationship with VF, SDE - through its owner and director Mr. Cotter - allegedly solicited VF's founder in 2003 at his home in Sacramento, California. This initial meeting allegedly led to the development of a relationship between the two companies that culminated four years later in the signing of two business agreements in 2007. These agreements entered SDE into a long-term contractual obligation with an entity principally operating out of Sacramento, as specifically noted in the agreements. The court noted that both agreements provide that any dispute arising between the parties would be governed by California law and the parties would attempt to mediate such a dispute in California. The court found that while the choice-of-law clause is not sufficient by itself to determine that Defendants availed themselves of the benefits and protections of the laws of the forum state, it is a relevant factor.

The court found that SDE - in addition to Mr. Cotter, the corporate officer who served as the "'guiding spirit' behind the wrongful act" - both satisfy the standard of purposeful availment within the first prong. In *Davis*, 885 F.2d at 520-21, the Ninth Circuit allowed that "courts can exercise jurisdiction over an individual acting in an official capacity&where 'the corporation is the agent or alter ego of the individual defendant."' According to the Court, Mr. Cotter's many trips to California and communications with VF executives in which he refers to SDE in the first person made his role as an alter ego of the company hard to deny. In contrast, Ms. Cotter's lack of consistent communication with VF employees in either the negotiation process or the subsequent business relationship, as well as her never having visited California, led Judge England to rule that VF has failed to establish purposeful availment in her case.

The second prong of the Ninth Circuit's test holds that the claim must be one which arises out of or relates to the defendant's forum-related activities.

The standard laid out in this prong of the test requires that the conduct and contacts used to prove purposeful availment in the first prong gave rise to the current dispute. To evaluate this prong judges use the "'but for' test," where "'but for' the contacts between the defendant and the forum state, the cause of action would not have arisen." *Terracom*, 49 F.3d at 561.

Applied to SDE, the court found that but for SDE's solicitation of the contractual relationship with a California-based Plaintiff and entering into two long-term agreements with Plaintiff, Defendants would not have obtained Plaintiff's confidential information, and thus Plaintiff's causes of action for breach of contract would not have arisen.

Given Mr. Cotter's status within the court's eyes as the "alter ego" of SDE, Judge England extended his rationale for SDE meeting the standard for the second prong to Mr. Cotter. However, since Ms. Cotter's lack of purposeful availment in the matter precluded the possibility of her being brought into court under specific jurisdiction, the Court did not analyze her under the second prong.

In the first two prongs, the burden rests on the Plaintiff to prove that the Defendant meets all necessary requirements for specific jurisdiction. Once standing under the first two prongs has been established, the burden shifts to the Defendant to argue the third and final prong of the test, the exercise of jurisdiction must comport with fair play and substantial justice, i.e. it must be reasonable.

For a defendant to defeat jurisdictional claims under this test, they must prove that litigating in the current forum would be too difficult as to put them at a significant disadvantage. In deciding this prong, courts use the seven "reasonableness" factors laid out in *Bancroft*, 223 F.3d at 1088. They are: purposeful interjection; burden on Defendant; sovereignty concerns; the forum state's interest in adjudicating the matter; the efficiency of resolution in the forum; the importance of Plaintiff receiving a convenient and effective resolution; and the availability of an alternative forum. Given the high level of interaction with residents of the forum, the nature of the contractual language linking SDE and Mr. Cotter to California, including a California choice of law provision, California's strong interest in protecting its residents, the parties' inclusion of an arbitration provision providing for arbitration in Illinois for disputes, and the benefits of technology and modern travel which have lowered the costs and burden of litigating in the current forum, the Court found that the majority of the "reasonableness" factors weighed in favor of the Plaintiff. Evaluating SDE and Mr. Cotter simultaneously, the court found that neither had presented compelling evidence why the specific personal jurisdiction in the current forum would be unreasonable.

After evaluating each defendant against the Ninth Circuit's three prong test, the Court denied the motion to dismiss in the case of both SDE and Mr. Cotter, and granted the motion to dismiss with leave to amend in the case of Ms. Cotter.

Because both of Plaintiff's claims, including the claim for misappropriation of trade secrets, arise out of the parties' contractual relationship, the court reasoned that it was not necessary for the court to

conduct the "purposeful direction" analysis which is typically analyzed in tort suits. However, the court found that were it to consider the "purposeful direction" prong, it would conclude that Plaintiff has sufficiently demonstrated that SDE purposefully directed its alleged tortious actions at California under the "effects" test. The court reasoned that the Plaintiff has alleged that SDE engaged in intentional tortious acts of trade secret misappropriation, thus satisfying the first prong of the "effects" test. The court further found that the second prong is also satisfied because SDE allegedly "engaged in wrongful conduct targeted at a plaintiff whom [SDE] knows to be a resident of the forum state." Finally, if SDE misappropriated Plaintiff's trade secrets, it should have known that Plaintiff would likely suffer harm in California, which is where Plaintiff's principal place of business is located.

In the end, the court refused to grant the motion to dismiss because the court was convinced that SDE initiated a long-term business arrangement with a company it knew to be principally located in Sacramento, CA. In addition, according to the court, Mr. Cotter's intertwined existence with SDE as its founder, owner, director and alter ego made him equally suspectible to personal jurisdiction in California federal court. Ms. Cotter's lack of identifiable involvement in the business relationship between VF and SDE led the Court to rule that Plaintiff "failed to allege sufficient personal conduct directed at California that would justify hailing [her] into this Court." A subsequent filing in the case reveals that SDE's and Mr. Cotter's attorneys are now seeking to withdraw from the case based in part on the Defendants' continued contention that the court does not have proper jurisdiction over them.

This decision highlights the importance of including enforceable choice of law, forum selection, and consent to jurisdiction provisions in your company's business agreements involving international transactions and parties, as well as suing in your home forum first should there later be a dispute to attempt to secure jurisdiction. Critical contract components such as these are essential because the chosen substantive law governing the dispute is typically more favorable in the selected forum for the resident party and there may be increased costs of suit and lack of familiarity and/or level of comfort in the selected forum by the foreign party that may prove dispositive.

Federal Judge In California Holds That Unauthorized Use Of Copyrighted Password-Protected Computer Diagnostic Software Can Be The Basis Of A Copyright Infringement Suit and Trade Secret Misappropriation Claim

By Paul E. Freehling (May 31, 2012)

Burroughs Payment Services manufactures document scanning equipment for banks and others. Embedded in the equipment are copyrighted computer programs, accessible only by entering a password, which provide the user with software to diagnose problems with the equipment. While servicing the equipment of a Burroughs customer, Symco Group allegedly accessed and used Burroughs' software without that company's authorization.

Burroughs promptly sued Symco in the federal court in Atlanta, alleging copyright infringement and trade secret misappropriation. More than 18 months later, following various rulings by the Atlanta court, Burroughs dismissed its complaint there without prejudice and re-filed early this year in the Northern District of California. A few weeks ago, Magistrate Judge Spero in the California court denied most of Symco's Rule 12(b)(6) motion to dismiss. *Burroughs Payment Sys., Inc. v. Symco Group, Inc.*, 2012 WL 1670163 (N.D. Calif., May 14, 2012).

Copyright infringement

Symco asserted that its affirmative defense based on 17 U.S.C. § 117(a)(1) (the owner of a copy of a computer program may make or authorize the making of another copy if doing so is "an essential step in the utilization of the computer program in conjunction with a machine," provided that the copy "is used in no other manner") is not rebutted in Burroughs' complaint and is dispositive because Symco's conduct constituted a category of copying that is "lawful per se." Clearly, Burroughs' customers purchased or leased equipment, but Burroughs alleged that they were neither owners nor licensees of the software at issue here and, therefore, they could not lawfully authorize Symco to make or use a copy of the software. The court held that the question of whether Symco's §117(a)(1) defense defeats Burroughs' copyright infringement claim required development of a factual record.

Symco also raised an affirmative defense based on 17 U.S.C. § 117(c) (under specified circumstances, the owner or lessee of a machine that contains an authorized copy of a computer program may make a copy for the purpose of maintenance or repair of the machine). The court said that without a factual

record it could not determine whether Symco's conduct was permitted by §117(c). For these reasons, Symco's motion to dismiss Burroughs' copyright infringement claim was denied.

Trade secret misappropriation

Symco insisted that, in the case of computer software, under the applicable statute (the California Uniform Trade Secret Act) only the source code can be a trade secret, that Burroughs did not aver that Symco misappropriated the source code, and that the images appearing on a screen when Burroughs' software programs are run do not constitute trade secrets. Symco argued that *Silvaco Data Systems v. Intel Corp.,* 184 Cal.App.4th 210(2010) compelled dismissal of the claim. The court disagreed and stated that Silvaco does not support a contrary result. In that case, the court held on summary judgment that where the alleged trade secret was the source code, merely executing and running the programs did not constitute misappropriation because there was no "use" within the meaning of the CUTSA.

The court further reasoned that:

> The reasoning in *Silvaco* does not apply here, however, because the alleged trade secrets are the materials and screen images that are allegedly accessed by Symco without authorization rather than the source code. Thus, in contrast to simply executing source code, which the court in Silvaco likened to eating a pie made with a secret recipe, Symco is alleged to have used secret information it improperly obtained to service the equipment of Burroughs customers, which might be analogized to actually reading the secret recipe in order to bake the pie. Therefore, the Court concludes that Silvaco does not support dismissal of Burroughs' trade secret misappropriation claim at this stage of the case.

Burroughs also responded that the images relevant here are not publicly available because of the required and protected password. Thus, Symco could not access the images by proper means, and they are the subject of reasonable efforts by Burroughs to maintain secrecy. The court concluded that "the alleged trade secrets are the materials and screen images that are allegedly accessed by Symco without authorization." Therefore, sufficient facts were alleged to preclude dismissal of the complaint.

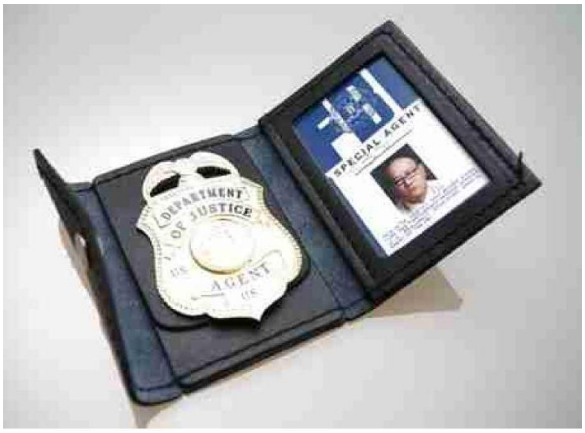
DMCA

The only part of Symco's Rule 12(b)(6) motion that was granted pertained to a count in Burroughs complaint based on the Digital Millennium Copyright Act, 17 U.S.C. § 512 (a service provider is not liable for infringement of material transmitted by an automatic technical process, at the request of another person, without selection or copying of the material by the service provider). A similar count had been included in Burroughs' complaint in Atlanta, but the court there dismissed that count with prejudice. Symco argued "res judicata." Burroughs countered that there never was a final adjudication on the merits in Atlanta. The court concluded that both issue and claim preclusion barred Burroughs from proceeding with its DMCA claim except for misconduct, if any, occurring after that claim was dismissed in Atlanta.

This case teaches that the unauthorized use of copyrighted and password-protected computer applications can constitute copyright infringement and trade secret misappropriation. However, the particular facts and circumstances here will determine whether Symco's affirmative defenses ultimately defeat Burroughs' copyright infringement claims, and whether Symco benefitted from accessing Burroughs' alleged trade secrets without authorization.

You Think Trade Secrets Are Important? So Does the FBI

By James D. McNairy (June 1, 2012)



The FBI recently launched an initiative to curb the growing rise of trade secret and other intellectual property theft. The FBI estimates that U.S. companies have suffered over $13 billion in economic losses since October 2011 attributed to intellectual property theft, which includes the estimated future market value of stolen trade secrets.

With a website dedicated to educating the public about intellectual property theft, in May 2012, the FBI took the unconventional approach of launching billboards in nine U.S. cities with the message "Protect America's Trade Secrets." As reported by the Wall Street Journal, the push behind the FBI's initiative is that state-sponsored espionage targeting trade secrets and other intellectual property of U.S. companies is growing so fast that it is a national security concern.

Thieves have shifted their focus from defense contractors—which have grown increasingly sophisticated in implementing security measures to prevent trade secret theft—to companies with less sophisticated security measures. To combat this trend, the FBI recently issued a press release with tips outlining warning signs that may indicate an employee is stealing company secrets. As highlighted by the FBI, increasingly thieves use electronic means such as thumb drives and other USB storage devices to pilfer company secrets. John Marsh's blog Trade Secret Litigator also has a nice summary of the FBI's tips.

Although the federal government often uses the Economic Espionage Act, to pursue state-sponsored trade secret theft, companies have a variety of civil tools available to pursue employee theft of company confidential, proprietary, and trade secret information. For example, forty-seven states have adopted versions of the Uniform Trade Secrets Act. And those states that have not adopted UTSA—Massachusetts, New York, and Texas—have a body of common law which recognizes and protects trade secrets.

With advances in technology that sometimes outpace the time required to secure patent protection or which a company does not want to publicly disclose in an issued patent, trade secrets are on the rise. Given this, it is imperative that companies proactively protect their trade secrets—not only for national security, but also for the bottom line.

New Hampshire Federal District Court Broadly Interprets Preemption Provision In State's Uniform Trade Secrets Act

By Ryan Malloy (June 7, 2012)

In a recent decision, *Wilcox Indus. Corp. v. Hansen*, 2012 U.S. Dist. LEXIS 63668 (D.N.H. May 7, 2012), a federal judge for the District of New Hampshire interpreted the New Hampshire Uniform Trade Secrets Act's (the "NHUTSA") preemption provision to preempt all non-contract claims based on unauthorized use of information even if the information at issue is not a trade secret.

In *Wilcox Indus. Corp. v. Hansen*, plaintiff Wilcox, a manufacturer of military equipment, filed a complaint against former consultant Mark Hansen and his new employer, Advanced Life Support Technologies, Inc. ("ALST"), alleging misappropriation of trade secrets, unfair competition, and other state law claims after Hansen incorporated Wilcox's confidential and trade secret information into ALST's competing life support device. Wilcox also alleged that defendants solicited its existing and prospective customers to purchase ALST's competing product by using confidential information that Wilcox had entrusted to them, all in violation of a non-disclosure and nonsolicitation agreement and a royalty agreement. Defendants moved to dismiss all claims. The Court granted in part and denied in part the motion to dismiss, and found that plaintiff's claims for unjust enrichment and breach of fiduciary duty were preempted by the NHUTSA.

By its plain language, the NHUTSA "displaces conflicting tort, restitutionary, and other law of this state providing civil remedies for misappropriation of a trade secret." The only exceptions are claims for contractual remedies, criminal remedies, and other remedies not based on misappropriation.

The District Court adopted the Supreme Court of New Hampshire's holding in *Mortgage Specialists, Inc. v. Davey*, 153 N.H. 764, 776 (2006), finding that a claim survives preemption only to the extent that it alleges wrongful conduct independent of any alleged unauthorized use of information, provided that the independent allegations are sufficient to plead all elements of the claim. In *Mortgage Specialists, Inc. v. Davey,* the Supreme Court of New Hampshire reasoned that the preemption provision was designed "to preserve a single tort action under state law for misappropriation of a trade secret as defined in the statute and thus to eliminate other tort causes of action founded on allegations of misappropriation of information that may not meet the statutory standard for a trade secret."

In essence, the District Court determined that the NHUTSA broadly classifies information either as a protected trade secret, as defined in the statute, or as unprotectabe information. The full text of the opinion can be found here. Ken Vanko's Non-Compete Blog also has a nice overview of the decision and its implications.

Virginia Supreme Court Muddies Damages Valuation of Lost Goodwill In Trade Secret Matter

By Rebecca Woods (June 18, 2012)

The Virginia Supreme Court has complicated the valuation of lost goodwill damages in trade secrets matters in its June 7, 2012 decision in *21st Century Systems, Inc. v. Perot Systems Government Services, Inc.,* No. 110114.

The matter arose from the departure of several employees from Perot Systems Government Services, Inc. ("Perot"), who subsequently joined a competitor company. Perot filed suit with multiple counts, including breach of fiduciary duty, breach of non-disclosure agreement, breach of non-competition and non-solicitation agreements, violation of Virginia's business conspiracy act, and violation of Virginia's Uniform Trade Secret Act. During trial, Perot provided evidence that several of the key employees had downloaded numerous Perot documents and accessed those files while working at the competitor. Defendants challenged the propriety of Perot's damages expert, but the trial court denied the motion to strike, instead striking defendants' counter expert for failure to adequately disclose his opinions prior to trial. The jury returned a verdict in favor of Perot on all claims, including $4 million in compensatory damages and $12 million in trebled damages, most of which was predicated upon lost goodwill damages.

The key issue on appeal was the propriety of Perot's damages expert's valuation of Perot's lost goodwill damages. Perot's expert had sought to follow the methodology used and accepted by the Virginia Supreme Court in *Advanced Marine Enters. V. PRC Inc.,* 256 Va. 106, 501 S.E.2d 148 (1998). Specifically, the expert sought to calculate the difference between the price the business would sell for and the value of its non-goodwill assets. He did so by using the actual sale figures and Dell's valuation of Perot's goodwill, as reported in SEC filings. The majority on the Supreme Court took issue with this approach, noting that because the expert had used actual sale figures, "Perot was required to demonstrate that its sale price to Dell reflected an actual loss of goodwill as a result of the [misconduct]." The employees had departed in the summer of 2009, and the sale to Dell was completed in November 2009, but Perot introduced at trial no evidence regarding the diminution in value of Perot's fair market value or identifiable assets during this time frame. To the contrary, the majority noted that Dell had paid a premium for Perot, and there was no evidence at trial that Dell discounted Perot as a result of the employee departures. As a result, the Court concluded that Perot had not, as a matter of law, demonstrated that it actually lost any goodwill.

The majority distinguished *Advanced Marine*, in which the plaintiff company lost employees to a competitor and was sold before the trial court decided the case. The record indicated that the price for

the sale of the company did not change after the departure of the relevant employees. The expert in *Advanced Marine* did not look to the actual sales data, however, to determine the lost goodwill damages. Instead, the expert examined the sales of two comparable businesses, subtracted the value of each "comparable company's" assets from its sales price to determine the goodwill associated with each comparable sale, and then apportioned this estimated goodwill figure among the number of employees. This derived figure was then applied to the departed employees of Advanced Marine. The Virginia Supreme Court approved of this methodology, noting that the departed group of employees had "goodwill value for purposes of maintaining the customer relationships necessary for contract retention." No similar testimony was provided in the instant case, noted the majority.

Two justices dissented from the majority opinion. The dissents argued that the majority was applying a higher standard of proof to Perot than the Court had applied in *Advanced Marine*. The dissent noted that lost goodwill valuations are inherently difficult, but the methodology used by Perot's expert was sensible and consistent with *Advanced Marine.*

It is difficult to make sense of the methodology accepted by the Virginia Supreme Court in *Advanced Marine* but rejected in *21st Century*. In the former, the sales price did not reflect a lost valuation, but the Court accepted the analytically derived damages figures on the presumption, supported by testimony, that there would be future lost goodwill. In *21st Century*, the actual sales data also did not reflect lost value, but the Court required that it do so to sustain a lost goodwill valuation. Parties claiming lost goodwill damages should thus be cautious in relying upon actual data, rather than analytically derived data, unless the actual data demonstrate the lost goodwill. Further, *21st Century* cautions that there needs to be testimony regarding the existence of the lost goodwill, e.g., that departed employees will harm the relationships necessary to retain customers.

California Federal District Court Issues Decision On Reasonable Secrecy Measures, Trade Secret Identification, and Preemption

By James D. McNairy (June 19, 2012)

A recent California federal district court decision in *FormFactor, Inc. v. Micro-Probe, Inc.,* Case No. C 10-3095 PJH highlights the importance of companies proactively taking measures to protect their trade secrets before litigation arises and specifically identifying trade secrets that have allegedly been misappropriated.

FormFactor, a company which designs, manufactures, sells and supports high-performance advanced wafer probe card assemblies, alleged that a competitor, Micro-Probe, Inc., had been hiring FormFactor personnel for the express purpose of having them disclose FormFactor confidential technical and marketing information. FormFactor filed suit alleging, patent infringement, trade secret misappropriation, breach confidence, unfair competition, and civil conspiracy. FormFactor also sued the former VP of its DRAM Business, Mr. Browne, who joined Micro-Probe and was alleged to have misappropriated FormFactor trade secrets.

The parties filed cross-motions for summary judgment on the non-patent claims. In granting Micro-Probe's motion, the court highlighted several trade secret litigation fundamentals that, in its view, were not satisfied by FormFactor. The court then held that FormFactor's non-trade secret claims (other than patent infringement) were preempted by CUTSA.

Specifically, the court held that:

1. FormFactor had not described its trade secrets with sufficient particularity or shown that the information claimed to be trade secret in fact qualified as trade secrets.

    (a) The court cited common law and California Code of Civil Procedure § 2019.210 for the requirement that trade secret plaintiffs identify trade secrets with "sufficient particularity", which FormFactor had not done through submission of lists of files allegedly misappropriated by defendants. That FormFactor's list contained many entries only identifying file names that even FormFactor's 30(b)(6) designee could not identify as trade secret were cited by the court as evidence that FormFactor had not met its burden ("Here, neither the List nor the testimony of FormFactor's witnesses provides the requisite showing to clearly identify what each individual thing is that it alleged to be trade secret"); and

(b) In holding that FormFactor had not shown that the information at issue qualified as trade secrets, the court highlighted the following facts:

(1) there was no evidence that FormFactor made reasonable efforts to protect the secrecy of any particular trade secret because:

i. There was no written agreement with Browne to protect FormFactor's trade secrets;

ii. FormFactor allowed Browne to retain his contact information when he left FormFactor;

iii. FormFactor allowed/authorized Browne and other employees to work from home (including using personal email to conduct FormFactor business, and to back up FormFactor data onto external hard drives);

iv. FormFactor did not request that Browne return any FormFactor data when he tendered his resignation and left the company; and

v. After being ordered by the Magistrate Judge to "conduct an internal investigation to determine which of its listed trade secrets had never been disclosed publicly," FormFactor was not able to provide a specific information as to how the information was maintained in confidence.

2. FormFactor had not provided evidence of misappropriation. Specifically, FormFactor's reliance on Browne's copying files onto his home computer and admitting that he "used" information at Micro-Probe that he learned at FormFactor failed to show misappropriation because:

(a) There was no policy at FormFactor for or against employees working from home, or for or against the backing up and downloading of FormFactor files;

(b) There was no evidence that Browne and FormFactor ever entered into a written employment agreement, a non-disclosure agreement, a non-compete agreement, or a non-solicitation agreement. Although Browne signed an agreement while at FormFactor, providing in part that after his employment had terminated, he would not "claim[], construe[], or pre-sent[] as property" any "work product created on the job using FormFactor information or property", the court held that the agreement did not provide that Browne would not retain any Form-Factor documents after terminating his employment—just that he would not claim ownership of such documents;

(c) When Browne resigned and was asked to leave the same day, no one inquired regarding any back-up files he might have on his home computer; and

(d) FormFactor provided no evidence of improper/unauthorized copying by Browne or use by defendants of any specific trade secret included on FormFactor's trade secret designation list. Although the court relied on several facts to reach this conclusion, among them were its rejection as unreliable of FormFactor's expert's opinion that from a from "a neurological and physiological standpoint, Mr. Browne cannot do anything but use [Form Factor's] information given the similarity of his job at [Micro–Probe] with his job at [FormFactor] and the length of time." The court also held that, in proffering this opinion, FormFactor was trying to invoke the so-called inevitable disclosure doctrine, which is not recognized in California.

Having found that FormFactor's trade secret claim had not raised a triable issue of material fact, the court then found that the trade secret claim preempted FormFactor's breach of confidence and unfair competition claims because they were "based on the same nucleus of operative facts as the trade secret misappropriation claim." Although the court recognized that there is "some dispute" among the courts as to whether CUTSA preempts claims for misappropriation of confidential information not rising to the level of a trade secret, the court rejected application of that law here because "Form Factor's position has consistently been that there is no distinction between the alleged trade secret information and the alleged confidential information" at issue.

The *FormFactor* decision highlights the importance of identifying, maintaining the confidentiality of, and taking proactive steps to ensure that outgoing employees have been appropriately screened to determine whether they have retained company confidential, proprietary, and trade secret information. Failure to do so while asserting a claim for misappropriation of trade secrets can not only cause the trade secret claim to fail, but cause potentially otherwise viable non-trade secret claims to be preempted by CUTSA.

Five Practical Guidelines on PROTECTING YOUR GREAT BUSINESS IDEA

As a special feature of our blog –special guest postings by experts, clients, and other professionals – please enjoy this blog entry about protecting business ideas by technology lawyer and IP strategist Joren De Wachter. Joren serves as a Vice Chair with me on the ITechLaw Intellectual Property Law Committee and has an excellent blog of his own on current technology issues. Enjoy Joren's article.

- Robert Milligan, Editor of Trading Secrets

By Joren De Wachter (June 20, 2012)

Congratulations! You have come up with this great business idea, and you are developing a way to bring it to the market.

But you need things. You need business partners, distribution partners, customers, maybe even investors.

So how do you protect your business idea? How do you make sure other won't steal it? Here's some essential guidelines on protecting your great business idea.

1. What is an idea?

An idea is just that. It's an idea, not a business.

Great ideas are never stolen, because they are not secret. They have always been around for some time. Google did not invent the idea of Internet search. Facebook did not come up with the idea of social media. Skype did not come up with the idea of video-phone over the Internet. Apple did not invent the iPad, it only significantly improved the execution.

And that distinction, the distinction between an idea and its execution, is crucial.

When we talk about "protecting", we typically think of Intellectual Property Rights ("IPRs"). And IPRs (patents, copyright, designs, etc) never protect ideas. They protect expressions of those ideas. They protect the way the idea is executed upon, and the way the idea is made into a concrete product or service in the market.

So don't worry too much about your ideas. When, after a lot of hard work, those ideas are slowly turning into a product or service, that's when you should start thinking about protection. But typically not at the level of ideas. And besides, when you have a brilliant insight, it's much more likely that someone else of the 7 billion on this planet had it before you. But that's OK, because the value is in the execution, not in the idea itself.

2. What is great?

What is a great idea? It's an idea you can execute upon, an idea that addresses a pain or need in the market, an idea that other people will recognize as great. What that means, is that, by and large, the only way you will find out if you have a great idea, is to talk about it.

To check it out, discuss about it, with potential partners, potential clients, potential investors. Until and unless you discuss your idea, you won't know if there's an actual market for it.

Except if you don't really care whether you have customers and can build a business, it is not a good idea to hide your idea away, and build a product and service on that secret idea, without first checking if there is a demand.

And the only way to check if there is an actual or potential demand, is to share your idea with others.

What's more, others know things you don't. If you share your idea, they will come up with additions, new viewpoints, interesting suggestions, all things you wouldn't have thought if you had kept your idea secret. It will strengthen not only your idea, but, much more importantly, your business model and the execution you will give to your idea.

And don't be afraid, they can't steal your idea. You don't "own" it anyway, you're just using it to build a product or service that you want to bring to the market.

And when a product or service is based on a great idea, the chances of your success are greater.

3. What is protection?

When we talk protection, we talk IPRs.

As I said before, IPRs only apply to the expression of ideas, not to the idea itself.

It is the effort you put into converting your great idea into a product or service that you can offer in the marketplace that you can potentially protect by IPRs.

But what does protection mean? First, and this is essential, IPRs do *not* give you the right to exploit your innovation. IPRs only give you the right to prevent others from producing or distributing a copy of your innovation. That difference may sound trivial, but it is not.

It means that protection is a negative right, not a positive one. When you obtain IPR protection (which may be essential for your business model), you obtain the right to block other people from doing certain things. Typically those things relate to copying or distributing the concrete expression of your idea.

But it will not necessarily guarantee that you can actually use yourself your idea (your IPR does not, per se, invalidate someone else's IPR), and it does not guarantee that others won't develop their own expression of your idea.

So, while protection is great, its importance can easily be overstated. Protection is a tool, not a purpose.

One of the important questions you will need to address is whether protection is actually appropriate for your business model, what it is you want to protect, and how you want to use that protection. And remember, in this field, as in any, return on effort is the most important parameter.

A final point on protection: since IPRs are negative rights, their use is actually fairly limited. There are three main ways to use IPRs: offensive, defensive, and to impress investors.

Offensive use of IPRs is what Apple is currently doing: It is suing a lot of competitors to block their access to the market, or get them to pay a license fee to protected technology or designs. Such use of IPRs is actually very expensive. Rumours mention amounts of several dozens of millions of Euros spent on these programs of litigation and enforcement.

While there may be a positive return on investment, it is unlikely to be a good business strategy for a startup. As a rule of thumb, this kind of strategy is not uncommon for larger, established businesses.

Defensive use of IPRs is using your IPRs to counter an attack from a competitor, who uses an offensive strategy (see above). Some kind of mutual partial destruction strategy. The typical result, after a lot of legal fighting, is often a cross- license. Here, the IPRs are used as a retaliation capability in case someone attacks you. But note, again, how the IPR itself will not give you the right to exploit the innovation you want to bring to the market.

Not much needs to be said about the third use of IPRs – it speaks for itself.

4. When is an idea yours?

The regime of IPRs is technical and complex. There is no simple approach to them – that's an unfortunate fact. The main reason for this is that IPRs are highly contextual.

But at the same time, IPRs are an essential structure of how you build a business model around the innovation you want to bring to the market.

IPRs will determine what rights you will grant to your customers; they will determine which rights you obtain upstream from your suppliers; they will influence whether you choose for an open (e.g. open source) or more closed model, or a hybrid in-between.

IPRs will determine your freedom to operate, but also indicate how to best use that freedom, so that you can find the right way to structure your business.

And that question of IPRs needs to be solved before you make your final decisions on how to structure your business and bring your product or service to the market.

In other words, before you start selling, you need to know what is yours, and what is not – and to what extent.

5. So, where's the business?

In the end, that is the key question. Ideas are not bought and sold. It is products and services that are bought and sold in the marketplace. Protecting a business, and the IPRs in that business in a way that supports the business model, are an excellent idea. But those IPRs don't make the business itself.

First build the business case, the business model, and the revenue model. Integrate in those models the information about what can be protected, how it should be protected, and how that will support and construct your business model.

Then build your business. And the value of that business will be in the way you execute your idea, rather than in the idea itself.

Good luck with your business.

Joren De Wachter is an experienced IP strategist, with a focus on ICT technology businesses. He can be reached at info@jorendewachter.com.

Massachusetts Federal Court Rejects Expansive View of Inevitable Disclosure Doctrine and Denies Preliminary Injunction

By Ryan Malloy (June 22, 2012)

On June 19, 2012, a Massachusetts federal court declined to apply an expansive interpretation of the inevitable disclosure doctrine during a preliminary injunction ruling, finding that the rule is best applied to establish irreparable injury supporting enforcement of a non-competition agreement and not as the basis for a future misappropriation of trade secrets claim.

In *U.S. Elec. Svcs., Inc. v. Schmidt*, 2012 U.S. Dist. LEXIS 84272 (D. Mass. June 19, 2012), plaintiff USESI, a national distributor of electrical products and services, sued two former employees and their current employer, Munro, for breach of contract, misappropriation of trade secrets, and unfair competition, among other allegations. Munro is a regional distributor of electrical products whose national accounts division competes directly with USESI. USESI claims that Munro and its former employees intended to compete with USESI for a specific account, which was scheduled to go out for bid for the first time in four years. One week prior to the bid, USESI filed its complaint and a motion for a preliminary injunction.

The court denied USESI's motion for a preliminary injunction after a hearing on May 14, 2012 for two reasons. First, the court found that none of the authorities cited by USESI stand for the proposition that allegedly *inevitable future misuse of trade secrets* is by itself sufficient to establish a violation of either common law or statutory obligations regarding trade secrets. In each case cited by USESI, the plaintiff had established the likelihood of success on the merits of a breach of contract claim based on a non-competition agreement, not (as here) a pure trade secrets claim, and in each case the plaintiff alleged that the defendant's breach had already occurred by the time of the preliminary injunction proceedings, not (as here) merely that defendant's actionable conduct was imminent and inevitable.

Second, even if the inevitable disclosure doctrine could provide a basis for demonstrating a likelihood of success on the merits, the court found that USESI failed to show that future disclosure would be inevitable, thereby precluding preliminary injunctive relief. Specifically, the court found that the defendant former employees' knowledge and level of responsibility with regard to the subject account was limited, particularly given that one of the defendants, a former manager, had not dealt with the customer for over two years.

The full text of the Court's statement of reasons for denying USESI's motion for a preliminary injunction can be found here. Also, please see Ken Vanko's blog on this interesting case.

California Federal District Court Finds That Plaintiffs May Assert A Claim For Alleged Misleading Actions of Agent and Misuse of Confidential Information Not Rising To Level Of A Trade Secret In Youth Hostel Dispute

By Robert Milligan (June 26, 2012)

In business, as in life, trust and communication are key to healthy and productive relationships. When these crucial elements are lost, as in the case of *What 4 LLC v. Roman & Williams, Inc*., 2012 WL 1815629 (N.D.Cal.), the fallout is often contentious and requires court intervention.

In a recent decision granting in part and denying in part defendants' motion to dismiss, Judge Edward M. Chen of the United States District Court for the Northern District of California examined the principal-agent relationship between the parties to determine what responsibilities each had to the other based on the relationship's underlying agreements and under California law.

On defendants' motion to dismiss, the court found that plaintiffs had stated a claim for alleged breach of fiduciary duty and concealment predicated on defendants' alleged misleading statements/conduct as to their intentions to perform under the parties' alleged agreement. The court further held that plaintiffs were permitted to assert an alleged claim for breach of fiduciary duty and concealment predicated on the disclosure of confidential information not rising to the level of a trade secret, notwithstanding California Uniform Trade Secrets Act ("CUTSA") preemption.

The plaintiffs, What 4 LLC and 1095 Market Street Holding LLC, planned and secured financing for a joint venture to open a "premium youth hostel" at 1095 Market Street, San Francisco, CA, including purchasing the property and conducting market research and analysis. After completing their designs, applying and receiving all requisite entitlements and permits, plaintiffs allegedly approached the defendants, Roman & Williams ("R & W") as well as its sole shareholders, Robin Standefer and Stephen Alesch, in November 2010 about hiring them for architectural and design services. On November 4, 2010, R & W signed a nondisclosure agreement prohibiting it from disclosing any of the confidential information given to it by plaintiffs, including market research and design. 1095 Market Street Holding eventually hired R & W on January 31, 2011 to work on the youth hostel, entering into a Letter Agreement. The Letter Agreement stipulated that R & W was to complete the project in six different phases ranging from concept to construction, and that other details would be finalized at a later date in a Definitive Agreement meant to supersede the Letter Agreement. In the interest of time, the parties agreed to proceed with the first two stages without signing a Definitive Agreement, which defendants completed in August 2011.

While R & W waited for orders to begin work on the next phase of the project, in October 2011 it allegedly began negotiations with plaintiffs' competitor, Sydell, to provide services for their own premium youth hostel project. In a subsequent meeting with Sydell on November 1, 2011, Ms. Standefer allegedly disclosed plaintiffs' confidential information in a bid to win the contract. On November 15, 2011, R & W allegedly met with plaintiffs to discuss the next steps of the 1095 Market Street project, failing to inform them that it had entered into a multi-year exclusive contract with Sydell to provide the same services it had, and was to provide plaintiffs. Allegedly learning about R & W's agreement with Sydell from a *Wall Street Journal* article on November 23, 2011, plaintiffs asserted the following causes of action: (1) breach of the nondisclosure agreement, (2) breach of fiduciary duty, (3) concealment, (4) breach of contract, and (5) violation of CUTSA. Defendants then brought a motion to dismiss plaintiffs' claims except the CUTSA claim.

Lumping the first and fourth causes of action together, the court began its analysis by examining defendants' contention that the two breach of contract claims (i.e., the Nondisclosure Agreement and the Letter Agreement) should be dismissed. Due to the fact that the two individual defendants, Ms. Standefer and Mr. Alesch, were not a party to either contract, a point which plaintiffs conceded, the Court granted the motions to dismiss the claims for these two. However, the court noted that "there are still viable claims for breach of contract against R & W."

Next in its analysis, the court determined whether or not R & W's actions constituted a breach of fiduciary duty and concealment. For its part, defendants argued that the claims are preempted by the CUTSA and that the claims are not plausible given the insufficient allegations that they owed a duty to plaintiffs. Codified in *California Civil Code § 3426*, the CUTSA includes a provision which states that the statute "does not affect... (2) other civil remedies that are not based upon misappropriation," which courts have interpreted to "preempt alternative civil remedies based on trade secret misappropriation." Plaintiffs stated in their complaint that all of the confidential information disclosed by R & W constituted trade secrets under the CUTSA. Although they argued in court that some of the disclosed information did not constitute trade secrets, Judge Chen agreed with defendants that CUTSA preempts the breach of fiduciary duty and concealment claims based on plaintiffs' original filing stating otherwise. The court, however, provided plaintiffs with leave to amend the claims to include, as an alternative theory, allegations that plaintiffs' confidential information did not constitute trade secrets but was otherwise actionable.

In response to R & W's assertion that they did not owe a duty to What 4 LLC or 1095 Market Street Holding LLC, plaintiffs argued that defendants did "because (1) they were Plaintiff's architects and (2) they were Plaintiff's agents." Citing *Palmer v. Brown*, where the court found that an architect's fiduciary duty to one client does not prohibit the architect from working with a client's potential competitor, the court did not find plaintiffs' first argument convincing. However, because plaintiffs hired R & W "to act as their agent" to bid and negotiate with suppliers on their behalf, the court found the existence of an agency relationship to be plausible. Citing the Restatement of the Law of Agency (3rd ed., 2006), the court noted that while an agent is not required to disclose its intentions to compete with a principal, it does have a duty not to mislead the principal about its own intentions. R & W allegedly continued to meet with plaintiffs and led them to believe it was committed to proceeding with the next phase of

development while previously entering into a multi-year exclusive contract with Sydell that prevented any such work. Therefore, although it found that there is no viable claim for breach of fiduciary duty based on defendants working for a competitor or concealing that fact, the court denied defendants' motion to dismiss these claims based on the allegations that defendants allegedly misled the plaintiffs.

This decision is noteworthy because the court rejected plaintiffs' claim that defendants' alleged breach of the exclusivity provision in their agreement constituted a breach of fiduciary duty and for the court's willingness to leave the door open to plaintiffs to assert a claim for breach of fiduciary duty and concealment based upon the misuse of information not rising to the level of a trade secret, notwithstanding CUTSA preemption.

Additionally, the case highlights that selecting reliable and trustworthy agents to assist with the implementation of a vision is paramount to the success of any business venture. When a principal-agent relationship fails, the costs to all parties can be enormous. The threat of these costs, including lost productivity and the price of litigating these disputes, should motivate business planners to be exceptionally thorough in vetting potential business partners. While these considerations are essential, it is also important for any business relationship to be anchored by a comprehensive contractual agreement which explicitly details the duties and responsibilities each party has to the other. By clearly outlining the parameters of a business relationship, both the principal and agent can attempt to protect themselves from any unwanted or unexpected results. Consultation with experienced legal counsel is often necessary to position a party for the best outcome, particularly in California where non-compete agreements and claims of theft of trade secrets and confidential information are highly scrutinized.

NLRB Continues To Crack Down On Employer Social Media Policies and Continues to Leave Doubt On What Provisions Designed To Protect Trade Secrets and Confidential Information Will Withstand Its Scrutiny

By Jessica Mendelson and Robert Milligan (June 28, 2012)

Facebook, Twitter, LinkedIn, Yelp, Foursquare....in today's modern world, a large and growing number of people are using social media in some capacity. Many employers have some sort of social media policy to regulate the use of social media by their employees. Some simply block social media websites on company assets in the workplace, while others have comprehensive policies that limit the type of information an employee can reveal on these websites at work or at home.

In recent months, employer social media policies have come under fire by the National Labor Relations Board (the "NLRB"), the federal agency which enforces the National Labor Relations Act (the "NLRA"). Under the NLRA, protected employees are given the right to act in conjunction with one another to improve wages and work conditions. The NLRA protects the rights of these employees to engage in concerted activity, and to bring group complaints to the employer's attention. Protected activities include discussions between employees regarding wages and workplace conditions.

In the past year, the NLRB's Acting General Counsel ("AGC"), Lafe Solomon, has issued three reports clarifying the NLRB's stance on social media policies. During that time period, the AGC has found the substantial majority of employer social media policies overly broad and unlawful. Of the twenty policies reviewed in the past three reports, only four were found to be legal under the NLRA.

The most recent operations management memorandum ("OMM"), which was issued on May 30, 2012, highlights the importance of a well-drafted social media policy, and continues to take the position that many employer's current policies are unlawful. Of the seven company policies cited in the OMM, six were found to be overbroad, and therefore unlawful. The report stresses the importance of careful drafting to avoid any broad language which employees could reasonably construe to prohibit protected activities. Additionally, a disclaimer stating that activities protected under Section 7 of the NLRA are not prohibited is insufficient to cure a defective policy according to the ACG.

Several of the allegedly unlawful specific policies addressed by Solomon's latest report include:

- A confidentiality rule that warned employees about sharing confidential information, without specifically identifying categories of non-NLRA protected confidential information.

- A warning that employees' online posts should be "completely accurate and not misleading."
- A policy that instructed employees to communicate in a "professional tone" without making "objectionable or inflammatory comments."
- A restriction on employee contact with the media.

The NLRB's memorandum has been heavily criticized by legal experts in recent days. According to some experts, the report is contradictory, and fails to make clear what policies would actually violate the NLRA. For example, according to the AGC, a provision prohibiting employees from distributing the employer's "secret, confidential or attorney-client privilege information" is legal, however, provisions such as "you should never share confidential information" and "don't release confidential guest, team member, or company information" are not. Are you confused? An additional problem with the NLRB's "guidance" is that the legality of the policies advocated has never actually been tested by a court of law. Some critics even argue the NLRB's policies go so far as to constitute agency overreaching.

For employers, the key question arising from these guidelines is how an employer can draft a social media policy which protects confidential, proprietary, and trade secret information, while complying with the NLRA. Employers need to ensure that their policies clearly articulate the business interests of the employer in imposing the restriction, and that such policies are not ambiguous and overreaching. Specific examples of confidential, proprietary, and trade secret information should be provided, and the policy should explain why the restrictions being imposed are necessary and to protect legitimate business interests. The policy should also provide examples of prohibited disclosures. The NLRB did include a social media policy that it approved in its latest report (starting on page 22) but many employers may not find that policy works for its workforce or has the level of detail and bright lines that many would have expected. We will continue to keep you posted on this constantly evolving area.

Missouri Federal Court Denies Summary Judgment Motion Finding Disputed Issue On Whether Trade Secret Exists Notwithstanding Lack of Confidentiality Agreements and Partial Disclosure to Copyright Office

By Paul E. Freehling (July 17, 2012)

Three years after entering into an oral subscription agreement relating to a specially designed, copyrighted internet-based computer software program, the subscriber stopped paying the required monthly fees. The reason, according to a 10-count federal court complaint, is that the subscriber modified the source code by copying it onto the subscriber's own server and thereafter used the unauthorized version. This allegedly constituted, among other misconduct, breach of contract (Count VII), copyright infringement (Count VIII), and a violation of the Missouri Uniform Trade Secrets Act (Count IX). The subscriber moved for summary judgment with respect to the trade secrets misappropriation count because (a) the source code had been disclosed to two of the plaintiff's employees neither of whom had signed confidentiality agreements, and (b) it had been partially revealed to the U.S. Copyright Office. A similar motion was filed concerning the alleged breach of contract which the subscriber contended was preempted by the Copyright Act and, consequently, was encompassed within Count VIII. As explained below, both motions were denied.

A source code that is not publicly disclosed can be a trade secret. So, the principal issue concerning Count IX (trade secret misappropriation) was whether reasonable efforts had been made to maintain the code's secrecy. The court observed that only the first 50 pages of the code, out of 80,000 lines, had been revealed to the Copyright Office and that, in any event, the Copyright Office limits access to deposited materials. Also, according to the court failure to require two employees to whom the code was disclosed to execute confidentiality agreements, while relevant, is not dispositive since a party need only take reasonable steps (not all possible measures) to protect its trade secret information. Here, those employees' computers were password-protected and were not freely accessible, and the code was not disclosed to customers. Accordingly, there was a question of fact as to whether the requisite protection of the trade secret occurred.

Preemption of breach of contract

The source code indisputably was copyrighted. The court held that the breach of contract claim was not preempted unless the contract rights were "equivalent to any of the exclusive rights within the general

scope of copyright." Here, the court explained, the contentions were different because to recover for breach of contract, the plaintiffs had to prove both the existence of a valid agreement and contract damages neither of which were necessary in order to establish copyright infringement.

This case, Two Palms Software, Inc. v. Worldwide Freight Management LLC, Case No. 4:10-CV 1045 (CEJ) (E.D.Mo., June 26, 2012), teaches that the owner of a trade secret should provide access to it only to persons with a need to know and should disclose no more of it to governmental bodies than absolutely necessary. Further, the opinion discusses the differences between copyright infringement on the one hand and on the other breach of a contract which relates to copyrighted material.

Legal Standards For Evaluating A Petition To Award Attorneys' Fees To A Defendant In A Trade Secret Misappropriation Case

By Paul E. Freehling (July 18, 2012)

Section 4 of the Uniform Trade Secrets Act provides, in part, that if "a claim of misappropriation is made in bad faith. . . the court may award reasonable attorney's fees to the prevailing party." The terms "bad faith" and "prevailing party" are not defined in the statute. Most of the few judicial opinions interpreting those terms as they are used in the UTSA in relation to an award of fees in favor of a defendant are not officially reported.

A recent California appellate decision found that the trial court applied the correct interpretation of section 3426.4 (California applicable trade secret attorneys' fee statute) and did not abuse its discretion in finding "bad faith" on the part of the plaintiff in bringing its trade secret misappropriation claim against defendants and awarded over $400,000 in attorneys' fees. For a nice summary of the case, please see John Marsh's blog post. The applicable case law construing the trade secret attorneys' fees statute in each state must be carefully analyzed to understand when attorneys' fees are recoverable in trade secret cases.

Bad Faith

A majority of such cases hold that a determination of "bad faith" requires that both objective and subjective tests are met (a few decisions suggest that fee shifting may be permissible if either the objective or the subjective test is met without requiring both). The objective component of "bad faith" refers to a baseless complaint. The subjective component refers to egregious behavior in filing or pursuing misappropriation litigation.

To qualify as a specious pleading, the complaint must be unsupported by facts. The absence of relevant evidence favoring the plaintiff has been held to be a strong indicator of frivolousness, but a reasonable belief that the claim was colorable when it was filed may defeat a motion for the award of fees to the defendant.

With regard to the subjective "bad faith" standard, an illicit motive in filing or pursuing specious litigation has been found where, for example, one or more of the following acts occurred:

a. The plaintiff filed the litigation in an attempt to interfere with the defendant's existing customer relationships which pre-dated the alleged misappropriation;

b. The plaintiff made no substantial effort to retrieve the allegedly misappropriated trade secrets (for example, there was a lengthy and unexplained delay in seeking injunctive relief);

c. The plaintiff was guilty of spoliation of key evidence;

d. The plaintiff changed the theory of the case each time the defendant successfully rebutted a prior theory;

e. The plaintiff unreasonably refused to produce, until after repeatedly being ordered to do so, internal communications that proposed vexatious, oppressive litigation tactics against a competitor; or

g. The plaintiff engaged in pretrial tactics designed primarily to increase the defendant's cost to defend. One of more of these activities may be sufficient to meet the subjective test.

Degree of Proof

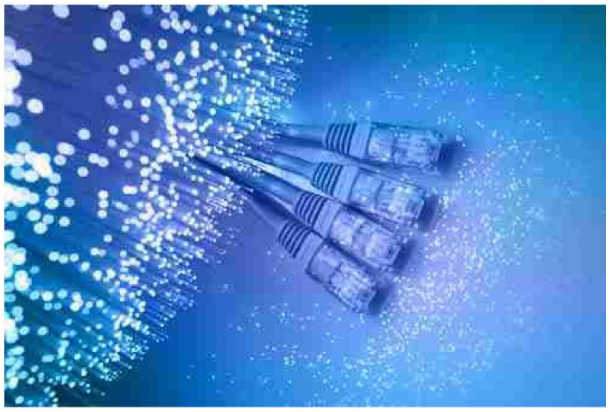
A minority of courts have written that a trade secrets misappropriation defendant seeking attorneys' fees must support the objective and subjective factors with "clear and convincing" evidence. In making the determination as to the applicable degree of proof, courts have considered whether an enhanced quantum is required for a fee-shifting decree in cases brought under such statutes and rules as a jurisdiction's Insurance Code relating to an insurer's bad faith refusal to defend or settle; Rule 11 of the Federal Rules of Civil Procedure, 28 U.S.C. ¶1927, or state counterparts; or 35 U.S.C. §285 concerning permissive attorneys' fees awards to the prevailing party in "exceptional" patent infringement litigation.

Prevailing Party

A trade secrets misappropriation defendant obviously would be the "prevailing party" after the entry of a final, non-appealable judgment dismissing all contested claims. But does the defendant qualify for an award of attorneys' fees if, say, after lengthy pretrial proceedings but before trial, the plaintiff voluntarily dismisses most of a misappropriation complaint without receiving any consideration? After a trial the court or jury awards the plaintiff only a nominal sum despite a demand for an exorbitant amount? The defendant prevails with respect to the trade secrets misappropriation claim, but the plaintiff is prevails in connection with a separate count filed by the plaintiff or regarding a counterclaim filed by the defendant?

Nevada Federal Court Rules That Plaintiff Must Identify Trade Secrets With Specificity Before Serving Discovery

By Jessica Mendelson (July 25, 2012)



A Nevada federal court recently held that a plaintiff must identify trade secrets with specificity prior to seeking discovery from the defendant regarding that claim, adding Nevada to the growing number of jurisdictions with that requirement.

In this case, *Switch Communications Group v. Ballard*, Case No. 2:11-cv-00285-KJD-GWF, the plaintiff owned and operated computer data centers in Las Vegas. Mr. Ballard, the defendant, had been employed by Switch as the company's Chief Financial Officer for two years, before his employment was terminated in 2006. According to the complaint, as a result of his employment, Ballard had acquired substantial knowledge of confidential information, including the location of plaintiff's carrier fiber and structure of carrier fiber agreements, location of key client installations, the terms of Switch's agreements with customers, and other such information. Switch alleged Ballard was preparing to build a competing business and utilize these trade secrets, and sued him for misappropriation of intellectual property, breach of contract, unfair commercial advantage, unjust enrichment, copyright infringement, and tortious interference with contractual relations.

As the case progressed, the defendant served interrogatories on the plaintiff, seeking to require the plaintiff to provide more specific information concerning its trade secret claims. The plaintiff was asked what trade secrets and other intellectual property the defendant had allegedly misappropriated. The plaintiff's initial answer to the interrogatory simply stated categories of trade secrets, but not the trade secrets themselves. The court found this was insufficient. The plaintiff then proceeded to serve discovery on Ballard, who argued that he should not be required to respond, since the plaintiff had not yet described the trade secrets with sufficient particularity.

The court held that Ballard was not required to respond, and that a party alleging a claim for misappropriation of trade secrets must disclose the trade secrets with reasonable particularity before being allowed to compel discovery. In making this ruling, the court relied *on DeRubies v. Witten Technologies*, 244 F.R.D. 676, 680-81 (N.D.Ga. 2007), which stated four policies supporting a reasonable particularity standard in alleging the existence of a trade secret. First, if discovery of a defendant's trade secrets were automatically allowed, it would result in fishing expeditions. Second, if the plaintiff fails to identify the trade secret at issue with some degree of specificity, there is no way of knowing what information is relevant in responding to discovery requests. Third, a lack of particularity makes it difficult to mount a defense, since a defendant may not be aware of what the trade secret

actually is, and finally, requiring a plaintiff to state what the trade secret is prior to misappropriation ensures that the plaintiff will not mold its cause of action around the received discovery.

The court also held that the defendant was required to supplement discovery responses once the trade secret was defined with reasonable particularity. Under Federal Rule of Civil Procedure 26, there is a duty to supplement discovery responses, and the court found that Ballard would have an obligation to comply once Switch properly defines the alleged misappropriated trade secrets. The court denied the plaintiff's motion to compel, holding Ballard need not respond to Switch's discovery requests until the trade secrets were defined with reasonable particularity.

Potential plaintiffs and defendants in trade secret misappropriation cases ought to keep this ruling in mind. A plaintiff who files a trade secret misappropriation complaint must be very specific in identifying the trade secret, and must be prepared to defend the specificity, at least in Nevada. Similarly, a defendant needs to be prepared challenge the plaintiff's trade secret identification if appropriate before providing substantive responses to discovery.

Considerations In Determining Whether To Grant To A Prevailing Trade Secret Misappropriation Plaintiff A Permanent Injunction In Addition To Substantial Damages

By Paul E. Freehling (August 7, 2012)

When a plaintiff alleging trade secret misappropriation obtains a judgment for substantial damages, the award may serve solely to compensate for past wrongs, or it may redress both past and future injuries.

The plaintiff filing a post-trial motion for the entry of a permanent injunction presumably is claiming that the defendant's continued use of the misappropriated trade secrets will cause damages that were not included in the judgment. Under what circumstances should this post-trial motion be granted?

There are prerequisites that apply to every motion for an injunction. These include a showing of irreparable harm in the absence of an injunction, inadequate remedy at law, balance of the hardships favoring the moving party, and little or no injury to the public interest. Further, the injunction must be tailored to the specific case and no broader than necessary to provide complete relief. Some jurisdictions require proof by clear and convincing evidence that each of the foregoing requirements is satisfied.

Having just been tagged with an award of money damages, the party opposing the motion for a permanent injunction is likely to argue that any alleged future grievance – just like past harm – can be remedied by suing at law. An additional argument could be that the damages award constituted adequate relief for both past and future injuries. For example, if the trade secret involved in the case is a compilation of customer and market data that becomes stale over time, and if a period of years has elapsed between the misappropriation and the judgment, there may be no future injury for which compensation will be owed. On the other hand, highly technical and sensitive data may have a longer useful life that continues for an extended period.

A requested injunction, following a substantial damages award, that prevents a former employee – even one who misappropriated trade secrets – from pursuing the occupation for which she or he is trained may be scrutinized more closely than an injunction ordering that confidential information be returned or not used. Similarly, a request for an injunction that would prevent the defendant from doing business with a customer whose relationship with the defendant pre-dates the misappropriation may be suspect.

Trading Secrets

In a few recent decisions, courts have indicated more reluctance to enter an injunction with respect to a trade secret developed not by the party seeking the injunction but by an entity that merged with or was acquired by the movant. Some courts presented with a motion for entry of a permanent injunction after a large damages judgment in a misappropriated trade secrets case also have expressed skepticism about the need for the requested injunctive relief if there was no earlier attempt to obtain a preliminary injunction.

In short, there can be obstacles to obtaining both a lot of money and a permanent injunction as a result of a trade secret misappropriation. However, in an appropriate case, those obstacles may be overcome.

Indiana Federal Court Holds That A Confidentiality Agreement Without Any Limitations Violates Indiana Law And That A Suit For Misappropriation Cannot Be Brought By A Plaintiff Who Uses A Trade Secret With Permission But Does Not Own It

By Paul E. Freehling (August 8, 2012)

Shortly before leaving the employ of Swanel Beverage, Inc. (a manufacturer of soft drinks, juice products, and energy beverages), Bodemer – Swanel's national sales and marketing manager who "was involved with almost every facet of Swanel's business" – incorporated Innovative Beverage, Inc. Right after Bodemer resigned from Swanel, Innovative commenced operations as a competitor. Then, he and Innovative filed a declaratory judgment action in the Southern District of Indiana alleging that his confidentiality and non-competition agreements with Swanel were unenforceable and were not violated. Swanel, of course, counterclaimed for breach of contract and violation of the Indiana Uniform Trade Secrets Act. Following discovery, Bodemer moved for summary judgment with respect to both his complaint and Swanel's counterclaim. Federal Judge James Moody's multi-faceted decision on Bodemer's motion included the rulings mentioned in the title to this blog and others. *Bodemer v. Swanel Beverage, Inc.,* Case No. 2:09 CV 90 (S.D. Ind., July 31, 2012).

Swanel claimed that the mandated confidentiality was worldwide and lasted forever, and that it applied to every piece of information Bodemer had learned, and every document he had received, in the 15 years he had been employed by a corporation Swanel acquired and then by Swanel itself. Thus, enforcement would confer confidentiality on much information and many documents that were not secret and would prevent Bodemer from being employed in the industry with which he was most familiar. Judge Moody held that the agreement was invalid under Indiana law. While recognizing that the state's courts might be willing to enforce an unconditional promise to maintain business confidences if necessary in order to protect the employer's reasonable interests, the confidentiality agreement here did not pass that test. Further, it unduly restricted Bodemer's future employment opportunities and was contrary to the public interest.

Swanel tried one more gambit, requesting the court to blue-pencil the confidentiality agreement by inserting appropriate restrictions. According to Judge Moody, however, Indiana law authorizes a court to strike unreasonable provisions in a contract but not to add new ones.

The non-compete commitment provided a reasonable geographic limitation, 100 miles from the present location of the company, and it expressly permitted the court to modify that restriction if it was found to be unenforceable. Judge Moody ruled that the agreement was not violated because the only Swanel customer Bodemer was accused of stealing was located more than 100 miles away. (Swanel argued that, although the customer was more than 100 statute miles distant, it was closer than 100 nautical miles, but that argument was summarily rejected based on the "plain meaning" rule and because nautical miles are used only in sea and air navigation.)

Swanel had more success in resisting Bodemer's summary judgment motion with respect to alleged misappropriation of Swanel's list of distributors, the name of the vendor supplying Swanel with flavoring agents, Swanel's recipe for drink products, and its pricing structure. Bodemer insisted that these were not trade secrets, but the court held that a reasonable jury could disagree. It could find that a competitor would have to make a substantial investment of time, expense and effort to create Swanel's list of distributors. There was value in identifying the source of the flavoring agents because replication of Swanel's products by a competitor would be somewhat easier if the vendor's name was public. The fact that the name of the flavor house Swanel used was known to its employees was of no consequence because each had signed a non-disclosure agreement.

According to Judge Moody, since Swanel did not own the flavor house's formula, it could not be the basis for a trade secret misappropriation case filed by Swanel. However, notwithstanding Swanel's president's deposition testimony that the recipe for its drink products was "no big deal" because it simply consisted of the flavoring plus sugar and water, the court said that was just one man's opinion and the jury had to decide whether the recipe was a trade secret. Bodemer's claim that he could not be said to have misappropriated Swanel's pricing structure because he took no documents with him was rejected because that is not essential in order to prove misappropriation.

This case provides several lessons. It reminds us that a confidentiality agreement lacking reasonable time, geographic and subject-matter limitations may be unenforceable as a matter of law. Additionally, while some courts are unwilling to blue-pencil a contract under any circumstances, a court that will is more likely to exercise that power when the agreement can be made enforceable by modifying or excising provisions without adding new ones. Perhaps Judge Moody's very brief explanation for rejecting Swanel's claimed right to sue Bodemer with regard to the secret formula – because Swanel did not own it – would have been different if Swanel proved that it was the exclusive purchaser of that flavoring and that its contract with the flavor house permitted Swanel to bring a misappropriation lawsuit despite not being the owner of the trade secret. In that event, Swanel might have been held to have standing just as the holder of an exclusive patent, trademark or copyright license might have standing to sue for infringement, even though the licensee is not the owner of the patent, trademark or copyright, if the license includes a grant of the right to file such an action.

Ninth Circuit Issues Opinion Vacating Arizona Jury's Misappropriation Damages Award Because Plaintiff Failed To Apportion Between Confidential Profit Margin And Expense Rate Information And Other Non-Trade Secret Information

By Paul E. Freehling (August 17, 2012)

Employer METI guarded its confidential financial information by, among other methods, locking printed versions in a corporate vault and password-protecting the information with the password provided only to those who signed non-disclosure agreements.

Shortly before departing METI's employ, employee Romeo allegedly downloaded thousands of his employer's confidential financial documents onto multiple flash drives. After he was employed by METI competitor ISS, he allegedly used the information in a PowerPoint presentation to ISS staff. ISS saved the presentation and referred to it in subsequent strategy meetings.

In *Management & Eng'r'g Tech. Int'l, Inc. v. Information Sys. Support, Inc.*, No. 10-17784 (9th Cir., July 23, 2012), the trial jury's verdict that METI's financial information constituted trade secrets under the Arizona Trade Secrets Act, and that Romeo and ISS misappropriated them, was held to be supported by the evidence. Although ISS claimed that the proof showed possession but not use of the misappropriated property, the appellate court declined to second-guess the jury's verdict regarding liability.

Expert witness testimony at trial concerning the value of METI's financial information withstood ISS' challenge to its admissibility. The expert was CEO of his own intellectual property consulting company, and he had more than 20 years of experience valuing such property for use in damages litigation and licensing transactions. The Ninth Circuit quoted from its own 2010 decision in *Primiano v. Cook*, 598 F.3d 558, 564: "Shaky but admissible evidence is to be attacked by cross examination, contrary evidence, and attention to the burden of proof, not exclusion."

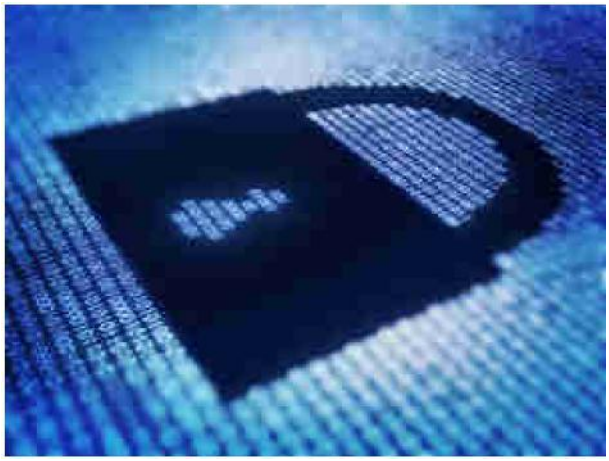
But METI was not entirely successful on appeal. At trial, METI also claimed trade secret protection for its employee roster and its ranking in a non-party's industry-wide "process improvement" program. All of this information was held to be publicly available and, thus, not a trade secret. Moreover, METI's expert witness testified to the lump sum a hypothetical buyer would have paid for all of the claimed confidential information but failed to show the value of just the information held on appeal to constitute

trade secrets. So, the damages award was vacated and the case was remanded for further proceedings. Lastly, the appellate tribunal rejected METI's challenge to the trial court's denial of METI's motions for awards of exemplary damages and attorneys' fees.

Because the Ninth Circuit's opinion is not precedential, the lessons learned from this case may have limited significance. However, the court did approve the way METI showed that it maintains the confidentiality of financial information. Perhaps the most important take-away for a plaintiff who alleges misappropriation of different categories of confidential information is to consider, in order to protect against only partial success because some categories are held not to constitute trade secrets, proving damages separately for each of the several categories.

Manhattan District Attorney Considers Formal Charges Against Computer Programmer For Alleged Theft of Confidential Trading Codes

By Jessica Mendelson (August 18, 2012)



On August 15, state proceedings were temporarily adjourned while prosecutors decide whether to file formal charges against programmer Sergey Aleynikov in this high profile trade secret/data theft matter.

Last week, Aleynikov was charged with state crimes for the alleged theft of confidential trading codes, despite the fact that the federal court of appeals had already dismissed federal charges earlier this year. The state prosecutors have not yet announced a formal grand jury indictment against Aleynikov.

Aleynikov first entered the limelight in 2009, after he was reported to the U.S. Attorney's office for allegedly stealing confidential trading code. According to the government's charges, Aleynikov allegedly copied and removed confidential company trading code to use at his new job at a startup company in Chicago. In 2009, federal prosecutors charged him with trade secret theft under the Economic Espionage Act and transporting stolen property in interstate commerce under the National Stolen Property Act (NSPA). In December 2010, he was convicted. The Second Circuit Court of Appeals overturned this verdict in February 2012, holding the stolen code was not a good or product intended for interstate commerce, and thus, Aleynikov had not violated either law. Aleynikov was released from prison in February 2012. Some legal commentators with the Second Circuit's decision.

It was thought that this may be the end of Aleynikov's legal troubles. However, on August 2012, Manhattan District Attorney Cyrus Vance filed state charges against Aleynikov. The District Attorney alleged Aleynikov had violated New York State law through "unlawful use of secret scientific material" and "unlawful duplication of computer related material." Both charges are felonies, and if convicted, Aleynikov could serve up to four years in prison. The case was recently adjourned, and Aleynikov was released on bail. Prosecutors have until October 23 to decide whether to file formal charges.

According to the Manhattan District Attorney's Office statement, the code allegedly stolen by Aleynikov is "so highly confidential that it is known in the industry as the firm's secret sauce." Furthermore, the District Attorney stated "employees who exploit their access to sensitive information should expect to face criminal prosecution in New York state in appropriate cases." We will keep you posted on this matter as proceeds in the New York state court.

Indiana Appellate Court Finds That Indiana Uniform Trade Secrets Act Preempts Common Law Misappropriation and Civil Conversion Claims In Mixed Martial Arts Broadcasting Dispute

By Ryan Malloy and Joshua Salinas (August 20, 2012)

The Court of Appeals of Indiana recently reversed and remanded a 2008 suit brought by the North American Boxing Council (NABC) against HDNet LLC (HDNet), in which the NABC alleged that HDNet stole its idea for a mixed martial arts (MMA) broadcast series after the parties had discussed a broadcast arrangement that never materialized into a formal contract.

The Court of Appeals held that the trial court erred in granting summary judgment because NABC's idea misappropriation claim fell under the Indiana Uniform Trade Secrets Act's (IUTSA) preemption provision and NABC's civil conversion claim did not fall within the "criminal law" exception to the preemption provision.

Plaintiff NABC is an MMA and professional boxing sanctioning body. Defendant HDNet is a high-definition television channel. In 2007, NABC and HDNet allegedly exchanged a series of e-mails to discuss HDNet's potential broadcast of MMA events. Of significant importance was an alleged email NABC sent to HDNet where NABC allegedly proposed and outlined its ideas for a unique weekly fight series model that was significantly different from other fight series models within the industry. The parties allegedly continued to exchange correspondence and discuss NABC's new proposed idea. While the parties did not have any confidentiality or non-disclosure agreements, NABC considered its unique fight series model to be a protectable commercial idea.

A dispute arose when HDNet formed a new company–HDNet Fights–to allegedly sanction, promote, and broadcast MMA events based on NABC's initially proposed model. NABC brought action against HDNet and asserted claims of, inter alia, idea misappropriation, trade secret misappropriation, and conversion of trade secrets.

NABC later moved for partial summary judgment on grounds that its idea misappropriation and conversion claims were not preempted under the ITUSA. The trial court granted NABC's motion, finding that the idea misappropriation and conversion claims against HDNet were not preempted under the IUTSA.

HDNet appealed. It argued that the IUTSA preempts common law idea misappropriation and civil conversion claims regardless whether the information at issue rises to the level of a statutorily-defined trade secret. The three-judge Appeals Court panel agreed.

As to the claim for idea misappropriation, the panel held that the claim amounted to a statutorily-defined trade secret, and stated that the "UTSA creates a 'two-tiered' approach to protection of commercial knowledge, under which information is classified only as either a protected 'trade secret' or unprotected 'general skill and knowledge.'... NABC's interpretation of the IUTSA would encourage piecemeal litigation and would thus fail to implement the legislature's intended goal of uniformity."

The panel rejected NABC's "plain meaning" argument that the preemption provision applies only to "trade secrets" and not "idea" misappropriation claims. The panel explained that this was a minority view that departs from the essential goal of the UTSA–uniformity among states adopting the statute. Specifically, the panel noted that the majority of jurisdictions hold that the UTSA preemption provision "abolishes all free-standing alternative causes of action for theft of misuse of confidential, proprietary, or otherwise secret information falling short of trade secret statutes (e.g., idea misappropriation....)." (quoting the Hawaii Supreme Court in *BlueEarth Biofuels, LLC v. Hawaiian Electric Company*, 235 P. 3d 310 (Haw. 2010)). Accordingly, the panel concluded that the trial court's summary judgment order was erroneous as a matter of law.

The panel also held that the trial court erred in granting summary judgment on the civil conversion claim because the claim does not delineate a criminal act and therefore is not saved by the criminal law exception to the IUTSA's preemption provision. The panel explained that a civil claim is "derivative" of criminal law and falls under the applicable exception when the civil claim is part of the same statutory scheme designed to combat the same wrongful activity as the criminal law, not simply because the claim provides a civil remedy for a crime.

The facts of this case again remind us of the importance of having written confidentiality agreements when exploring and discussing potential business with others. Moreover, the case illustrates that Indiana has an expansive preemption statute and that information not rising to the level of a trade secret may be difficult to protect in Indiana in the absence of an enforceable non-disclosure agreement.

Facebook Fans For Piggy Paint Not A Business Expectancy, Michigan Federal Court Dismisses Tortious Interference Claims for Facebook Page Takedown

By Joshua Salinas (August 22, 2012)

On August 9, 2012, a district court for the Western District of Michigan dismissed counterclaims of tortious interference with a business expectancy and conversion brought after the removal of a company's Facebook page and the alleged loss of its more than 19,000 "fans." (*Lown Companies LLC v. Piggy Paint LLC*, No. 11-cv–911 (W.D. Mich., Aug. 9, 2012)). This case illustrates how courts struggle with determining the value of Facebook friends, Twitter followers, and other social media "assets."

Plaintiff Lown Companies, LLC holds a registered mark "PIGGY POLISH" for nail polish products. Lown brought a trademark infringement action against Defendant Piggy Paint, LLC when Lown discovered that Piggy Paint was allegedly selling nail polish products under the mark "PIGGY PAINT NATURAL AS MUD." Lown also sent a take down request to Facebook, requesting removal of Piggy Paint's Facebook page on grounds of alleged copyright infringement (although it should have been brought based on alleged trademark infringement).

Facebook honored Lown's request. Piggy Paint consequently lost access to its Facebook page and access to its 19,000 "fans."

As a result, Piggy Paint raised several counterclaims against Lown, including tortious interference with a business expectancy and conversion. In particular, Piggy Paint alleged that it had a business expectancy in the more than 19,000 "fans" that "liked" its page. (Some commentators were surprised it had 19,000 fans in the first place - see Eric Goldman's scholarly and humorous blog on this case). Moreover, Piggy Paint alleged that Lown intentionally exercised control over Piggy Paint's mark by removing its page from Facebook.

The Court dismissed both counterclaims.

First, the Court found that "Piggy Paint has not and cannot show that the removal of the face-book page – which did not offer any means of placing orders or doing business – resulted in the loss of any business." The Court held that Piggy Paint's alleged business expectancy with its "fans" was "too

indefinite to form the basis of an actual expectation of business." Moreover, the Court recognized that Lown's removal request was based on its desire to protect own mark, not out of malice.

Second, the Court recognized that Facebook, not Lown, took down Piggy Paint's page. Thus, the conversion counterclaim was inapplicable to Lown to because Piggy Paint failed to allege that Lown had any authority or ability to control the page or force Facebook to remove it.

This case is important as the courts begin to address the ownership and value of social media "assets." It demonstrates the need explain the damages or harm incurred when bringing claims for the loss of social media friends, fans, or followers. The Court seemed to suggest that Piggy Paint may have proceeded on its tortious interference counterclaim if it explained how the loss of its "fans" caused a loss of business.

This case is analogous to the currently pending–and closely watched–*PhoneDog v. Kravitz* case, which involves a dispute over a company's alleged loss of its Twitter account and followers that were allegedly taken by a former employee. Similar to this case, the court in *PhoneDog* dismissed PhoneDog's tortious interference with a prospective economic advantage claim on grounds that PhoneDog failed to allege any facts regarding how the loss of its Twitter account and followers caused it any economic harm. The court subsequently allowed PhoneDog's claim to go forward once PhoneDog amended its complaint and explained how it lost advertising revenue from the loss of its Twitter account and followers: "there is decreased traffic to [the] website through the Account, which in turn decreases the number of website page views and discourages advertisers from paying for ad inventory on PhoneDog's website."

The *Piggy Paint* Court did not indicate in its opinion or order whether Piggy Paint's counterclaims were dismissed with or without prejudice. If the dismissal was without prejudice, Piggy Paint may be able to bring a tortious interference with a business expectancy counterclaim if it can provide specific facts and explain how the loss of its Facebook "fans" caused the loss of any business. This case also reflects a growing trend where courts refuse to accept conclusory allegations that the mere loss of social media "assets" is sufficient to show damages or losses.

This case also reveals the potential dangers in the use of social media to conduct business and as a company's primary marketing device. As seen in the *PhoneDog* case, issues will continue to rise regarding the ownership of social media accounts, connections through those accounts, and other valuable social media assets. In the recent *Eagle v. Morgan* case, a federal court in Philadelphia ruled an employer could claim ownership of a former executive's LinkedIn Account, where the employer had significant involvement in the creation, maintenance and operation of the account. Earlier this year, a Colorado federal court in *Christou v. Beatport*, LLC allowed a plaintiff's trade secret misappropriation claim based on the theft of MySpace "friends" to proceed.

These significant issues will continue to linger as the courts grapple with issues such as whether social media accounts and followers can be owned, misappropriated, converted, transferred, or assigned,

who may be liable when someone loses access to their social media accounts and followers, and what damages, if any, are recoverable.

Companies who utilize social media for business should consider the different protections and risks associated with each social network. For example, *Piggy Paint* demonstrates how a company can lose access to thousands of "fans" with simple takedown request from a competitor, at least in Michigan. The recent Facebook *(Piggy Paint*, Michigan), Twitter (*PhoneDog*, California), LinkedIn (*Eagle*, Pennsylvania), and MySpace (*Christou,* Colorado) cases, at least at this stage as the law develops, may reveal different levels of protection for each network in each state and may influence whether a company focuses their marketing efforts on a specific network.

While you can't put a price on friendship, it is becoming apparent that you may be able to in social media and sue for the loss or denial of that "asset"–so long as you provide specific facts and explain the actual value of the social media connection at least in some jurisdictions. We will continue to follow this rapidly evolving area.

Alabama Federal Court Issues Decision Regarding Measuring The "Amount In Controversy" When The Plaintiff's State Court Trade Secret Misappropriation Complaint Is Silent As To The Amount Of Damages And The Defendant Removes The Case To Federal Court

By Paul E. Freehling (August 23, 2012)

A recent Alabama federal court decision discusses how to determine the "amount in controversy" when a state court trade secret misappropriation case is removed to federal court based on diversity of citizenship, but the complaint is silent as to the amount of damages demanded.

In order to place a value on the allegedly misappropriated trade secrets, courts take into account such factors as a reasonable royalty the plaintiff might have charged for licensing the trade secrets, the plaintiff's lost income resulting from the alleged misappropriation, and the defendant's gross or net revenue received because of the claimed misconduct. In addition, consideration may be given to the estimated amount of the plaintiff's attorneys' fees that might be awarded, and an estimate of potential exemplary damages if the applicable statute permits such an award.

Plaintiffs Molex Company, LLC, an Alabama corporation, and its Cayman Islands marketing subsidiary Pacific Mining Reagents, Ltd., filed a trade secrets misappropriation suit in an Alabama state court against a Texas resident. The defendant was a former consultant to, and later the business manager of, Pacific. The complaint did not specify the amount of damages sought. Asserting that there was complete diversity of citizenship and an amount in controversy in excess of $75,000 exclusive of interest and costs, the defendant removed the case to federal court. Molex and Pacific conceded that diversity was complete but moved to remand on the ground that the amount in controversy did not meet the jurisdictional minimum.

The Alabama trade secrets misappropriation statute provides for an award of actual damages plus the defendant's profits and other benefits attributable to the wrongdoing. The defendant's profits equal its gross revenues from the misconduct, unless the defendant demonstrates deductible expenses and elements of profit attributable to factors other than the misappropriation. If the defendant engaged in willful and malicious misconduct, exemplary damages of not less than $10,000, plus attorneys' fees, may be awarded. The "amount in controversy" is the estimated sum of these amounts.

In determining whether it has subject-matter jurisdiction, courts consider whether the plaintiff could be entitled to more than $75,000 if liability is established. An assertion by the defendant in its removal petition that the "amount in controversy" exceeds the jurisdictional minimum usually will suffice unless it appears to have been pleaded "in bad faith" because, for example, the suit "obviously," or "to a legal certainty," cannot involve that much.

Although Molex and Pacific did not quantify their damages in the complaint, they did claim that the defendant used the misappropriated trade secrets to develop a product for sale to – that is, to "steal" – plaintiffs' $300,000 per year customer. The court concluded that, therefore, even if the plaintiffs' lost business were the only relevant criteria, the amount in controversy more likely than not exceeded $75,000. With the possibility of punitive damages and attorneys' fees awards added, the requirements for diversity jurisdiction were held to be satisfied, and so the motion to remand was denied. *Molex Co. v. Andress*, Civil Ac. No. 5:12-cv-2098-CLS (N.D. Ala., Aug. 10, 2012).

The defendant also challenged the Alabama court's personal jurisdiction over him since he maintained no office or residence in Alabama, he never set foot in that state or attempted to make sales to customers there, all face-to-face meetings with the plaintiffs' personnel took place in Texas, and he was paid by the Cayman Islands company (Pacific), not by the Alabama corporation (Molex). However, the plaintiffs countered that in the course of doing business the defendant regularly communicated by phone, fax and email with Molex's headquarters staff in Alabama. On balance, the court concluded that he purposefully conducted activities in Alabama, and that the alleged trade secret violations clearly were based in substantial part on his relationship with Molex. Therefore, he had sufficient "minimum contacts" with Alabama to warrant personal jurisdiction.

The opinion in this case provides a roadmap for supporting a claim that the "amount in controversy" meets the federal diversity jurisdiction standard when the complaint lacks specificity.

Using the International Trade Commission to Address Trade Secret Misappropriation Occurring Abroad

By Matthew Werber (August 24, 2012)

The Federal Circuit caught the attention of the ITC and trade secret litigators alike when it ruled in *TianRui Group Co. v. ITC* that the ITC can exercise its jurisdiction over acts of misappropriation occurring entirely in China.

The Commission initiated Investigation No. 337-TA-655 based on allegations that TianRui and a group of related respondents unlawfully accessed and used Illinois-based Amsted Industries, Inc.'s proprietary ABC process to manufacture imported steel railcar wheels. After unsuccessfully attempting to license the ABC process from Amsted, TianRui hired several employees from one of Amsted's Chinese vendors. After being brought to TianRui, the former employees disclosed Amsted's confidential information and enabled TianRui to begin using the ABC process to make steel railcar wheel parts bound for destinations in the U.S. The parties did not dispute that the acts of misappropriation occurred entirely in China. Following a trial before an administrative law judge, the Commission ultimately found that TianRui violated Section 337 and issued exclusion and cease and desist orders barring the subject TianRui wheel parts from entry in to the U.S.

On appeal, the Federal Circuit affirmed the Commission's determination. The majority found that 19 U.S.C. § 1337 ("Section 337") – the statute that governs the ITC's jurisdiction to investigate patent, trade secret and other intellectual property matters – focuses on the nexus between the imported articles and the unfair methods of competition rather than on where the misappropriation occurs: the determination of misappropriation was merely a predicate to the charge that TianRui committed unfair acts in importing its wheels into the United States. In other words, the Commission's interpretation of section 337 does not, as the dissent contends, give it the authority to "police Chinese business practices." It only sets the conditions under which products may be imported into the United States.

Less than eight months after the TianRui decision, Complainant SI Group, Inc., a Schenectady, NY based chemical manufacturer, followed Amsted's footsteps by requesting that the Commission investigate acts of misappropriation occurring entirely in China. SI Group alleges that Sino Legend (Zhangjiagang) Chemical Co., Ltd. and a group of related respondents (collectively referred to as Sino Legend) unlawfully accessed SI Group's trade secret process for making rubber resins and uses it to make imported resins.

According to the complaint, Sino Legend poached a plant manager from an SI Group manufacturing facility in Shanghai who disclosed SI Group's trade secrets to Sino Legend and enabled Sino Legend to bring the process in its own facility. On June 20, 2012, the Commission, after considering the complaint, announced their vote to institute an investigation, Certain Rubber Resins and Processes for Manufacturing Same (Inv. No. 337-TA-849). The parties are now engaging in fact discovery and the trial is scheduled to begin in February 2013.

Considering the ITC as a Trade Secret Litigation Forum

There is no question *TianRui* opened the ITC's doors to trade secret holders seeking to remedy misappropriation occurring abroad because some trade secret holders may find that the ITC is their only viable option. Most trade secret litigation occurs in state and federal courts (primarily state court). Yet, as a general proposition, the misappropriation must occur within the U.S. to fall within the state and federal court's jurisdiction and even then the misappropriators may flee the country to prevent effective service of process. Some U.S. companies have sought remedies in the country where the misappropriation occurred. Such efforts have resulted in varying degrees of success, however. SI Group, for example, alleges it pursued relief from Chinese authorities and courts. Yet, the Chinese courts have not taken any action according to SI Group's complaint. As such, many anticipate the number of Section 337 trade secret complaints to increase.

Trade secret holders considering filing a complaint in the ITC should be aware of certain considerations unique to the ITC litigation. For example, unlike district courts, the ITC generally does not have the power to order monetary relief. Instead, Section 337 gives the Commission authority to direct that infringing articles be "excluded from entry into the United States." Exclusion orders are enforced, in part, by U.S. Customs Border Protection ("CBP") officials who are instructed to identify articles subject to the exclusion order and prevent their entry into the U.S. While not a monetary award, an exclusion order is nevertheless a very powerful remedy. In *TianRui,* for example, the Commission issued an exclusion order prohibiting entry of the subject TianRui steel railway wheels for a period of ten years.

U.S. companies considering the ITC should also be aware that the ITC is subject to certain jurisdictional limitations that are not at issue in state or federal court litigation. For example, the trade secret holder must show the existence of a "domestic industry," or, generally speaking, an industry within the U.S. being affected by the infringer's alleged wrongful acts. In TianRui, the majority concluded Amsted satisfied the domestic industry requirement because the imported TianRui wheels could directly compete with wheels made by Amsted in its manufacturing facilities in the U.S. Yet, not all trade secret holders can meet this standard, particularly those with little or no U.S. presence. For more information on this interesting issue, please see the Seyfarth Shaw LLP webinar When Trade Secrets Cross International Borders.

Protecting Disclosure Of Trade Secrets Included In A Bid Responsive To A Government Request For Proposal

By Paul E. Freehling (August 25, 2012)

When confidential information or trade secrets are provided to a government agency in a bid for a public contract, they might wind up being disclosed to a competitor or others unless great care is taken by the bidder. Non-disclosure agreements are essential. Of course, all pages containing a trade secret should be designated as "confidential." Examples of other protective measures that might be utilized include placing on each such page limitations on permissible access, and referring in all written and oral communications relating to any of those pages that they contain proprietary data. If there are mock-ups or models embodying a trade secret, a non-disclosure agreement should be obtained from anyone permitted to see them. When, of necessity, a trade secret needs to be disclosed in court papers, an attempt should be made to submit them under seal.

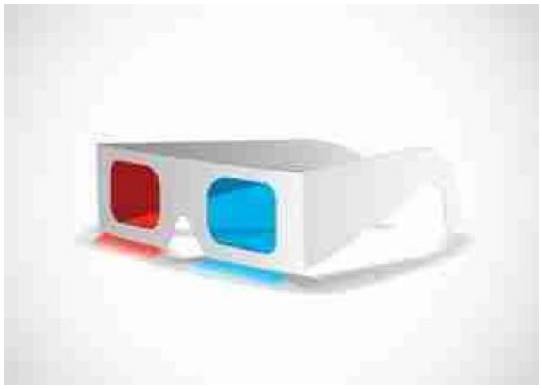
Under contract with school districts, Delcom designs and installs customized, interactive, and media-driven equipment used in classrooms. Delcom submitted two multi-million dollar bids in response to a RFP from a Dallas school district ("DISD"). A competitor, Prime, submitted one bid. Delcom was the highest ranked bidder, and contract negotiations with DISD commenced. About three weeks later, however, DISD notified Delcom that (a) the Texas Education Code disqualified the company because of its failure to disclose that one of its employees had been convicted of a felony, and (b) DISD intended to enter into contract negotiations with Prime.

Delcom promptly filed suit in a Texas court against DISD and Prime, asserting various tort and contract claims including misappropriation of trade secrets contained in Delcom's bidding documents and in a model classroom it built as part of its RFP bid. Delcom asked for injunctive relief. In the course of a TRO hearing, Prime returned to Delcom all of its documents that Prime had received from DISD, and Prime assured the court that none had been used. For these and other reasons, the trial court denied Delcom's request for injunctive relief against both of the defendants and dismissed the case against DISD. These rulings were affirmed on appeal. *Delcom Group, LP v. Dallas Indep. School Dist.*, Case No. 05-11-01259-CV (Tex. Court of Appeals, Aug. 17, 2012).

Delcom's litigation effort failed largely because of a number of facts unique to this case. The part of the decision most useful to attorneys and clients interested in trade secret law is the court's discussion, summarized in the first paragraph of this blog, of actions that can be taken to protect confidential information contained in a bid submitted in response to a RFP.

Alleged Breach of Non-Disclosure Agreement Related To 3-D Technology At Issue In New California Suit Involving Hollywood Heavyweights

By Jessica Mendelson (August 26, 2012)



In a legal matchup involving some Hollywood heavyweights, Thomas Randolph filed suit in Los Angeles Superior Court recently, alleging he was defrauded out of his stake in a prominent 3-D movie technology venture.

Randolph sued William Sherak, the son of Motion Picture Academy of Arts and Sciences President Tom Sherak and a prior chairman of 20th Century Fox's domestic film group; movie producer Christopher Mallick; actor Giovanni Ribisi, star of such films and television shows such as *Avatar, My Name is Earl,* and *Cold Mountain*; software developer Kuniaki Izumi; and William Morris talent agent David Phillips.

Randolph alleges that his company's alleged trade secrets were stolen in violation of a non-disclosure agreement, he was not paid his share of company profits, and he was falsely accused of self-dealing. Randolph also seeks damages for intentional interference with prospective economic advantage, intentional interference with contractual relations, fraud, negligent misrepresentation and breach of contract.

Mallick formed MRSF LLC, which was previously known as StereoD LLC in 2009. The company is one of the top 3-D conversion companies in the country, and its products include the films *Captain America, Avatar,* and *Thor*. The company allegedly planned to market and sell Izumi's software technology, and Randolph was allegedly hired to create the business plan for the company. Randolph, who was a principal at Kerner Technologies, a spin-off of George Lucas' Industrial Light and Magic at the time, allegedly initially met with Mallick in late 2008. During their meeting, Mallick allegedly expressed interest in converting two dimensional movies to three dimensional movies. According to the complaint, Randolph told Mallick about VDX technology, and persuaded Izumi to combine that technology with Kerner's CPX technologies, and then allegedly with Kerner's consent, Randolph entered into an agreement with Mallick.

As alleged in the complaint, the parties verbally agreed that Randolph would be the company's Chief Technological Officer, and would own a 5-10 percent stake in the company. Under the terms of the alleged agreement, he would also be entitled to license Kerner's CPX technology freely. Randolph and StereoD entered into a non-disclosure agreement prohibiting Randolph from disclosing the company's confidential information and business plan. Randolph alleges, however, that before the deal was even

completed, Phillips began conspiring against him over finder's fees, which he believed he was owed in exchange for introducing Randolph and Mallick. According to Randolph, Phillips allegedly double crossed him, notifying Ian Rose, Kerner's general counsel, that Randolph was self-dealing, and trying to exclude Kerner from any future deals. Mallick, who also believed he was owed a finder's fee, allegedly furthered the legend of Randolph's self-dealing. After rumors allegedly arose that Randolph was breaching his fiduciary duty to Kerner in February 2009, Randolph resigned from the company 2009, after he was accused of failing to disclose the VDX deal to Kerner Technologies.

Following Randolph's resignation from Kerner, Mallick, Ribisi, and Sherak ejected him from StereoD. According to the complaint, Randolph allegedly stayed in touch with Izumi, however, who assured him he would protect Randolph's interests, and that Randolph would still receive a cut of the profits. Mallick, Ribisi, and Sherak allegedly ended up making tens of millions of dollars when the company was purchased by Deluxe 3-D for approximately $50 million. The company then allegedly proceeded to implement a business plan that was quite similar to the "structure, objectives, development strategy, production methodologies, revenue goals and exit strategy" Randolph had envisioned in 2009. Randolph alleges that after the company's purchase, he discovered Izumi was part of the overall conspiracy against him, and that he himself lacked any equity or ownership interest in the company. Following this revelation, Randolph filed the lawsuit in July 2012.

Last year, talent agent David Phillips filed a similar lawsuit, against the company, alleging breach of oral partnership agreement, breach of contract, breach of fiduciary duty, and conversion. The case settled before trial for an undisclosed sum.

The interplay between Hollywood heavyweights, alleged breach of a confidentiality agreement, purported trade secrets, and white hot 3-D technology makes this new suit an interesting matter to follow and serves as an unfortunate reminder of how some business dealings can run astray.

When the Government Wants Trade Secrets: Presenting a Shield-or-Disclose Framework

By Elizabeth Rowe (August 29, 2012)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry by University of Florida Law Professor Elizabeth Rowe regarding protecting trade secrets from disclosure by the government. Professor Rowe's expertise is in intellectual property law. Her scholarship focuses on trade secrets, as well as the interaction of intellectual property policies with business and technology. She is a prolific scholar who has published numerous law review articles and contributed to several books. Professor Rowe's recent casebook is the first in the United States devoted exclusively to Trade Secret Law. Enjoy Professor Rowe's article

-Robert Milligan, Editor of Trading Secrets

I. INTRODUCTION

The government collects an enormous amount of information from companies that it stores, analyzes, and disseminates to government agencies, other companies, and the public. This practice increases the chances that information disclosed to the government that should remain secret does not. Accidental disclosures of confidential and trade-secret information do occur. Over the last few years, several government agencies have inappropriately handled or inadvertently disclosed company trade secrets. In one case, for example, the EPA disclosed one organization's trade secrets to an environmental organization. In another case, the FDA has been accused of inappropriately disclosing to a prisoner the secret formula to a drug, and posting on its website another company's trade secrets contained in a New Drug Application.

Disclosure of company trade secrets by the government to the public is already addressed in the elaborate regulatory scheme of agency rules and regulations, as well as in the FOIA case law. However, there is a paucity of case law and other guidance specifically relevant to cases where a company refuses to submit trade-secret information to the government ("refusal-to-submit" cases) and when the government is entitled to a company's trade-secret information. I propose a "shield or disclose" model that, among other things, makes clear the roles and burdens the various players must assume. It requires a threshold determination that the information in question qualifies for trade-secret protection under the common law. It also requires evidence of need, relevance, and potential harm before a court could order disclosure.

II. STRIKING THE BALANCE IN DISCLOSING TO THE GOVERNMENT

The unique nature of trade secrets—that they exist only so long as they are not disclosed or disclosed in confidence—requires an arrangement that ensures against accidental, unauthorized, or other improper disclosure. The owner of trade-secret information should never make a disclosure, either voluntary or involuntary, without enforceable restrictions against general disclosure. However, when it is determined that it is in the public's interest that the information be disclosed to the government, a delicate balance must be observed.

Accordingly, a clear model is needed to determine when trade-secret information should be submitted to the government in the first place. The model suggested here addresses disclosure to the government, not the subsequent and separate step of disclosure by the government to the public. The latter is already addressed, albeit not perfectly, in the elaborate regulatory scheme of agency rules and regulations, as well as in the reverse-FOIA case law. Thus, once the government has the information in its possession, whether received voluntarily or through compliance mandates, the current regulations are applicable to protecting them.

A. THE SHIELD-OR-DISCLOSE MODEL

The body of law that would allow corporations to refuse to submit proprietary information to the government, when they are not required to do so under a regulatory scheme, is trade-secret law. Because of the dearth of case law and other guidance specifically relevant to refusal-to-submit cases, I have considered a wider body of cases that implicate disclosures of trade secret by the government as well as disclosures made in the context of pending litigation. The end result is what I will refer to as the "shield or disclose" model.

Ultimately, the proposal creates a procedural and substantive path to identify the circumstances under which a court should compel a trade-secret holder to produce its trade-secret to the government. As a general policy matter, when the public interest in the disclosure outweighs the harm to the company from disclosure, the court may justifiably compel disclosure. What does that mean, however? How is it determined? These are the questions for which this framework aims to provide guidance. It is, admittedly, not the sole answer, but rather a modest step in the direction of achieving a more principled approach to refusal-to-submit cases, a step that is grounded in trade-secret law and consistent with the policy considerations that underlie governmental access and disclosure.

1. Company Establishes Trade-Secret Status and Harm

The first step of the process, having both procedural and substantive significance, requires that the trade-secret owner establish that the requested information qualifies for trade-secret protection and that harm will result from disclosure of the trade secret to the government. Whether the information in question meets the status of a "trade secret" should always be the threshold question, and it is the trade-secret owner's burden to make that showing. While companies often try to claim protection for confidential and proprietary business information, trade-secret protection applies only to the smaller subset of information that qualifies as an actual trade secret. Therefore, in most cases, this first question could be determinative of the entire issue of disclosure because if the information is not a

trade secret, then that significantly weakens the argument against disclosure. If the trade-secret owner is unable to establish trade-secret status, then the inquiry likely ends in favor of the government.

The trade-secret owner must then articulate the competitive harm that would be caused from disclosure of the information to the government. This is in keeping with trade-secret law's focus on protecting against unfair competition and the existing articulation of harm in some of the regulations as competitive harm. For example, SEC regulations require that a business provide information regarding the adverse consequences that could result from disclosure of confidential information, including any adverse effect on its competitive position. Similarly, on the likelihood that the disclosure would result in harm, EPA regulations require a showing of "substantial harmful effects to the business' competitive position" and "an explanation of the causal relationship between disclosure" and the harm. Moreover, in the FOIA context, competitive harm has been interpreted to mean that the harm flows directly from a competitor rather than from a customer or employee or other source. Thus, a trade-secret owner would need to establish the likelihood that such harm would occur if the information it produced to the government were to be obtained by its competitors.

2. Government Establishes Relevance and Need

Once the trade-secret owner has established the trade-secret status of the information and the harm that is likely to result from its disclosure, the burden then shifts to the party requesting the information (i.e., the government) to prove relevance and need for the information. This is similar to the good-cause burden under the discovery rules. Given the unique nature of a protectable trade secret and the devastating harm that could result from its disclosure, the better policy is that a trade secret should not be ordered produced unless the actual trade secret (as opposed to some other information related to the trade secret) is directly relevant to the inquiry for which it is sought.

Relevance, for the purposes of this proposal, is similar to the standard that has been used under Rule 26 of the Federal Rules of Civil Procedure. However, relevance should probably not be interpreted as broadly for trade-secret purposes as it is under the discovery rules. Whereas the underlying rules and policies in the discovery context favor greater disclosure between the parties, trade-secret law, on the other hand, is grounded in secrecy and the requirement that trade secrets should not be disclosed without appropriate assurances of confidentiality by the receiver. Accordingly, this might suggest that the relevance standard should be interpreted narrower than under the discovery rules. The current FOIA rules and cases do not require that the party requesting information from the governmental agency establish relevance. However, given the higher scrutiny that should be given to the disclosure of trade secrets, it makes sense to require a showing of relevance.

While the FOIA rules do not require a showing of need either, evidence of need is required under my proposal. The government requestor should demonstrate need for the information separate and apart from relevance. This inquiry would focus on such considerations as: (1) whether the information sought is available elsewhere; (2) whether acceptable substitutes for the information can be found from other sources; (3) whether the public interest in receiving the information can only be protected via receipt of

the trade-secret information; and (4) whether the public could suffer injury to their health or safety if the information is not released to the government.

3. Court Balances Need Versus Potential Injury

Satisfied that the requested information qualifies for trade-secret protection, the court must ultimately balance the government's showing of relevance and need against the trade-secret owner's claim of injury that could result if disclosure is compelled. In considering the government's need for the information, the court could factor in who the requestor is and the purpose for which the information is sought. None of the existing approaches pay particular attention to these questions, but they could add value when dealing with trade-secret cases. A further consideration may be whether the trade-secret information is critical to the government or the public. If not, perhaps the company can comply without disclosing the specific trade secret. If yes, then disclosure with greater assurance of protection might be advisable, possibly ordering, for instance, that the information is outside the agency's discretion to disclose or that it be "sealed."

Moreover, the court could also consider the nature of the trade secret in evaluating need and risk of injury. Because trade secrets can be virtually any kind of business information, it may matter whether the information sought is the secret formula to the company's core product, or a list of the company's customers; the encryption code to a black box or the record of drivers' braking patterns during an unintended-acceleration incident.

The shelf life of the information could also be considered to determine whether the nature of the information is such that it will no longer be secret after a short period of time. It could, for instance, be a marketing-related secret that will be divulged or reverse-engineered after a product is released. In that situation, the court may lean toward not ordering disclosure, since the requestor will likely have access to the information by legitimate means in a relatively short period of time. This assumes, however, that there is no immediate critical need for the information.

Whether the trade-secret owner can persuade the court of the harm that could result if the trade secret is ordered disclosed is a very important part of the balance that the court must aim to achieve. The scope of harm, whether limited to that by a competitor, for instance, compared to a more widespread public harm, may matter. However, defining harm can be difficult. The risk of harm is an important component of this evaluation and could be influenced by the government's assurances of safeguarding the trade secret.

Besides harm to the company, the court may also consider harm to the public if the information is not produced to the government. This would therefore allow for those circumstances where the health and safety of the public are so threatened that disclosure should be compelled. In other words, the harm to the public would outweigh any competitive harm that the proprietor of the trade secret may suffer. As recognized under well-settled takings principles, the government's use of information for the public good (with adequate compensation) would not likely violate constitutional norms. Accordingly, a court in its discretion could order disclosure in those circumstances.

4. Court Determines Scope of Order

After weighing the various considerations, a court could find that production of the trade-secret should not be ordered. This will end the inquiry and the trade-secret owner prevails. On the other hand, if the court determines that production should be compelled, then the delicate task of crafting an appropriate protective order will remain. A court should not compel production of a trade secret without a protective order and appropriate safeguards for protection of the secret.

The court could choose from a range of options, depending on the particular case, to determine the appropriate scope of the order. For instance, limited disclosure could be ordered, such that the government may not receive the entire trade secret, but part of it. This does not appear to be the current scheme under FOIA, which is an all-or-nothing approach. Thus, there could be a middle-ground approach, one that would meet the requestor's need for the information while still protecting the trade-secret owner's interests. A mosaic approach might also work, where the trade-secret information is disaggregated such that the disaggregated form does not reveal the trade secret, yet it remains valuable information to the requestor. The FTC rules, for instance, provide for the disclosure of disaggregated information to other agencies, and to the extent the secret information can be segregated from the nonsecret information, a portion of the record may be disclosed to a FOIA requestor. In some circumstances, a court could order disclosure contingent upon some payment to the trade-secret owner. This would be akin to a compulsory license where, for instance, the court has deemed that withholding the information from the public will have an injurious effect on the public welfare.

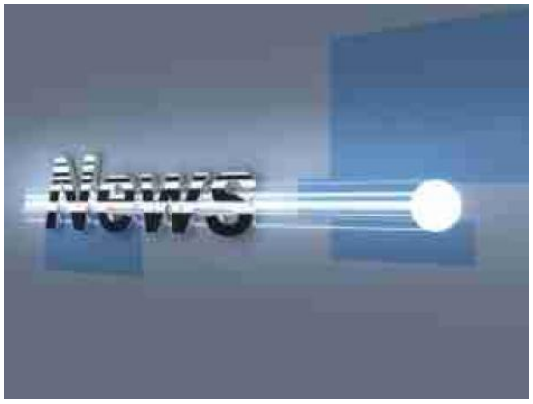
III. CONCLUSION

Refusal-to-submit cases raise some delicate issues on both sides, since the interests of all involved parties must be given very serious consideration. While these cases will necessarily be decided on a case-by-case basis, an approach that takes into account trade-secrecy principles, in addition to a more structured approach to government-disclosure policies, will better achieve the balance between secrecy and access. It will also allow for the crafting of more creative solutions that are better able to serve the needs of the respective parties. The shield-or-disclose model presented here helps meet those ideals by making clear the parties' burdens of proof on showing harm, relevance, and need before trade secrets are to be handed over to the government. Ultimately, it provides a more balanced, more specifically tailored approach that offers more of a middle-ground solution than currently exists.

Professor Rowe's piece is derived from a law review article which first appeared in the Iowa Law Review. The article more thoroughly presents and explores the background research leading to the development of the shield-or-disclose model, including a discussion of existing agency regulations governing trade secrets. *See* Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?* 96 Iowa Law Review 791 (2011). Professor Rowe thanks Lamar Miller for providing research assistance on this piece.

Extraordinary 20-Year Global Injunction For “Bulletproof” Trade Secrets Theft

By Joshua Salinas (August 31, 2012)



We previously blogged in our 2011 year end review about a noteworthy trade secret misappropriation case where DuPont Co. successfully obtained a jury verdict of approximately $920 million in damages against rival Kolon Industries Inc. DuPont sued Kolon for the alleged theft of trade secrets regarding a proprietary fiber used to make “bulletproof” police and riot gear.

Yesterday, U.S. District Court Judge Robert Payne (E.D. Virginia) issued a 20-year worldwide permanent injunction against Kolon, which prohibits Kolon from producing and manufacturing its Heracron fibers that were found to use and incorporate DuPont’s trade secrets.

John Marsh at Trade Secret Litigator has an excellent discussion of this astonishing decision and explains how this decision may have tremendous implications throughout the U.S. and worldwide.

One of the major takeaways from this case is Judge Payne’s holding that the U.S. Supreme Court’s 2006 decision in *eBay Inc. v. MercExchange, L.L.C.*–which had a significant impact on patent cases because it eliminated the presumption of irreparable harm–does not apply to trade secret injunctions. In particular, Judge Payne found that *eBay* applied to federal statutes (e.g. patent, trademark, copyright), but not Virginia’s Uniform Trade Secrets Act.

In light of the recent proposed legislation for a federal trade secret statute, we wonder whether such a federal statute would change Judge Payne’s analysis and the applicability of *eBay* to trade secret injunctions.

"Prior Restraint" Doctrine May Preclude Enjoining A Newspaper From Publishing Misappropriated Trade Secrets

By Paul E. Freehling (September 3, 2012)

A reporter for a business publication somehow obtained information contained in a privately held company's confidential interim financial statements. As the reporter was about to disseminate that information in an email alert to the publication's subscribers, the company sued, described the financials as trade secrets belonging to the company, and obtained from a Louisiana state court judge a TRO enjoining issuance of the email. The defendant removed the case to the Eastern District of Louisiana federal court where a magistrate judge conducted a preliminary injunction hearing and then ruled that freedom of speech and of the press guaranteed by the First Amendment trumped the company's efforts to prevent a potential violation of the Louisiana Uniform Trade Secrets Act. *Rain CII Carbon, LLC v. Kurzy*, Civ. Ac. No. 12-2014 (E.D. La., Aug. 20, 2012).

Rain CII Carbon, LLC is one of the largest coke calciners in the world (coke calciners convert a by-product of the oil refining process into a material essential to aluminum smelting). Its quarterly financial compilation statements are confidential, made available only on a secure, password-protected website to persons who have a right to the information and who sign a non-disclosure agreement.

The day after a compilation of Rain's 2012 second quarter financial results appeared on the company's website, business publication Debtwire, a member of the Financial Times Group, prepared the email alert reporting Rain's earnings. What particularly rankled the company was that its highly confidential gross margins could be calculated from information in the email alert.

Rain immediately filed suit against Debtwire in a Louisiana state court, requesting a TRO – and preliminary and permanent injunctions – to stop the publication. That court granted the TRO. Debtwire's emergency appeal was unavailing, whereupon Debtwire removed the litigation to federal court based on diversity jurisdiction. Rain promptly filed an amended complaint, adding Kurczy (the reporter who broke the story) and corporate affiliates of Debtwire as defendants, and Rain moved to remand on the ground that complete diversity was lacking. The motion to remand was denied. A preliminary injunction hearing was scheduled for one week later, the parties stipulating that the TRO would remain in place until the hearing.

The hearing took place on a Friday. Among the documents admitted into evidence was Kurczy's affidavit in which he swore that he had not accessed Rain's secure website and had not seen the

earnings compilation itself. The court issued its ruling the following Monday which was only three weeks after the compilation had been prepared. For purposes of the motion for preliminary injunction, the judge accepted Rain's contentions that its earnings compilation constituted a trade secret and that publication might cause irreparable economic harm to the company. Nevertheless, finding that the information in the email alert was truthful and was of potential interest to the email's subscribers, the court held that Rain had failed to overcome the strong presumption against a prior restraint.

First Amendment cases suggest that a litigant must overcome significant obstacles in order to persuade a federal court to enjoin the press from publishing truthful information on a matter of public concern, even if what is to be published is a trade secret. Having had more success in the state courts than in the U.S. District Court, Rain currently is in the process of appealing to the Fifth Circuit Court of Appeals denial of the motion to remand.

The Use of Digital Forensics in Trade Secret Matters (Part 3 of 3)

By Jim Vaughn (September 5, 2012)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy the third part of a three part blog series by digital forensics expert Jim Vaughn, a Managing Director of Intelligent Discovery Solutions.

Welcome to part 3 of this three-part series. Part 1 covered the BYOD concept and storage devices/areas considered for trade secret investigations, Part 2 covered forensic artifacts potentially located on devices such as Blackberrys, iPhones/iPods or Androids, and now Part 3 will cover the design and application of protocols.

Because protocols are necessarily fact and equipment specific, this is not intended to be an out of the box protocol, but instead it is a pseudo protocol used as an attorney guide to the discussion points you will probably have with your forensic expert when drafting an actual protocol.

Let's assume a set of hypothetical facts: Several departed employees went to work for the same competitor. These employees may have left all at once, or through a trickle effect over time that eventually raised suspicion. The former employer has raised theft of trade secrets allegations.

How do the facts play into the need to develop a protocol, or do they?

Within these facts, an effective protocol should include the means to identify, preserve, collect, review, produce (return), and remediate the data of interest. These protocol guidelines are intended to assist Plaintiffs, Defendants, or Forensic Neutrals.

The Anatomy of a Protocol

What is a Forensic Protocol? For purposes of this blog I will describe it as a set of agreed upon instructions between the legal team(s) and the forensic team(s) to provide for the consistent, methodical, high quality collection, cataloging, and analysis of electronic devices.

In addition to how to produce and remediate, a typical protocol will contain instructions on how to mechanically collect your devices, instructions on how to document your devices, and instructions related to the analysis of interest.

You may also desire to pre-plan and document searches of the collected data for specific keywords, investigate the usage of online repositories for storage of sensitive data, search for personal email usage, and investigate the transfer of sensitive data to personal computers or other personal devices such as smart phones or tablets.

You may consider the inclusion of custodian questionnaires and/or affidavits from the individuals involved. These are designed to give the peace of mind that all new employer data sources and employee personal devices/storage areas have been identified, searched and remediated.

Your forensic expert should have a solid understanding of what questions to ask to understand the many types of data sources that could play a role in the investigation and what company and system configurations need to be considered to execute an effective protocol.

Imaging / Collection of Data

Part 1 listed several data sources for consideration. If data collection techniques are part of your protocol, know there are several ways to collect data and the method of collection may be dependent on the source being collected. Included here are three different methods to forensically collect data from a workstation (e.g. laptop/desktop):

The hard drive will be physically removed from the workstation(s) to be imaged and attached to one side of an industry recognized forensic imaging hardware device.

If deemed better to leave the original hard drive in the workstation for imaging, then an industry standard forensic software program capable of being run from CD will be used for creating the forensic images.

If the laptop is using encryption, the login credentials will be provided so a live forensic image can be created.

For other data sources, there are specific methods and/or tools that are standard within the forensic community. Protocol verbiage may be precise as to the required tools to be used, or more general to include language that just requires it to be performed and documented in a forensically sound way. Generally speaking, the larger the collection effort and the more people involved, the more helpful precise language will be. In either case your forensic expert should quality control the forensic collections for completeness and accuracy.

Your protocol should include verbiage that will document particularities of each data source identified or collected as part of the protocol. This will include the computer/server's make, model, and serial number, and if possible, documentation of the hard drive(s) located inside each computer. Depending on the circumstances, you may want pictures as part of the documentation.

Device Documentation/Analysis of Interest

Now that you have the evidence forensically captured, let's look at items you may want to include in the protocol as part of the analysis. These items will help you determine certain things like when the hard drive was put into use, when the operating system was installed, users of the computer(s), what external devices were connected and what files were opened from these connected devices. Some sample wording for these activities include:

1) Investigate and document the format date of the hard drive(s);

2) Investigate and document all dates of installation (and/or reinstallation) of the operating system;

3) List all Windows accounts, including all administrator accounts, system accounts and user accounts, and include documentation of the following information for each account:

    a) When the account was created;

    b) When the account was last accessed (used);

4) Investigate and document the existence of any type of external device connected to any hard drive (e.g., thumb drives, CD-ROMs, DVDs, external hard drives, etc.);

5) Investigate and document the dates, types of software, manufacturers of any software, and name(s) of any software used to potentially wipe, erase, or shred data on any computer hard drive(s);

6) Investigate and document the dates and name(s) of any software used to perform virus scans, and whether such programs were used; and

7) Investigate and document the existence of any link file(s) that show files being opened from any remote location, CD/DVD or an externally connected device.

In summary, this blog post was designed to help lawyers and clients understand the pros, cons and challenges when considering the use of protocols. I hope it has helped you gain a better understanding of how to approach trade secret investigations from a technical perspective, causes you to ask a lot of technical questions and to use your forensic expert as your "geek speak" translator.

Mr. Vaughn is a digital forensics expert who has given testimony in nearly 65 cases involving topics such as evidence preservation, documentation of events, and computer forensic methodologies. In addition to being an EnCase Certified Examiner (EnCE), Mr. Vaughn is certified by the International Association of Computer Investigative Specialists (IACIS) as a Certified Forensic Computer Examiner (CFCE). Mr. Vaughn has extensive experience working on litigation and consulting matters involving computer forensics, e-discovery and other high technology issues. He serves his clients through the litigation or consulting lifecycle by assisting them with important issues like data scoping, preserving, gathering, processing, hosting, review and production, as well as deeper diving issues uncovered through the use of computer forensics. Mr. Vaughn can be contacted at

jvaughn@idiscoverysolutions.com. Please note that each case may be unique and this single blog post is not intended to fully cover everything related to trade secret investigations or constitute advice, legal or otherwise. It is always best to consult a qualified person to assist with any investigation.

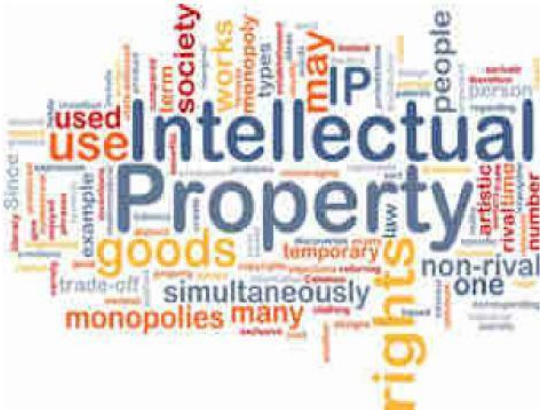
Trading Secrets

When Everything Becomes Software, How Does That Affect IP Strategy?

As a special feature of our blog —special guest postings by experts, clients, and other professionals— please enjoy this blog entry about the impact of software on IP strategy by technology lawyer and IP strategist Joren De Wachter. Joren serves as a Vice Chair with me on the ITechLaw Intellectual Property Law Committee and has an excellent blog of his own on current technology issues. Enjoy Joren's article.

-Robert Milligan, Editor of Trading Secrets

By Joren De Wachter (September 8, 2012)



Everything becomes software

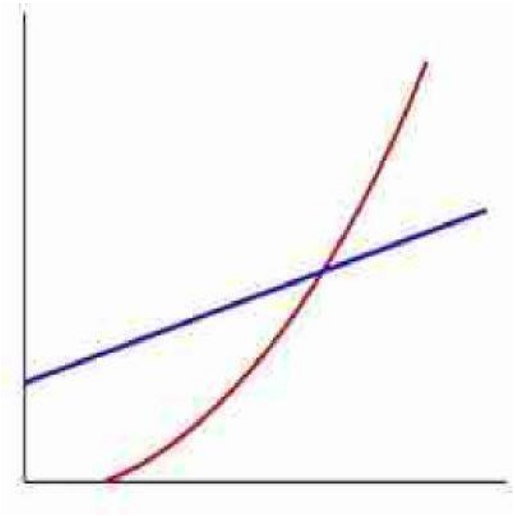
Marc Andreessen, co-founder of Netscape and currently co-founder and general partner of the venture capital firm Andreessen-Horowitz, wrote in August 2011 in the Wall Street Journal about how "Software is eating the world."

While Mr. Andreessen was building on earlier observations, such as the author of this article, that software is the "viral" industry, as it infects all other industries, he did provide some focus onto a very important phenomenon. This phenomenon is the fast growing importance of software in pretty much any industry or human activity. This reflects is the practical side of the fact that we are converting (updating?) into a digital world.

This is a profound change, with many consequences.

One consequence is that the software invasion is not limited to the way products function or are sold. While it is true that a phone is no longer a phone, but a very powerful small computer with a basic personal conversation application, just like a car is turning into a very powerful large computer with a basic personal transportation application (an App that will automate soon), the presence and impact of software is much more pervasive than that. All other aspects of business, and society, tend to become computerized. From supply chain management to enterprise resource planning, from marketing to HR, from legal to sales (force.com), all aspects of activity become computerized, and the relative importance of software in all of those aspects is growing.

A second consequence is that the growth of the digital part of an activity inevitably outpaces the growth of the non-software part. This is caused partly by Moore's law, but also by the fact that software is not



called “information technology” for nothing. Information tends to multiply, and increase its productivity, much faster than hardware.

The graph gives a pretty good illustration of what happens when software enters into an activity or product. The red line represents growth in software added value, the blue line in hardware added value. The relative importance of software tends to grow at exponential or semi-exponential rates, while the non-software parts grow at a more linear rate.

Inevitably, the software becomes the most valuable and important part of the product, service or activity.

And this has some profound consequences on the way businesses define their IP strategy.

Why is this relevant to IP strategies?

There are two reasons why the viral effect of software is very relevant to all IP strategies.

The first reason is related to the business models that apply to software. Software is brought to market through business models that are different from those used for hardware or services. One of the important differences is that software is not sold, but licensed. While the license can be bundled with other aspects of business, such as services (maintenance, support, implementation, etc), and those services will often play an essential part in building the business, the license is always a core part of any software business model.

And the great advantage of licenses is their flexibility and versatility. Software licenses range from extremely closed to extremely open. Rights of licensees can be very wide, or very limited. There are relatively few legal limitations on how you can license software. And this, in turn, offers great potential to structure, adapt and modify business models in new and different ways.

In practice, it means that, as the relative importance of software in a business offering is growing, such a business acquires more flexibility to modify and fine-tune its business model and strategy.

The second reason is that software is one of the few technologies where both patents and copyrights apply. Copyright applies to the code in which software is written. But copyright only protects against copying the particular code of a piece of software, it offers no protection to the functionality expressed through that code.

On the other hand, it is possible to patent certain functionalities of software. Even though the conditions of patentability vary between the major jurisdictions, the principle remains the same: patents will apply to a function of the software, regardless of the code that expresses that function.

This means that the viral effect of software, once it has "contaminated" a business, and software becomes an important part of the value proposition of such business, has as a practical effect that it will add complexity and variability to IP strategies, because more IP rights will apply to a much wider range of possible business models.

IP rights actually don't fit very well with software

But there's more.

When we look at how software businesses deal with IP rights, we notice that, until relatively recently, "technical" IP rights, by which I mean patents and copyrights (but not trademarks), did not have a very strong influence on either technological development or business models around software.

There is in reality very little software that gets patented, and, while copyright is a key element in determining the licenses under which software is sold, there is actually very little use of copyright in its "classical" way, which is to prevent competitors from using your copyright.

It is only since software has invaded the market of mobile telephones that we start to see a lot of patent litigation and enforcement around this technology – and this raised awareness of IP is related to the technical interaction between the software and the hardware, rather than the software itself.

The reason why IP rights are in general weak in software is related to the specific characteristics of software, which operates at three levels – and IP rights don't deal with those levels in the same way.

The three levels at which software operates are technology, functionality, and content.

Technology is the level where we may find patents: technology is the underlying core of software, and the level at which software interacts with hardware. But, as said, while some aspects of this level are patentable, and do get patented, a lot of innovation of software at this level does not benefit from a strong protection IP strategy. This relates e.g. to software languages, middleware, operating systems and similar technologies.

The reason why IP rights don't work very well at this level is because their success is dependent on their open character. Think of the original story of Microsoft, who beat Apple back in the 80s and 90s, because Microsoft's technical standards were open, and anyone could (and did) program for Windows, whereas Apple kept everything closed and was almost pushed into irrelevance.

This story is repeated in the success of the Apple App store in the beginning of the 21st century: only because the development kit is effectively completely open, was Apple able to get developers to bring out those millions of Apps with their billions of downloads. In other words, the more you close the system (for which you could potentially use patents), the less success you will have in the market. At the level of functionality, the story is worse. Not only is it much harder to patent "pure" software functionality, it is also much more useless. This is caused by the relative flexibility and ease with which such functionality can be created – the arms race is heavily tilted against patenting functionality. And

copyright, as we know, does not protect functionality. Finally, as far as content is concerned, while copyright applies, it will not come as a great shock to hear that Information Technology enables free copying, from a technical perspective, much easier than its opposite, the rather ineffectual DRM or digital rights management. This is, in turn, re-inforced by the advent of user generated content, a tendency that blurs the line between function and content, and that turns every consumer of content into a producer of more, derivative content. This is a phenomenon that current IP rights have no valid answer to – and so they risk being ignored, which is exactly what we start to see with phenomena like Pinterest, but even Twitter and Facebook. Moreover, the speed of innovation in software is staggering. 50% of all software used today is less than three years old. That means that the turnover rate of technology is so fast, that the classical approach of IP rights, aimed at recovering over longer periods of time the initial investment in technology, has not sufficient time to take root. So we see how "classical" IP rights are significantly weaker and less relevant in the software world, because of the characteristics of software. And that's not all.

The shock of Open Source

Open Source uses IP rights, for a purpose that aims specifically at preventing IP rights to apply. The copyleft, viral, licenses such as the GPL (the GNU General Public License), effectively prevent the normal operation of IP rights, where an exclusive right holder will be enabled to enforce the protections offered by IP rights to demand a premium or rent for the right to use the technology developed. This is done through enforcement of the copyright license, which obliges the licensee to respect the four freedoms of Open Source, which include the freedom to run on any technology, and modify the software – approaches that are anathema to classic IP strategies. And Open Source is no longer a marginal phenomenon, it is quickly becoming mainstream. Current estimates are that more than one third of all code written in 2011 was written in Open Source code. Open Source proponents claim that 75% of all enterprise software contains Open Source elements, and predict that this number will rise to 99% by 2016. In most markets where Open Source enters and acquires critical mass, proprietary software providers tend to get pushed out of the market, or become marginal players themselves, surviving only through a focus on niche markets or niche functionality. This is caused by the fact that most users, and certainly B2B users, find that Open Source software tends to be better, more innovative, more secure and more stable than their rival proprietary products. Time-to-market is significantly faster for Open Source software, step-in costs are lower, and vendor lock-in issues are much easier to handle. Moreover, any industry dealing with open standards will have a tendency to go to Open Source. It is no coincidence e.g. that, as the car manufacturing industry wants to continue to cut costs and ensure interoperability between its different providers, OEM or otherwise, up the value chain, it is moving into the Open Source direction. This will have an important impact on how IP rights are used. To put it as a caricature: if everything becomes software, and all software becomes Open Source, are IP rights doomed?

The increased relevance of IP strategies

I don't think IP rights are doomed. What will have to change, though is how we use IP rights, and how we define what an IP strategy is. Historically, an IP strategy is about protecting investment in innovation

and technology. With the advent of software, and the rising importance of Open Source, that will have to change in a number of ways. The first change is that the question on use of IP rights in the business model will become more complex and more sophisticated, both in terms of more IP rights that apply, and a much wider variety of business models available. The second, and most fundamental, change is how IP rights will be used. IP rights will no longer be used to simply "protect" innovation, they will become an essential tool that determines how innovation is brought to the market. Just like Open Source uses copyright (an IP right) to enforce its anti-IP philosophy, so will any business and IP strategy have to look at the way it can use IP rights as an essential part of the structure of the business model, supporting the ultimate goals of the business. Another important consequence will be the relative decline of the importance of "technical" IP rights, such as patents and copyrights, versus the growing importance of trademarks, designs and logos. These are IP rights that are not based on technical or creative innovation, but on identifying and distinguishing a product or service from its competitors. As the protective aspect of technical IP rights becomes less relevant, the importance of identity IP rights, and branding in general, will increase. This is because businesses will coalesce their technical skills around the value of their brand and trademarks, rather than through the possibility to block technical copying by competitors. A good example of this trend is Red Hat, the first $1 billion Open Source provider. Their license to Linux or other Open Source products is based on a combination of services, specific customization, technical support and the use of the Red Hat logo and brand. For a lot of Red Hat products, the source code is available but you have to invest time and money to get it, and potentially approve it. Why not spend that money on the reassurance of a skilled provider who will help you solve your problems? After all, for a lot of products, customers find that the question "does it work" matters a lot more than "who owns the IP"? Other IP rights may struggle. It seems difficult to see how Trade Secrets can remain very relevant when the amount of data produced by humanity (including its computers) continues to explode at a rate of a 100% increase every 18 months, and where every second year can claim to have produced more data than in the entire history of mankind until the end of the previous year. The problem is not so much that we will forget how important Trade Secrets are, it is just that the relative cost of keeping something secret will become prohibitive when all the other information drops 50% in cost every 18 months. It is another example of the immense creative destruction power of the combined exponential increases in computing power, communication capability and data storage. What that means is that IP strategies will no longer be able to focus simply on the "protection" side of IP rights, but will have to work with the structural, constructive side of IP rights, enabling businesses to better understand what their unique value-add is, and then structure IP rights around that value-add, and bringing it to the market in the most efficient way for that business. And the balance between those different IP rights will become, even more than today, a key consideration in any business strategy. In other words, IP strategies become, much more than today, a key part of the heart of the business model itself.

Joren De Wachter is an experienced IP strategist, with a focus on ICT technology businesses. He can be reached atinfo@jorendewachter.com.

Religious Organization's Trade Secret Misappropriation Claim Against Anonymous Blogger Survives Anti-SLAPP Motion to Strike In California Federal Court

By Robert Milligan and Joshua Salinas (September 9, 2012)

Balancing the rights of businesses to protect their economic interests with the rights of individuals to freely express themselves can be a complicated act requiring nuanced application of the law; even more so when the business is of a religious nature. In a fascinating case out of California, Judge Lucy H. Koh of the United States District Court for the Northern District of California, weighed the merits of a trade secret misappropriation claim made by a religious organization against the merits of two anonymous bloggers' claims under the first amendment.

The case, *Art of Living Foundation v. Does 1-10*, 2012 WL 1565281 (N.D. Cal, May 1, 2012), involves two alleged former adherents to the religious and spiritual teachings of the plaintiff who have allegedly since become outspoken critics of the organization. They allegedly went so far as to label the group as a "cult and a sham" and allegedly post the group's proprietary materials on the Internet. Judge Koh ultimately granted an anti-SLAPP motion for one of the defendant anonymous bloggers, but denied the motion pertaining to the blogger that had allegedly admitted to disclosing and posting AOLF's alleged trade secret materials on the internet.

The Art of Living Foundation ("AOLF") is the United States branch of the international Art of Living Foundation based in Bangalore, India, and is a California corporation. Founded in 1981 by Sri Sri Ravi Shankar ("Shankar"), the group boasts chapters in over 140 countries and touts itself as "an international nonprofit educational and humanitarian organization. " AOLF is "dedicated to teaching the wellness and spiritual lessons of Shankar" by offering courses on meditation, yoga, and specialty rhythmic breathing techniques.

The two Doe Defendants, allegedly known pseudonymously by their blog names "Skywalker" and "Klim," are alleged former AOLF teachers who have been critical of AOLF's treatment of members, financial management, and the effects of AOLF teachings on its participants. Both Skywalker and Klim allegedly created their own individual blogs to provide a critical perspective on AOLF and Shankar.

On June 1, 2010, Skywalker allegedly began posting AOLF materials on his blog. These materials allegedly included notes about AOLF's proprietary breathing techniques, training methods, and audio recordings of meditation chants. Around August 25, 2010, an India-based charity founded by Shankar sent a takedown notice to Wordpress - the host of Skywalker's blog –under the Digital Millennium

Copyright Act. Wordpress notified Skywalker of the takedown notice, who shortly thereafter removed AOLF's materials from his blog. The court noted that AOLF itself did not discover that its materials had been posted on Skywalker's blog until late August 2010, after Skywalker had already removed the materials pursuant to the aforementioned takedown notice.

AOLF subsequently brought action against Skywalker and Klim for, inter alia, trade secret misappropriation. Skywalker and Klim moved to strike the trade secret misappropriation claim under California's anti-SLAPP statute (Cal. Civ. Code Proc. § 425.16). The anti-SLAPP statute protects individuals from litigation that is strategically brought to discourage public participation or punish the exercise of one's constitutional right to free speech.

To be successful, a special motion to strike brought under California's anti-SLAPP statute must pass muster under a two-step analysis: (1) the defendant must show that the plaintiff's reason for bringing suit "arises from an act by the defendant in furtherance of the defendant's right of petition or free speech in connection with a public issue," and (2) the plaintiff must then establish a probability that the claim will prevail. Determining that Skywalker's publication of the documents in question was a public issue directly connected to his criticisms of AOLF, the court found that the Defendants had made a prima facie showing that AOLF's suit arose from a protected act.

The burden then shifted to AOLF to show a "probability of prevailing" on its trade secret misappropriation claim. The court noted, however, that this showing involves a relatively low threshold for proving a triable claim. (See *Mindy's Cosmetics, Inc. v. Dakar*, 611 F.3d 590 (9th Cir. 2010)). Skywalker and Klim contended that AOLF could not meet its burden because the information and techniques related to breathing techniques and other kinds of meditation information posted online were public knowledge, and thus, not trade secrets. Meanwhile, AOLF argued - and the court agreed - that the training guides contain additional unique information related to teaching methods and instruction that were not public knowledge, and could qualify as a trade secret.

To further meet the "minimal merit" of a trade secret claim necessary to overcome the anti-SLAPP motion, AOLF had to make a showing that the information contained in the allegedly protected documents is "sufficiently valuable and secret to afford an actual or potential economic advantage over others" and that it had made a reasonable effort to keep the information secret. Financial reports submitted by Plaintiff showing that it generated revenue from the courses and lessons contained in the confidential teaching manuals were enough to convince the court that the documents had significant economic value. In declarations submitted to the court, AOLF stated that it keeps these documents on password-protected computers in password protected files, and that it requires both instructors as well as students to sign non-disclosure agreements upon enrollment.

Defendants argued that the non-disclosure agreement at the bottom of AOLF's course registration forms was not sufficiently conspicuous, and that Plaintiff had failed to produce evidence of similar non-disclosure agreements by the other 140 AOLF chapters around the world. The court found, however, that "[j]ust because there is something else that [Plaintiff] could have done does not mean that [its] efforts were unreasonable under the circumstances." See *Id*. at 33 (citing *Hertz v. Luzenac Grp.,* 576

F.3d 1103, 1112-13 (10th Cir. 2009)). The court found that the UTSA requires "reasonable efforts" to protect a secret, not maximum security. The court reasoned only "in an extreme case can what is a reasonable precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits" in a particular commercial context, which involves issues of fact. See id. at 34 (citing *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.,* 925 F.2d 174, 179 (7th Cir. 1991). Given the evidence of a reasonable effort by Plaintiff to keep the information contained in the teaching manuals secret, in addition to the novel information contained therein, Judge Koh found that AOLF had met the minimal standard of maintaining its trade secret claim.

In further defense of their anti-SLAPP motion, Skywalker and Kilm argued that the case should be thrown out due to "excessive entanglement with free exercise" as well as for a lack of misappropriation. The excessive entanglement defense argues that deciding a case of this nature would force the courts to rule on religious doctrine, thereby violating the separation of church and state. Citing *Religious Tech. Ctr. v. Netcom On–Line Cmty. Servs.,* 923 F.Supp. 1231 (N.D.Cal. 1995), Judge Koh disregarded this argument, noting that "there is no authority for excluding any type of information [from trade secret protection] because of its nature alone." In particular, Judge Koh explained that, "it is possible for the Court to adjudicate Plaintiff's trade secret claim by resort to neutral principles of trade secret law and without excessive entanglement in matters of religious doctrine or practice."

As for the lack of misappropriation argument, Judge Koh was inclined to agree that in the case of Klim, there was no evidence to support a finding of misappropriation. However, given Skywalker's admission that he had in fact posted the teaching manuals on his blog, the same could not be said for him. As a result, the court granted in part the anti-SLAPP motion as to Klim, but denied in part the motion as to Skywalker.

On June 12, 2012, the parties held a Settlement Conference and a settlement was reportedly reached. (See settlement details and other information about the case at Citizen Media Law Project's website). Pursuant to the settlement agreement, Skywalker and Klim published a joint statement informing its blog readers about the settlement and that their blogs would be frozen on June 19, 2012. They noted in their statement that there are no restrictions on the Does to create new blogs, and that no identity had or would be disclosed in relation to this litigation and settlement. In return, AOLF agreed to drop the lawsuit with prejudice and to pay Skywalker and Klim's attorney's fees.

No matter the type of business or service offered, it is in the interest of all businesses to vigorously defend their trade secrets by taking the necessary precautionary measures. For example, the fact that AOLF required all participants – both students and teachers – to sign non-disclosure agreements was key evidence to demonstrate AOLF's "reasonable efforts" to protect its trade secrets and ultimately defeat Skywalker's anti-SLAPP motion.

This case also reaffirms that information that may be related to religion can be protected as a trade secret. The court recognized that a defendant cannot simply deprive a plaintiff's information trade secret protection simply by invoking the Free Exercise Clause. Indeed, this would raise other problems

other the Free Exercise Clause by depriving religious organizations of protections of civil law that are available to others.

Finally, this case illustrates that information disclosed publicly online for a short period may not necessarily lose its trade secret status. The court did not seem overly concerned that AOLF's materials had been posted online for several months and viewed by several hundred members of the public before Skywalker received a takedown notice and removed the materials. It is evident though that companies must move promptly to have any protected information removed from the Internet once they become aware of it should they want to protect its trade secret status and pursue available remedies against those who have improperly posted it.

Despite Allegations That Something Fishy Was Occurring, Kentucky Federal District Court Rules That Texas Corporate Defendant Was Not Subject To Personal Jurisdiction In Trade Secret Misappropriation Suit

By Paul E. Freehling (September 21, 2012)

MPI, a Texas company, went to Kentucky and allegedly attempted to hire two Luvata employees, Foster and Meredith. Foster joined MPI soon thereafter. Over the course of the next few months while Meredith remained a Luvata employee, he and Foster allegedly spoke by phone repeatedly. In addition, prior to leaving Luvata for MPI, Meredith allegedly copied his employer's computer files that described a trade secret manufacturing process, identified its customers, and contained its financial information. Once Meredith became an MPI employee, it allegedly replicated Luvata's confidential manufacturing process and began competing with Luvata which then sued MPI, Foster and Meredith in a Kentucky federal court.

MPI's motion to dismiss for lack of personal jurisdiction, on the ground that the Kentucky long-arm statute does not permit the exercise of jurisdiction over MPI and a related defendant company, was granted. The ex-employees' Rule 12(b)(6) motion to dismiss the misappropriation claim against them was denied. *Luvata Electrofin, Inc. v. Metal Processing Int'l, L.P.*, Case No. 11-CV-00398 (W.D. Ky., Sept. 10, 2012).

Luvata is in the business of electrocoating ("e-coating") coils used in the heat transfer industry. Luvata maintained that its e-coating process is unique, is a trade secret, and cannot be reverse engineered. Foster was allegedly the company's production supervisor, and Meredith was "intimately involved in running the" e-coating process. All Luvata employees signed non-disclosure agreements (but there was no non-compete provision).

At an e-coating conference held in Kentucky, MPI endeavored to hire both Foster and Meredith. After both initially declined, Foster left Luvata and went to work for MPI. Over the course of the next few months, he allegedly spoke to Meredith by phone more than 30 times, and at least twice Meredith reviewed Foster's computer files at Luvata which contained trade secrets. In addition, Meredith allegedly copied onto his own CD and thumb drives files from his and Foster's computers. On his last day at Luvata before joining MPI, Meredith allegedly used a program that "cleaned 'unnecessary files"' from his and Foster's computers. Foster allegedly told Luvata's general manager that MPI was building

an e-coating line, based on information Foster learned at Luvata, and that MPI soon would be competing with Luvata. MPI allegedly proceeded to reproduce Luvata's secret e-coating process and began soliciting Luvata's customers, and Luvata sued.

MPI's motion to dismiss Luvata's complaint for lack of personal jurisdiction was granted because, according to the court, MPI did not engage in acts in Kentucky that bore a "reasonable and direct nexus" to Luvata's allegations of misappropriation of trade secrets. The court conceded the possibility "that something fishy was occurring" between MPI and Meredith but added that was only conjecture since Meredith may have been acting unilaterally to increase his value to his new employer. However, the court found sufficient to state a cause of action Luvata's claim that Foster and Meredith violated their non-disclosure agreement with Luvata by disclosing its trade secrets to MPI. Luvata's breach of fiduciary duty claim against its two ex-employees was dismissed as preempted by the Kentucky Uniform Trade Secrets Act.

Under the circumstances of this case, and particularly in light of the court's decision denying the ex-employees' Rule 12(b)(6) motion, the order dismissing Luvata's lawsuit against MPI could be described as harsh, especially without giving Luvata an opportunity to take discovery. The suggestion that Meredith might have been acting on his own seems far-fetched but possible. Moreover, it is surprising that Luvata's allegations held to be conjectural in connection with granting MPI's motion to dismiss were found "to plausibly give rise to an entitlement to relief" as against the individuals. Of course, Luvata might have had an airtight action against them if they had signed non-competition agreements. Please see our recent post regarding a Kentucky appellate case containing an overview regarding enforcing non-competes in Kentucky.

If Confidential Information Constituted A Trade Secret On The Date It Was Misappropriated, The Misappropriation Is Actionable

By Paul E. Freehling (October 4, 2012)

A district court for the Eastern District of Wisconsin recently held that even though misappropriated information no longer was a trade secret on the date the wrongdoer was sued, a misappropriation lawsuit may be maintained if the information qualified as a trade secret on the date of the wrongdoing. *Encap, LLC v. The Scotts Co., LLC,* Case No. 11-C-685 (E.D. Wis., Sept. 14, 2012).

The case involved a dispute between two companies in the lawn and garden industry. Plaintiff Encap has invented many novel platform technologies in the seed, mulch, and fertilizer industries. Defendant The Scotts Company is well known for its Miracle-Gro, EZ Seed, and Turf Builder Grass Seed products.

In early 2002, Scotts personnel allegedly had several introductory confidential communications with persons at Encap inquiring about Encap's platform technologies. In particular, Scotts was allegedly interested in how Encap's encapsulated seed technology absorbed water. Scotts allegedly requested cases of Encap's new seeds for testing purposes.

In June of 2002, Encap allegedly sent Scotts a confidential memorandum, which allegedly contained certain Encap trade secrets. For example, the memorandum contained information about encapsulating seeds to aid in water absorption, using the color of mulch as a watering indicator, and developing a business strategic business plan to exploit these new technologies. The memorandum, however, provided that Scotts agreed to keep the document confidential and not use or disclose the data within. A dispute arose when Scotts allegedly used Encap's confidential information from the memorandum without authorization to make similar competitive products and derive substantial profits.

Encap subsequently sued Scotts for patent infringement and trade secret misappropriation.

Encap later brought a motion to dismiss Encap's trade secret missapropration claim for failure to state a cause of action. Shortly before Scotts' motion, Encap requested leave of court to file its 2002 confidential memorandum under seal.

The court entered an order rejecting Encap's request on the ground that the memorandum was "ten years old and does not contain any apparent trade secrets or underlying data, such as chemical formulas or manufacturing processes." Scotts' motion to dismiss the claim of misappropriation was

based on the absence of a trade secret, as seemingly determined by that order. However, the court reasoned that the decision with respect to filing the memorandum under seal "does not mean that some of the information [in the memorandum] was not a trade secret in 2002 and thereafter when Scotts is alleged to have misappropriated," and to have used, the information for its own advantage. So, the motion to dismiss was denied.

This decision teaches that, at least in Wisconsin, just because information no longer is confidential at the time a misappropriation case is filed, a cause of action can be stated if (a) the information constituted a trade secret when the misconduct occurred, and (b) damages resulted. So, whenever trade secrets are disclosed pursuant to a confidentiality agreement, the party making the disclosure should remain alert for a considerable period to the possibility that the agreement was violated.

The Trade Secret Is In the Swirl Cupcake: Bakery Sues To Protect Its Signature Icing Topping

By James Yu (October 5, 2012)

Apparently it's not just the sweet, delicious taste of Magnolia Bakery cupcakes that had people lining up in droves for a box or three since it opened its first store in Greenwich Village, New York over 15 years ago.

According to a Complaint filed on September 20, 2012 by Magnolia, entitled *Magnolia Intellectual Property, LLC v. Buba Trawally, et al.,* Civ. A. No. 12-7102, in the U.S. District Court for the Southern District of New York, the cupcakes are also distinguishable and highly valued because of their "unique, distinctive, and immediately recognizable look – the 'Magnolia Signature Swirl' icing topping." Magnolia maintains as trade secrets its cupcake recipes, including the Signature Swirl, which it claims has become well recognized and associated with the Magnolia name. According to articles attached as exhibits to the Complaint, it takes anywhere from 8 to 40 hours of training to perfect the Signature Swirl. It should come as no surprise, therefore, that the company requires each of its bakers to sign confidentiality agreements to protect its trade secrets, as well as other proprietary and confidential information.

The Complaint alleges that one of Magnolia's former bakers, while still employed with Magnolia, started a company called Apple Café Bakery Corporation, then opened up a competing retail bakery shop in Greenwich Village shortly after he left Magnolia's employ. According to the Complaint, Apple Cafe Bakery created "Knock-Off Cupcakes" with the same swirled icing topping "in an attempt to capitalize upon Magnolia's unique and distinctive Magnolia Signature Swirl Trade Dress." The Complaint also accuses the defendants of misappropriating Magnolia's cupcake recipes. The Complaint asserts a total of eight causes of action, including federal and state statutory trade dress infringement, trade dress dilution, breach of contract, trade secret misappropriation, unfair competition, and tortious interference. Defendants have not yet responded to the Complaint.

While the Complaint seeks permanent injunctive relief, in addition to monetary damages, no motion for a preliminary injunction has been filed by the Plaintiff yet. This action may be an investment by Magnolia to further protect its trade secrets and to serve as a warning to other bakers and competitors that Magnolia will aggressively enforce its confidentiality agreements and protect its business interests through litigation. An important lesson that many companies learn after the fact is that a failure to take any legal action against misappropriation or unfair competition could arguably be construed as either an unintended waiver of a trade secret or embolden other employees to ignore their confidentiality or non-compete agreements.

From a legal standpoint, it remains to be seen whether and to what extent Magnolia's signature icing swirl is a protectable interest or sufficiently distinctive and famous in its look to entitle Magnolia to injunctive relief against any trade dress infringement or dilution arising from a competitor's alleged use of the same or similar topping. Magnolia has indeed brought suit against another alleged competitor in the past for infringing on the Magnolia mark (see *Magnolia Operating, LLC v. Jennifer C. Appel,* No. 10-cv-9312 (S.D.N.Y.)), but that case appears to have settled shortly after it was filed. We will keep you posted on this tasty new case.

Florida Court Rejects Argument That Plaintiff Must Make "Threshold Finding" of Trade Secret Before Proceeding With Discovery

By Joshua Salinas and Jessica Mendelson (October 10, 2012)

A Florida District Court of Appeal recently confirmed that plaintiffs in trade secret misappropriation cases must identify their trade secrets with reasonably particularity before conducting discovery. *AAR Mfg., Inc. v. Matrix Composites, Inc.,* No. 5D11–3802, 2012 WL 3870419 (Fla.App. 5 Dist., 2012). The Court of Appeal, however, rejected the notion that, as a threshold matter, the plaintiff was also required to prove the existence of its trade secrets.

Plaintiff Matrix Composites, Inc., manufactures and designs carbon fiber composites for the aviation, medical, and space industries. For example, these critical composite structures are used in F22 fighter jets and are extremely useful for stealth and weight reduction. (Also check out this great video from Matrix's website about the use of composites in fighter jets).

The case arose when Matrix sued a competitor, AAR Manufacturing, in Florida state court alleging misappropriation of trade secrets pertaining to various product molding processes.

During discovery, Matrix requested certain documents from AAR pertaining to AAR's trade secrets. AAR filed a motion for a protective order to prevent the discovery of its own trade secrets on grounds that discovery could not continue until Matrix first identified its own trade secrets with reasonable particularity. The trial court denied AAR's motion for the protective order, finding Matrix had identified its own trade secrets with reasonable particularity. Accordingly, the trial court ordered AAR to produce the requested discovery documents to Matrix within sixty days.

AAR petitioned the District Court of Appeal of Florida, Fifth Circuit for relief from the order denying its motion for the protective order. In particular, AAR argued that the trial court failed to make a "threshold finding" that Matrix's allegedly misappropriated trade secrets actually existed before ordering AAR to disclose its own trade secrets.

The Court of Appeal denied AAR's petition in part. The court recognized that, in trade secret misappropriation cases, a plaintiff is required to identify its trade secrets with reasonable particularly before proceeding with discovery. (See *Del Monte Fresh Produce Co. v. Dole Food Co.,* 148 F.Supp.2d 1322 (SD. Fla. 2001).

The Court of Appeal, however, rejected the notion that the trial court was required to make a "threshold finding" regarding the existence of trade secrets in misappropriation. Specifically, the Court of Appeal rejected any "threshold finding" requirement that may derived from the recent *Revello* case. (See *Revello Medical Management, Inc. v. Med-Data Infotech USA, Inc.* 50 S.3d 678, 679 Fla. 2d DCA 2010) (stating that prior to proceeding with discovery in trade secret cases, "[t]he plaintiff must, as a threshold matter, establish that the trade secret exists").

This case is significant because the Florida Court of Appeal has set the record straight with respect to the pre-discovery requirements for trade secrets misappropriation cases. Florida does not have a pre-discovery trade secret identification statute (see e.g. California Code of Civil Procedure § 2019.210), but this procedure is well established through Florida case law. It appears that the 2010 *Revello* case overly expanded these pre-discovery requirements to add a threshold finding that trade secrets exist. The Court of Appeal used the instant decision to eliminate any further confusion regarding pre-discovery trade secret identification.

Trade Secret Lawsuit Filed Against Heavy Metal Band Regarding "Drum Set Loop Coaster"

ByJoshua Salinas (October 17, 2012)

On September 20, 2012, a trade secret misappropriation lawsuit was filed against rock star drummer Tommy Lee and his band Motley CrUe in Los Angeles Superior Court.

Plaintiff Howard Scott King alleges in his complaint that in 1991 he developed an idea and concept for a "Tommy Lee Loop Coaster." The concept consists of a platform on wheels that follows a loop-shaped track. A drum set is attached to the wheeled platform and follows the track in a complete loop, allowing the drummer to play the drums upside down. Other drummers in rock bands have used similar stunts at live shows for many years. Media outlets have previously reported on the dispute and the parties' contentions.

King alleged that he disclosed the idea to Lee and Lee's band in 1991, and subsequently received signed confidentiality agreements (which have been misplaced or lost) from Lee's agents. King also alleged that he has since maintained the secrecy of his idea and only disclosed the idea as necessary to implement it.

King allegedly brought action against Lee and Motley Crue after he discovered that they were allegedly using his alleged drum set loop coaster idea for a worldwide concert tour in 2011. King alleges that the defendants disclosed the purported trade secret to another company, which made a similar loop coaster for use by the defendants at the concerts. He alleges that the idea is the centerpiece of many performances and was used in commercials and promotions for the band.

King alleges that he has suffered damages in excess of $400,000. King has asserted claims for trade secret misappropriation, unfair competition, and breach of promise.

It will be interesting to see how the court deals with the absent confidentiality agreements, especially since the parties may have difficulty remembering the exact terms and provisions of any purported confidentiality obligations.

Additionally, while this case is still in its infancy, the plaintiff will likely have a very difficult time establishing that his alleged idea qualifies as a trade secret under California law, particularly demonstrating that the information provided derives independent economic value from not being generally known to others or to others who can obtain economic value from its secrecy and is subject of efforts that are reasonable to protect its secrecy.

While a separate idea theft claim may still be actionable under California law, to pursue such a claim, the plaintiff will need to demonstrate that the defendants voluntarily accepted the disclosure knowing the conditions on which it was tendered and that the defendants used his work. Defendants may also challenge the claim on the grounds of independent development, which constitutes a complete defense.

A response is not yet due to the complaint and defendants have yet to file their response. We will keep you posted on this entertaining case.

Sports Agent Non-Compete and Trade Secrets Dispute Heats Up in California

By Robert Milligan and Jessica Mendelson (October 19, 2012)

With the NBA basketball season almost upon us, a high profile legal battle between an aspiring NBA sports agent and his former agency continues to heat up in Los Angeles federal court. The case involves some interesting non-compete, trade secret, and privacy issues.

In April 2012, we first alerted you to the colorful case of *Mintz v. Mark Bartelstein & Associates d/b/a Priority Sports & Entertainment,* Case No. 12-02554 SVW (SSX), (C.D. Cal.), where Aaron Mintz, a National Basketball Players Association (NBPA) certified player-agent, brought a declaratory relief suit seeking to invalidate his non-compete agreement with his former employer, Priority Sports & Entertainment ("Priority").

Mintz, based in Los Angeles, left Priority in March 2012, accepted a position with competitor Creative Artists Agency ("CAA"), and immediately sought declaratory relief to invalidate his two year non-compete agreement.

As the case has progressed, Mintz has added additional claims against Priority for violations of the Computer Fraud and Abuse Act, the Electronic Communications Act, and California Penal Code section 502, as well as claims for defamation, invasion of privacy, intentional inference with contractual relations, and violation of Business and Professions Code section 17200. Mintz has also asserted some of the claims against Priority principle Mark Bartelstein.

Mintz alleges that he worked eleven years for Priority and then decided to pursue a better opportunity with CAA. Apart from the two year non-compete, which he claims violates Business and Professions Code section 16600, Mintz claims that the fourteen-day notice of termination provision in his employment agreement violates section 16600 as well. Mintz claims that the notice provision restricts his ability to terminate his employment, and thereby prevents him from competing with Priority, at its discretion, for two weeks after termination in violation of California law.

The non-compete contains an Illinois choice of law provision but no separate action to attempt to enforce it has been initiated in Illinois to date.

Mintz also claims that after he resigned Priority hacked his personal email account, reviewed his contract with CAA, and disclosed its terms to third parties. He also claims that defamatory statements were made to basketball executives, players, and family members of players to persuade players not to

follow Mintz to CAA. Among some of the NBA players on the parties' joint witness list are Dominic McGuire, Jordan Crawford, Paul George, Danny Granger, and Acie Law.

Priority counterclaimed against Mintz asserting claims for breach of contract, breach of covenant of good faith and fair dealing, breach of duty of loyalty, misappropriation of trade secrets, intentional interference with contractual relations, intentional interference with prospective economic advantage, conversion, violation of California Penal Code section 502, defamation, trade libel, conspiracy, and unfair competition. Priority has also asserted some of the claims against CAA.

Priority alleges that under his employment agreement Mintz was required to provide Priority fourteen days' notice prior to his termination. Instead, Priority alleges that Mintz immediately terminated his employment and filed suit against Priority depriving it of "its negotiated opportunity to communicate with its clients before Mintz's departure and to attempt to retain their business and manage an orderly transition process." Priority claims that Mintz formulated a strategy designed to keep Priority from learning of his plans to join CAA in order to give CAA an unfair advantage in its efforts to attract several of Priority's clients. Priority also alleges that Mintz disclosed information regarding Priority's contracts with its NBA clients and used confidential information to solicit Priority's clients. In essence, Priority claims that Mintz and CAA conspired to steal Priority's clients.

Mintz has brought a motion for summary judgment on his claims and Priority's claims, along with CAA. Priority brought a motion for partial summary judgment on its claims against Mintz for breach of contract and breach of duty loyalty. The summary judgment hearings are set for October 29, 2012 along with the pretrial conference. The trial is set for November 13, 2012 before the Honorable Stephen Wilson.

Mintz claims in his opposition papers, among other things, that Priority's duty of loyalty claim fails because California employees have every right to take preparatory steps to look for a new job and consult an attorney to protect one's legal rights without violating their duty of loyalty to their existing employer. He also claims that Priority's trade secret claim fails because, among other things, client names, contact information, contract terms and commission splits with third party handlers do not qualify for trade secret protection.

It will be interesting to see how the court addresses the notice of termination provision and section 16600 argument as some employers use notice provisions in their employment agreements, particularly with executives. Additionally, the court may provide some guidance on what trade secrets, if any, exist, in the context of a sports agent dispute, as well as what other information may be protectable under a contract theory.

One interesting discovery issue handled by Magistrate Judge Segal in the case involved Priority's attempt to obtain Mintz's phone records from a smart phone he used during his employment with Priority.

Priority subpoenaed Mintz's phone records from the cellular provider, seeking ten categories of documents, including dates, times, originating and receiving telephone numbers, as well as the text

messages from the cellular phone. In response, Mintz filed a motion to quash the subpoena, arguing that it was overbroad and sought confidential information. Priority argued the information was necessary to prove their counterclaims that Mintz had made false and defamatory statements regarding Priority and improperly solicited Priority's clients. Furthermore, Priority argued that Mintz lacked an expectation of privacy in the phone, since Priority argued it owned and paid for the telephone account. Additionally, Priority argued that by acknowledging an employee manual stating that "personal information on company telephones shall be the property of Priority Sports," Mintz waived any right to privacy he might have had.

Ultimately the court granted the motion to quash with respect to the content of the text messages, but denied the motion to quash with respect to the non-content information, which consisted of the dates, times, and telephone numbers for specific calls during a relevant period.

Under the Stored Communications Act ("SCA"), communication service providers are traditionally prohibited from divulging private communications to certain entities or individuals. The SCA does not contain an exception for civil discovery subpoenas. However, under the SCA, communication providers can divulge "non-content information to non-governmental entities." According to the court, the bulk of the information requested in the subpoena was subscriber information, rather than the content of the messages. Furthermore, the court reasoned that since Priority was not a government entity, the information was "not barred from disclosure" under the SCA.

With respect to the content of the text messages, the court granted the motion to quash. The court ruled, however, that while Priority could not obtain the messages directly from the provider, it could obtain the messages directly from Mintz pursuant to a document request under Federal Rule of Civil Procedure 34, subject to Mintz's privacy objections, which were not before the court. According to the court, the information was within "Mintz's control" and could be obtained by Mintz from the provider.

The court also addressed Mintz's privacy interest in the non-content information. Judge Segal reasoned that the phone started out as Mintz's personal phone, but eventually became his business phone. Since the phone was used for business purposes, the court reasoned that Mintz had a limited expectation of privacy in the non-content information, and a protective order could be used to guard against any unwarranted intrusion into his privacy. Please see Eric Goldman's blog for a more detailed discussion of Judge Segal's ruling and SCA developments.

For litigants in trade secret and non-compete cases, the ruling is important because it provides guidance concerning discovery directed to probing allegations of solicitation, trade secret misappropriation, and other business and privacy torts. It is also an important reminder for employers to have strong policies that provide for ownership interests in company smart phones as well as that permit employer monitoring of company owned devices. The court credited those facts in requiring the production.

We will continue to follow this case, and keep you apprised of future developments as it moves toward the November trial date.

Zynga Sues Former Employee For Trade Secret Theft While Defending Its Acquisition Of Other Alleged Proprietary Information

By Jason Stiehl (October 29, 2012)

On October 12, 2012, Zynga, a major provider of social game services based in San Francisco, filed suit against its former general manager of its highly successful CityVille game, Alan Patmore. Zynga alleges that Patmore, after allegedly refusing to acknowledge his confidentiality obligations, wandered out of the offices of Zynga with 760 computer files, which he uploaded to his personal Dropbox account. Adding fuel to the fire, Patmore then allegedly attempted to uninstall Dropbox from his computer, leaving forensic artifacts in his wake. Included in the allegedly copied files were:

- Data concerning the method by which Zynga identifies which games and game mechanics will be successful;
- Internal assessments of every game feature rolled out over the last quarter for CityVille;
- Internal assessments and lessons learned for Zynga's other hit games;
- The green-lit design document for an unreleased game in development; and
- Confidential revenue information.

In addition to the various files, Zynga alleges Patmore also copied his entire email box, containing fourteen months of confidential communications.

Published reports indicate that Patmore is joining Zynga rival Kixeye.

Although there are many things notable about this lawsuit (including the decision by Zynga not to bring a CFAA claim following the recent 9th Circuit decision in *United States v. Nosal*), perhaps the most interesting aspect of this case is an element often over-looked in trade secret cases: proving Zynga actually has a proprietary interest in the information removed.

As some readers may recall, we blogged on the litigation between Zynga and its competitor, SocialApps, LLC ("SA"), wherein SA alleged that Zynga had stolen the source code for FarmVille during due diligence of its company. There, the court held that while certain images and features were available in the public domain, issues remained as to whether Zynga had improperly accessed and used SA's proprietary source code.

Complicating this further, Zynga is enmeshed in litigation with EA Sports, who, in August, sued Zynga for copyright infringement, claiming it improperly utilized copyrighted material from EA's "The Sims Social," which EA claims Zynga learned through its recent hire of key EA employees. Last month, Zynga countersued, alleging that EA had engaged in improper anti-competitive behavior by attempting to induce Zynga to enter into a no-hire agreement. In response, EA's spokesman alleged that Zynga had engaged in a persistent plagiarism of other artists and studios.

In the end, Zynga may resolve this matter with Patmore without ever having to provide its proof to a jury (although based upon Kixeye's recruiting video, it appears that Kixeye may put up a fight). This new case does, however, present a strong illustration of some of the underlying decisions a company has to consider before bringing trade secret litigation against a former employee who may know a company's most internal secrets.

Royalties Awarded for Theft of Skycam Trade Secrets

By Joshua Salinas and Jessica Mendelson (October 30, 2012)

Think that patents, trademarks, and copyrights are the only intellectual property where reasonable royalties are available? Think again! On September 27, 2012, a district court for the Northern District of Oklahoma found "exceptional circumstances" existed to award a royalty injunction for the misappropriation of trade secrets. *Skycam, LLC v. Bennett*, No. 09-CV-294-GKF-FHM, 2012 WL 4483610 (N.D.Okla. Sept. 27, 2012).

Background Facts and Procedural History

The case involves two competitors in the aerial camera industry, Skycam and Actioncam. Both companies manufacture aerial camera systems used for sporting event broadcasts. The cameras are suspended by a set of cables over the playing field and maneuvered to provide a unique above-action perspective during live sporting events. Many viewers who watch football games or soccer matches are familiar with these "flying" robotic-like cameras. Videos of these aerial cameras in action can be seen here.

A dispute arose when Skycam's Chief Engineer, Patrick Bennett, allegedly left to join a competitor, Actioncam. Bennet was responsible for the research and development of Skycam's aerial camera systems and allegedly had full access to Skycam's engineering and design documents. Skycam alleged that Actioncam developed a competitive aerial camera system under the guidance of Bennett and through the use of Skycam's trade secrets.

Skycam sued Bennett, alleging he had breached a non-disclosure agreement, misappropriated trade secrets, and engaged in unfair competition. The trade secrets allegedly misappropriated included the use of lasers and reflectors for aerial survey, site surveys and field guides, management techniques, obstacle avoidance systems, as well as numerous other Skycam systems.

In September 2011, a jury found in favor of Skycam on the breach of contract, misappropriation of trade secret, and unfair competition claims, and awarded damages to Skycam. Skycam subsequently filed a motion for permanent injunction on the misappropriation of trade secrets and unfair competition causes of action. Skycam sought a prohibitory injunction that would prohibit Actioncam from utilizing Skycam's trade secrets and from placing false and/or misleading advertisements and representations about Actioncam's systems. Skycam also requested, in the alternative, reasonable royalties under the Oklahoma Uniform Trade Secrets Act ("OUTSA") should the court find "exceptional circumstances" existed regarding Actioncam's future or potential use of Skycam's trade secrets.

Trade Secret Misappropriation Claim

With respect to the trade secret misappropriation claim, rather than granting the prohibitory injunction, the court held a royalty injunction was appropriate. The court found that granting an injunction would eliminate Actioncam's ability to use its aerial camera systems and essentially put Actioncam out of business. The court further reasoned that a prohibitory injunction would eliminate competition and technological innovation in the relatively small aerial camera market, and thus, would be harmful to the public interest. Thus, the court found the imposition of a royalty was adequate to protect the parties' interests, and the case presented "exceptional circumstances" that would permit such a remedy under the OUTSA.

On this basis, the court awarded damages based on royalties of $5,000 per event covered by Action-cam during the period of September 3, 2011, through February 28, 2013. This time period was based on Skycam's expert's testimony stating that it would take approximately three to four years for a camera system like Skycam's to be developed.

Unfair Competition Claim

The court granted the injunction for unfair competition, finding "the threatened injury outweighs the harm that the injunction may cause" and that an injunction would not "adversely affect the public interest" as required by Tenth Circuit law.

In the original jury verdict, five different types of false and misleading statements were alleged as the basis for the alleged violations of the Oklahoma Deceptive Trades and Practices Act and the Lanham Act: statements regarding (1) speed and accuracy, (2) field graphics for a "First and Ten line," (3) secondary supporting cable and power safety reels, (4) other capabilities of the Skycam system, and (5) other capabilities of the Actioncam system. The jury failed to specify which types of statements it found false and misleading, and the defendants argued that Skycam should not be entitled to an injunction prohibiting all five types of statements as a result. However, the court found otherwise, since, "where a verdict is general, a court must presume that any and all issues were decided in favor of the prevailing party."

Based on the jury verdict, the court found irreparable injury, and found the balance of hardships weighed more heavily in Skycam's favor. The court granted an injunction prohibiting false or misleading claims regarding any of the previously mentioned topics. Finally, the court also required Actioncam to place a corrective advertisement on any public advertising over the next six months.

Takeaways

This case reminds us that reasonable royalties are available under the UTSA for trade secret misappropriation. Although reasonably royalties were not available under the UTSA when the statute was originally drafted in 1979, its subsequent amendments have since allowed this remedy. States differ in the availability and application of reasonable royalties for trade secret misappropriation based on their implementation of the UTSA. California, however, has recently allowed this remedy regardless of whether actual damages are unprovable as a matter of fact or law. See *Ajaxo, Inc. v. E*Trade Financial Corp*., 187 Cal. App. 4th 1295 (2010).

Thus, trade secret holders should consider requesting reasonable royalties as an alternative to a permanent injunction when appropriate. While prohibitory injunctions are often preferred, this alternative remedy helps trade secret holders avoid leaving the court empty handed.

Mobile Game Rivals Clash In California Trade Secret and Unfair Competition Suit

By Jason Stiehl (November 14, 2012)

The litigation between Kixeye and Zynga, two rivals in the mobile gaming market, has heated up over the past week.

Last month, we wrote about the alleged removal of dozens of files and emails by former Zynga app-maker, Alan Patmore. Last Thursday, apparently based upon information learned in discovery, Zynga upped the stakes, naming Kixeye in the First Amended Complaint and seeking a temporary restraining order against Kixeye.

Yesterday, Kixeye fired back, bringing a cross complaint against Zynga for unfair competition, alleging that Zynga had filed the First Amended Complaint against Patmore and Kixeye only as a tool to stifle competition and gain access to Kixeye's trade secrets. Notably, Kixeye alleges in its complaint that Zynga learned during expedited discovery that of the purported cache of files removed, Patmore only may have provided two files to a Kixeye employee, and that neither of which could have constituted a trade secret. Thus, despite knowing this, Kixeye alleges that Zynga amended its complaint, not only continuing the suit against Patmore but also improperly naming Kixeye to gain additional access to its information through discovery. Kixeye further alleges that the two businesses occupy different market segments using the analogy of a Ducati (Kixeye) and a minivan (Zynga).

The use by Kixeye of California's unfair competition statute in the trade secret world is unusual. It is worth noting that under patent law, for a company to allege litigation constitutes unfair competition, courts have required that the party allege that the litigation was a "sham," that is, "objectively baseless," and that it has a general anti-competitive effect on the market. Whether these requirements will apply in this context, or whether Kixeye's current pleading sufficiently meets these elements remains to be seen. We will keep you posted as this contentious litigation develops.

Breach of Fiduciary Duty and Trade Secret Misappropriation Alleged In "Preppy Clothing Dispute" Involving Fashion Designer Tory Burch

By Jessica Mendelson (November 23, 2012)

A high profile trade secret dispute among the board members of one of the fashion world's most well-known companies has the American fashion elite taking sides. Last month, Christopher Burch filed a breach-of-contract and tortious interference complaint against his ex-wife, fashion mogul Tory Burch, in Delaware Chancery Court. In response, Tory filed counterclaims in early November, in which she accused Christopher of stealing trade secrets to establish stores which looked suspiciously like her own boutiques.

Tory Burch and her ex-husband, J. Christopher Burch, co-founded the fashion empire Tory Burch LLC in 2003. The company is an apparel and accessories brand providing consumers with luxury apparel and other goods. As Oprah Winfrey stated in 2005, the company is "the next big thing in fashion." Today, the company's annual sales total more than $700 million annually.

The Burches divorced in 2006, and both Tory and Christopher remained on the board of Tory Burch LLC. Christopher continued to pursue other projects, and in 2008, began to lay the groundwork to launch his own apparel brand, C.Wonder. The company opened its first store in October 2011. Its products included clothing, accessories, and home décor, all of which allegedly resembled Tory Burch's products, but were sold at a significantly lower price. Allegedly, the store copied the Tory Burch brand, using similarly styled lacquered front doors and store fixtures, as well as furniture and rugs which closely resembled those found in the Tory Burch stores.

In June 2011, Christopher provided the Board of Directors ("the Board") of Tory Burch LLC with notice that planned to sell his shares of the company. The Company then engaged Barclay's Capital to assist in the process of locating a buyer. This project was referred to as "Project Amethyst."

The events which followed the opening of C. Wonder vary depending on who is telling the story. Tory alleges the company sought to "arrive at a consensual resolution of its dispute" with Christopher, despite his violations of his fiduciary duties. In her counterclaim, she states the company continued to move forward with Project Amethyst to find a new investor to purchase Christopher's stake in the company. In addition, five of the seven board of directors agreed that Christopher would need to enter into a settlement agreement to protect Tory Burch LLC's brand and confidential information prior to completing any sale. According to Tory's version of the story, the three bidders positioned to purchase

Christopher's required such an agreement to be in place before they would agree to invest, and Christopher's refusal to agree prevented the sale from taking place. Christopher tells the story very differently, alleging Tory had cut off his power and "hijacked the bidding process" through which he had been attempting to sell his stake in the company. Furthermore, he alleges Tory manipulated third party bidders into requiring him and his company, C Wonder to reach a one-sided and onerous settlement agreement with the Company regarding trade secret misappropriation and trade dress infringement allegations.

On October 2, 2012, Christopher filed suit against Tory, the other directors, and Tory Burch LLC, requesting a declaratory judgment stating the defendants could not restrain him from pursuing other business ventures. Additionally, Christopher alleged the Board had breached the Operating Agreement by preventing him from engaging in other business ventures, tortiously interfered with his business relationships, and improperly interfered and acted in bad faith to impede his ability to sell his shares of the company.

On November 5, 2012, Tory filed counterclaims against Christopher, alleging Christopher had stolen trade secrets from Tory Burch LLC to establish stores which closely resembled Tory Burch boutiques. Tory alleged Christopher had stocked the stores with mass-market knock-offs of her luxury brand , and that under the terms of the operating agreement, he did not have the right to create knock-off goods, and his right to compete was qualified and limited by his other obligations as a director. Tory's counterclaim alleges Christopher breached his fiduciary duty by using confidential information belonging to Tory Burch LLC and engaging in unfair competition for his personal benefit. Additionally, Christopher allegedly misappropriated trade secrets from Tory Burch LLC, which he then used in creating C Wonder. Tory's counterclaim also alleges unfair competition, breach of contract, and deceptive trade practices. She further requests injunctive relief to stop Christopher's use of Tory Burch LLC's confidential information and company inventions.

Heavyweight fashion industry players like Anna Wintour and Diane Von Furstenburg have already spoken out in support of Tory Burch. According to Anna Wintour, the editor of Vogue, "As far as we're concerned [this is] 100% Tory's business, and we've never had anything to do with Chris." Diane Von Furstenburg, the President of the Council of Fashion Designers of America, echoes Wintour's support, characterizing Christopher's behavior as "bizarre and nasty."

The case is still in the early stages, but has already drawn attention for some colorful hearings. At the first scheduling hearing, which occurred on November 1, 2012, Chancellor Leo Strine promised not to burden anyone's holidays with this "preppy clothing dispute. . . I'm sorry, but this is — this is not a case about intercontinental ballistic missiles." In proposing an April trial date, Strine reflected on the popularity of "really ugly" duck shoes, "slightly irregular alligator shirts," and how "real WASPS actually don't go and pay full Polo price. . . at Macy's. No way. They actually will find a bargain. That's how they got to be, you know, WASPs." Strine went so far as to suggest, jokingly, that the best way to evaluate the similarities between the C. Wonder and Tory Burch brands would be a fashion show featuring the parties' attorneys. Finally, Strine discussed his recent reading of John Cheever's works, and explained its impact on the dispute. "Totally unrelated to this case, I've been deep in it, in an autumnal Cheever

phase. ” he said. “So I’ll have to just keep that up through the case. Have you read your Cheever lately? You know who he is? … And Mad Men will be coming back at some point in time. So I think if you read Cheever, go see the new Virginia Woolf revival and watch Mad Men, we’ll be all geared up and in the mood for this sort of drunken WASP fest. Are they WASPs? Are the Burches WASPs? Do we know?”

Whether Chancellor Strine’s preliminary views of this “preppy clothing dispute” lead to a quick resolution between the parties remains to be seen. We will continue to keep you apprised of future developments as the case progresses.

California Federal Court Finds Arbitration Agreement's Exclusion of Injunctive Relief for Trade Secrets and Unfair Competition Claims Is Not Unconscionable

By Joshua Salinas and Grace Chuchla (November 29th, 2012)

The fight over an employer's attempt to enforce arbitration agreements in the face of wage and hour class action claims is a common one in the world of labor and employment law. In fact, this is the very question that a federal district court for the Eastern District of California recently considered in *Steele, et. al v. American Mortgage Solutions d/b/a Pinnacle*, 2012 WL 5349511 (E.D. Cal., Oct. 26, 2012). Finding for the employer, the court, in its October 26th order, granted the defendant's motion to compel arbitration and dismissed the plaintiff's class action claims without prejudice. However, in doing so, the court also provided noteworthy analysis regarding the relationship between arbitration agreements and a company's efforts to protect its trade secrets, making this order a must-read for both trade secret litigators and those involved with wage and hour class actions and involved in drafting arbitration agreements.

Background Facts

The facts in this case are fairly straightforward. Pinnacle is a Pasadena, California based company that provides maintenance services and personnel. As a prerequisite to employment, Pinnacle required its employees to sign a binding arbitration agreement. Like most arbitration agreements, this agreement covered nearly all claims that could arise between Pinnacle and its employees and required that any disputes be settled "exclusively by final and binding arbitration before a neutral Arbitrator." Plaintiffs, all of whom signed such an agreement, brought suit under various California and federal laws alleging that Pinnacle required them to work more than forty hours a week without providing timely overtime compensation. After receiving the Complaint, defendant's attorney sent a letter to opposing counsel stating that Plaintiffs were bound by arbitration agreements. Plaintiffs, however, did not withdraw their complaint, and Pinnacle subsequently filed a motion to compel arbitration.

The court's analysis of Pinnacle's arbitration agreement first looks to the agreement's scope and then to its procedural and substantive conscionability.

Scope of the Agreement

The scope of the agreement does not cause the court concern; citing to various cases interpreting the Federal Arbitration Act ("FAA"), the court found that "the plain language of the Agreement covers plaintiff's claims in this case, all of which have been held to be subject to arbitration under the FAA." Additionally, the court dismissed plaintiffs' arguments that California wage and hour claims are exempt from the FAA. As the court saw it, plaintiffs' reliance on *Gentry v. Superior Court*, 42 Cal. 4th 443 (2007), and *Hoover v. American Income Life Insurance*, 206 Cal. App. 4th 1193 (2012), was for naught, as these cases were "either overruled or inapplicable" to plaintiffs' claims.

Procedural and Substantive Unconscionability

Under California law, both procedural and substantive unconscionability are required for an arbitration agreement to be enforceable and both elements are analyzed under a sliding-scale test. Plaintiffs in this case received their first win with the court's finding that ***the lack of an opt-out clause rendered the arbitration agreement procedurally unconscionable***. However, the tables turned back in Pinnacle's favor with the court's analysis of the agreement's substantive unconscionability, which is also where the court's analysis of trade secret claims and arbitration agreements lies.

When analyzing an arbitration agreement, courts evaluate the arbitration agreement's individual provisions for substantive conscionability to ultimately determine whether the agreement is "wholly unenforceable." In this case, suits seeking injunctive relief for unfair competition and/or disclosure of trade secrets received special attention because such suits are one the few types of claims that Pinnacle ***specifically excluded*** from mandatory arbitration under its agreement. As the court saw it, following the reasoning in *Ting v. AT&T*, 318 F. 2d 1126 (9th Cir. 2003), such exclusion raised the possibility of substantive unconscionability because it demonstrates a "stronger party…through a contract of adhesion, impos[ing] a forum on a weaker party without accepting the forum for itself." *Id*. at 1149 (*quoting Armendariz v. Foundation Health Psychcare Services*, 24 Cal.4th at 118, 99 (2000). Additionally, the court cited *Ferguson v. Countrywide Credit Industries, Inc.*, 298 F.3d 778 (9th Cir. 2002), which held that arbitration agreements that exclude claims that an employer is most likely to bring against an employee raise the suspicion of substantively unconscionable.

However, the key to the court's analysis is one short word – "***could***." Nowhere in its analysis does the court say that Pinnacle's exclusion of trade secret claims from its arbitration agreement unquestionably renders it substantively unconscionable. In fact, after looking at various other aspects of the agreement, ***the court's final conclusion is that nothing in Pinnacle's arbitration agreement is substantively unconscionable***. With respect to its exclusion of trade secret claims, there are "valid reasons, entirely independent from any intent to place the employees at a relative disadvantage or to generate one sided results, for excluding claims of unfair competition or trade secret violations from the mandatory arbitration agreement provisions of the Agreement." More specifically, the court recognized that, given the three-party nature of trade secret claims, arbitration is not the correct forum for such suits. Employers forced to arbitrate trade secret misappropriation claims would be forced to arbitrate against their former employee and bring suit in court against the former employee's current employer. Needless to say, such an arrangement would be a far cry from the Agreement's intent to bring efficiency to legal proceedings and could negatively affect the rights of the third-party current employer.

The court ultimately granted Pinnacle's motion to compel arbitration and to dismiss plaintiffs' claims without prejudice, thereby denying plaintiffs class relief.

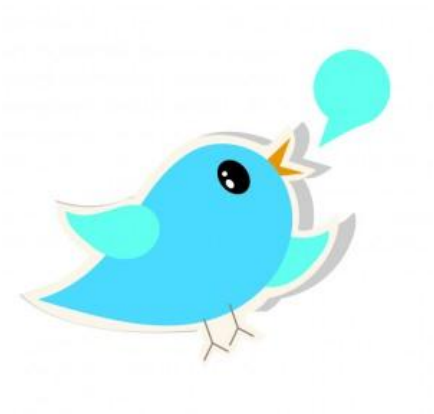
Takeaways

In short, this order may be a powerful tool for employers who are concerned both with mitigating the potential for class action suits in court and with protecting their trade secrets. With respect to the exclusion of suits for injunctive relief for the misappropriation of trade secrets, the "could be substantively unconscionable" reasoning that one finds in *Ting* and *Ferguson* has swung in the "not substantively unconscionable" direction. Indeed, the arbitration agreement's carve out of injunctive relief for trade secrets and unfair competition in this case is consistent with the Ninth Circuit's interpretation of the FAA to allow injunctive relief in the court even in arbitrable disputes, and a similar exception under California's Arbitration Act.

Pinnacle's exclusion of trade secret claims has stood the test of the court, and a commonsense analysis of how trade secret claims actually play out in the real world has prevailed over what could have been an unforgiving scrutiny of Pinnacle's exclusion of trade secret claims in the arbitration agreement.

Former PhoneDog Employee Off the Hook in Closely Watched Trade Secrets Spat

By Jessica Mendelson and Joshua Salinas (December 5th, 2012)



We previously blogged about the case of *PhoneDog v. Kravitz*, a Northern District of California case that called into question the ownership of Twitter followers on an employee's professional account following the employee's departure from the company. After over a year and a half of litigation, the parties have finally reached a settlement agreement.

Noah Kravitz, a former employee of PhoneDog, an "interactive mobile news and reviews website" was sued by his former employer, which claimed Kravitz unlawfully continued to use PhoneDog's Twitter account following his departure from the company. At the time of Kravitz's departure in October 2010, the twitter account had 23,000 followers. As of today, the account has more than 27,000 Twitter followers. Kravitz claims he took the Twitter account with the website's blessing. Phone Dog, however, sued Kravitz, demanding compensation for the Twitter followers Kravitz acquired through his employment with the company. This lawsuit was the "first to put a price tag on the worth of a Twitter user," (i.e. $2.50 per follower) and tackled the question of "who owns a professional Twitter account started during a period of employment."

The terms of the settlement are confidential, yet the parties have confirmed Kravitz will maintain sole custody of the Twitter account at issue. Additionally, the settlement will resolve all legal claims between the parties. "I'm very glad to have worked this out between us," Kravitz said in a statement. "If anything good has come of this, I hope it's that other employers and employees can recognize the importance of social media … good contracts and specific work agreements are important, and the responsibility for constructing them lies with both parties."

As Kravitz suggests, the case highlights the importance of clearly establishing ownership of social media before problems arise. Employers who make use of social media accounts should create contractual agreements that clearly state who owns these accounts. (See e.g. Ardis Health, LLC, Curb Your Cravings, LLC and USA Herbals, LLC v. Ashleigh Nankivell, 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011) (awarding injunctive relief and ordering former employee to return social media passwords to employer who had written ownership agreement). In the long run, creating such contracts can be significantly cheaper than the litigation that could ensue without such an agreement. This is especially true given the questionable value of Twitter followers, who can be "fickle [and] unpredictable." Although there is clearly a value in having such followers, legal experts, such as Eric Goldman, question whether it is really worth the cost of litigation in the case of such disputes, or whether the parties should simply create new accounts.

Legal experts advise that one way to avoid such disputes is to require employees to agree "that the company, not the employee, owns the account and that employees must return all social media logins and passwords at end of employment." This can be done through a written ownership agreement that explicitly lays out expectations about whether the account is meant for business or personal use. This is especially true given that "social media accounts often mix the personal and the professional, so from a practical standpoint making a clean break may not be possible." Please also see John Marsh's Trade Secret Litigator blog for a nice summary of the cases in this space.

Such agreements should be customized based on the employer's planned use of social media accounts for their specific business. Additionally, having such an agreement in place allows employees to create separate personal accounts if they so desire, which may prevent them from facing a situation similar to that faced by Kravitz. Finally, employers should also incorporate into such agreements that the employee agrees to return the passwords to the accounts upon the termination of their employment. Employers should be cautious, however, in wording such agreements in light of recent laws designed to protect employees' personal social media accounts.

NBA Sports Agent Slams Non-Compete and Trade Secret Claims and Scores 85K Jury Verdict Against Former Agency For Privacy Violation

By Robert Milligan and Jessica Mendelson (December 7th, 2012)

We have previously blogged on the colorful sports agent case of *Mintz v. Mark Bartelstein & Associates d/b/a Priority Sports & Entertainment et al.,* Case No. 12-02554 SVW (SSX), (C.D. Cal.), where Aaron Mintz, a National Basketball Players Association (NBPA) certified player-agent, and his former employer, Priority Sports & Entertainment ("Priority Sports"), clashed in California federal court regarding his departure from Priority Sports to Creative Artists Agency ("CAA").

The case recently concluded after a two-day jury trial in downtown Los Angeles, California resulting in a verdict awarding Mintz $85,000 on his invasion of privacy claim for Priority Sports' access of Mintz's personal email account after he left the company.

As discussed below, the case, apart from its colorful facts, has several key takeaways for employers.

General Background and Claims

By way of brief background, Mintz left Priority Sports in March 2012, accepted a position with competitor CAA, and immediately sought declaratory relief to invalidate his non-compete agreement with Priority Sports. As the case progressed, Mintz added additional claims against Priority Sports for violations of the Computer Fraud and Abuse Act ("CFAA"), the Electronic Communications and Privacy Act ("ECPA"), and California Penal Code section 502, as well as claims for defamation, invasion of privacy, intentional inference with contractual relations, and violation of Business and Professions Code section 17200. Mintz asserted some of the claims against Priority Sports principle Mark Bartelstein.

Mintz alleged that he worked for Priority Sports for eleven years and then decided to pursue a better opportunity with CAA. Apart from the two year non-compete, which he claimed violated Business and Professions Code section 16600, Mintz claimed the fourteen-day notice of termination provision in his employment agreement violated section 16600 as well. Mintz claimed that the notice provision restricted his ability to terminate his employment, and thereby prevented him from competing with Priority Sports for two weeks after termination in violation of California law. Mintz's employment contract prohibited Mintz from soliciting company clients or business on behalf of a competitor or performing any activities for a competitor during his employment with Priority Sports. It further provided

that, for two years after his termination, Mintz was prohibited from soliciting company clients or providing services that are similar to the services provided by Priority to company clients.

Mintz also claimed that after he resigned Priority Sports hacked his personal email account, reviewed his contract with CAA, and disclosed its terms to third parties. He also claimed that defamatory statements were made to basketball executives, players, and family members of players to persuade players not to follow Mintz to CAA.

Priority Sports counterclaimed against Mintz asserting claims for breach of contract, breach of covenant of good faith and fair dealing, breach of duty of loyalty, misappropriation of trade secrets, intentional interference with contractual relations, intentional interference with prospective economic advantage, conversion, violation of California Penal Code section 502, defamation, trade libel, conspiracy, and unfair competition. Priority Sports also asserted some of the claims against CAA.

Shortly before the trial, the Court ruled on both parties' motions for summary judgment. As described in more detail below, the Court granted Mintz's motion for summary judgment with respect to his claims for violations of California Penal Code section 502 and invasion of privacy, but denied the motion for summary judgment with respect to his claim under California's unfair competition statute. The Court also granted summary judgment in favor of Mintz and CAA on each of Priority Sports' counterclaims, and denied Priority Sports' motion for partial summary judgment on its claims for breach of contract and breach of the duty of loyalty against Mintz. The Court also granted summary judgment in favor of the defendants on Mintz's claims for declaratory relief, violation of the CFAA, and violation of the ECPA.

Mintz's Motion for Summary Judgment on His Claims

The Court's ruling on the parties' summary judgment motion resolved a number of significant issues in the case. Mintz's employment contract with Priority Sports included both a two-year non-compete agreement and a requirement that he provide fourteen days written notice prior to leaving the company. Rather than provide notice, Mintz resigned to Bartelstein by telephone. Upon hearing of Mintz's resignation, Bartelstein allegedly responded, "Wait until I tell the world about this. You made your bed, you better be ready to lie in it."

Additionally, after Mintz resignation, Priority Sports' counsel allegedly instructed another employee to access Mintz's personal email account without Mintz's permission. The employee obtained a temporary password without Mintz's consent and accessed Mintz's gmail account for at least twenty minutes. It was undisputed that the employee viewed a copy of Mintz's employment agreement with CAA. The next day, Mintz's colleague emailed Mintz the following message: "I'm in shock! Rumor on the street is that CAA is paying you less money over 4 years then [sic] you would have made here. I don't get it[.] You had a 50-year guaranteed deal here." Mintz also contended that defendants leaked his employment terms with CAA to a third party.

Mintz requested a declaratory judgment that the non-compete was void but the Court found that he failed to meet his burden of demonstrating an actual controversy. At the hearing, defendants responded that their refusal to stipulate that Priority would not enforce the non-compete was not based

on any desire to enforce the non-compete provision, but rather their concerns with the overbreadth of the proposed stipulation provided by Mintz's counsel. The Court concluded that there was no evidence that defendants had attempted, in this or any other litigation, to enforce the non-compete clause. The Court, therefore, concluded that Mintz had not met his burden of demonstrating an actual controversy with "sufficient immediacy and reality to warrant the issuance of a declaratory judgment."

With respect to the notice of termination provision, the Court found that Mintz did not take issue with the notice requirement itself, but argued that the clause was unenforceable because it prevented him from competing for clients after leaving Priority Sports. In short, according to the Court, Mintz only contended that the two-weeks' notice provision is unenforceable "to the extent Priority Sports asserts it prevented Mintz from competing for clients, including his own clients, after his resignation." The Court stated that Mintz misconstrued defendants' position regarding the provision. According to the Court, in their opposition, defendants conceded that the notice provision "did not prevent Mintz from terminating his employment or from joining CAA; nor did it prevent Mintz from competing fairly with Priority Sports after his termination date." (Opp. at 9). Instead, defendants only argued that Mintz breached the notice provision by failing to give fourteen days' notice of his resignation. According to the Court, Mintz cannot conjure an actual controversy by distorting defendants' position on the notice provision. Given the foregoing, the Court concluded that because Mintz and defendants' positions were not in fact opposed, there was no actual controversy over the effect of the notice provision. Therefore, the Court granted summary judgment for defendants with respect to Mintz's claims for declaratory relief.

The Court then granted summary judgment for Priority Sports on Mintz's CFAA claim concerning the access to his personal email account. Under the CFAA, to bring a civil action, damages or loss to the victim must fall under five specific circumstances. Mintz alleged in this case that there was "loss to 1 or more persons during any 1–year period . . . aggregating at least $5,000 in value." 18 U.S.C.§ 1030(c)(4)(A)(i)(I). Under the CFAA, "loss" is defined as "any reasonable cost to any victim." 18 U.S.C. § 1030(e)(11).

Here, the Court found that the evidence Mintz presented failed to satisfy the threshold, because Mintz's legal fees here were paid by CAA, and not Mintz, the victim in the offense. As a result, this expense could not be considered a cost to him. Additionally, the Court held that the expense of the litigation did not count as a loss under the CFAA because it was not "essential to readying the harm of the unauthorized access." The Court reasoned that Mintz knew right after his departure from Priority Sports that it was responsible for the offense, and that it had accessed Mintz's employment contract with CAA. According to the Court, all Mintz needed to do to secure his gmail account – indeed, all he could do – was to change the password and the back-up email address used to retrieve the password. The Court concluded that it defies common sense to believe that Mintz's subsequent legal efforts to confirm Priority Sports' involvement were "essential to remedying the harm" of the unauthorized access. Accordingly, the Court concluded as a matter of law that the litigation costs in the case do not count as a "loss" under the CFAA.

With respect to the ECPA claim, the Court granted summary judgment in favor of Priority Sports. Mintz alleged Priority Sports had intentionally intercepted his electronic communication. However, the Court found no interception, since the emails were not accessed during transmission, but after receipt.

In a bit of a surprise considering its ruling on the CFAA claim, the Court did, however, find that Priority Sports violated California Penal Code section 502 by "knowingly accessing" Mintz's gmail account and wrongfully obtaining data without his permission. Section 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit. Under the plain language of the statute, any amount of damage or loss may be sufficient." *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08–05780 JW, 2010 WL 3291750, at *4 (N.D. Cal. 2010) (holding that the fact that plaintiff "expended resources" to stop further violations of § 502 sufficed to establish damages, even if such resources only comprised a few "clicks of a mouse" and some "keystrokes"). Upon review, the Court found that the undisputed facts showed that Priority Sports knowingly and without permission used a computer to wrongfully obtain data, in violation of § 502(c)(1). Specifically, defendants did not dispute that at the direction of Priority Sports' counsel, a Priority Sports employee accessed Mintz's gmail account without permission, and viewed the contents of several emails, including Mintz's employment agreement with CAA. (Opp. at 9). The Court further found that Mintz experienced sufficient damage to support a private right of action. The Court found that it was undisputed that after the hacking incident, Mintz spent some time restoring his gmail password and investigating who had hacked the gmail account. (Mintz Decl. ¶ 19). In light of the foregoing undisputed facts, the Court concluded that Defendants violated California Penal Code § 502. Accordingly, the Court granted Mintz summary judgment on the § 502 claim.

The Court also granted summary judgment for Mintz on the invasion of privacy claim. According to the Court, Mintz had a legally protected interest in his personal email account, along with a reasonable expectation of privacy. By accessing this account, Priority Sports committed a serious invasion of Mintz's privacy interest without reasonable justification.

Finally, with respect to the unfair competition claim, the Court declined to grant summary judgment, finding Mintz had failed to show a loss of money or property resulting from unfair competition as required by Proposition 64.

Mintz and CAA's Motions for Summary Judgment as to Priority Sports' Counterclaims

The Court granted Mintz's motion for summary judgment on Priority Sports' breach of contract counterclaim because of Priority Sports' failure to provide factual support for this claim. Priority Sports claimed, among other things, that Mintz breach his contract by working for CAA prior to his resignation, soliciting players on CAA's behalf prior to his resignation, and failing to provide fourteen days written notice. While the parties' disputed whether one NBA player was solicited by Mintz prior to his departure, there was no evidence that the player left Priority Sports to join Mintz at CAA. The Court found that Priority Sports did not demonstrate that it suffered any damages as a result of any conduct by Mintz. The Court also found that Priority Sports could not establish damage resulting from Mintz's failure to give fourteen days' notice. Priority Sports contended that the lack of notice "deprived Priority

Sports of the opportunity to reach out to those of its clients who had worked with client-service teams that included Mintz and to secure its relationships with those clients before Mintz's departure was a fait accompli." (Opp. at 16). According to the Court, the sole support for this assertion was Bartelstein's declaration, in which he claims that because of the lack of notice, he was unable to contact a client until five days after Mintz's resignation. (Bartelstein Decl. ¶ 7). But Bartelstein also conceded that the client remained with Priority. Finally, the Court stated that Priority Sports failed to identify a single client that it lost as result of Mintz's failure to give notice. Based on this deficient showing, the Court concluded that no rational fact-finder could conclude that Mintz's failure to give notice damaged Priority Sports. The Court also dismissed Priority Sports' breach of the implied covenant of good faith and fair dealing, finding it to be based on the same speculative assertions.

Priority Sports' claim that Mintz breached his duty of loyalty was also rejected by the Court. According to the Court, under California law, an employee does not breach his duty of loyalty merely by preparing to compete with his employer. In addition, there was no showing that Mintz's actions had actually harmed Priority Sports. According to the Court, there was no evidence that Mintz actually solicited Priority Sports' clients nor did Priority Sports present facts that described how it was harmed by Mintz's preparatory steps. Priority Sports also failed to direct the Court to any evidence, for example, that Mintz's plan making resulted in the loss of a client. Based on this reasoning, the Court found there was no triable issue of breach or damages.

The Court also granted Mintz's motion for summary judgment on the misappropriation of trade secrets counterclaim, finding that Priority Sports failed to offer specific evidence of misappropriation. According to the Court, "Priority Sports' Opposition is utterly devoid of evidence that Mintz or CAA misappropriated any trade secrets belonging to Priority Sports." Furthermore, the Court granted summary judgment for Mintz on the intentional interference with contractual relations claim, finding "Priority Sports has failed to present any evidence that CAA committed any independently wrongful act to induce Mintz to breach or disrupt its at-will employment contract with Priority Sports." The Court also granted Mintz's motion for summary judgment on the conversion claim, finding that the ownership of the blackberry that Mintz used while employed by Priority Sports was disputed, and therefore, there was insufficient evidence to assert a claim of conversion. Additionally, the Court granted Mintz's motion for summary judgment on defamation and trade libel, finding that Priority Sports had failed to produce evidence of the specific libelous statements Mintz allegedly made. Finally, the Court found there was insufficient evidence of either conspiracy or unfair competition by CAA, and granted CAA's motion for summary judgment on both counts.

Jury Verdict in Favor of Mintz

The trial, which concluded on November 14, 2012, was essentially limited to a determination of damages on Mintz's claims for violation of Penal Code § 502 and for invasion of privacy. Mintz elected not to pursue his affirmative claims for defamation, interference with contractual relations, and violation of California's unfair competition statute.

The jury awarded damages on Mintz invasion of privacy claim of $85,000 against Priority Sports, which was apportioned $80,000 for past noneconomic loss, including emotional pain/mental suffering, and $5,000 for future noneconomic loss, including emotional pain/mental suffering. The Court granted the Defendants' motion for a directed verdict regarding punitive damages, finding Priority Sports' conduct insufficiently malicious, oppressive or fraudulent to qualify for punitive damages. The Court reasoned that if the mere fact that Priority Sports had unlawfully and intentionally accessed Mintz's gmail account rose to the level of malice, "every intentional tort would give rise to punitive damages." The Court also found that Mintz was not entitled to emotional distress damages on his Penal Code § 502 claim because he did not disclose those damages in his complaint or discovery disclosures.

Takeaways

*__Don't access your employees' personal email accounts.__ The Court's handling of the CFAA and the Penal Code § 502 claims is interesting. While Mintz could not maintain a claim under the CFAA because to there was no "loss" and Mintz's subsequent legal efforts to confirm Priority Sports' involvement were not "essential to remedying the harm" of the unauthorized access, Mintz was able to maintain a California Penal Code section 502 claim, as well as an invasion of privacy claim, based upon the same conduct. Accordingly, employers should not access their employees' personal email accounts, even if conducting a workplace investigation, unless they receive express written consent from the employees in question. Look for more Penal Code § 502 claims in light of this decision.

*__Consider using notice provisions with employees in your trade secret protection agreements.__ The Court's handling of the two-week notice prohibition serves as a reminder that California is very much a pro-employee state. Rather than address whether the two-week notice provision violates California's prohibition on non-compete agreements, the Court found that there was no controversy, and no damages resulting from Mintz's actions. According to the Court, Priority Sports failed to identify a single client it lost as a result of Mintz's failure to give notice, and thus, there was no resulting harm. Notwithstanding, the Court did not indicate that the notice provision was unlawful. Accordingly, employers should consider utilizing reasonable notice provisions in their trade secret protection agreements. While you may not be able to recover damages, you may be able to use the breach of such provisions to leverage a threatened misappropriation of trade secrets claim and as evidence of an ill intent by the departing employee.

__*Exit interviews are essential.__ A thorough exit interview with a departing employee is an essential part of an effective trade secret protection plan. An employee's failure to cooperate or evasive activities can be used by the employer to support a claim of threatened misappropration of trade secrets against the employee and also give an employer the heads up to investigate the employee's computer activities on its network as well as to secure company customer and employee relationships. Please see our recent webinar on Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours for more on effective exit interviews.

__*Need creative approaches.__ Some cases, if important to the company, necessitate creative approaches. Here, Mintz had NBA player relationships throughout the United States, Priority

Sports was based out of Illinois, Mintz had regular communications with its Illinois staff and traveled to Illinois for business meetings, and the non-compete was governed by Illinois law. With Priority Sports and Mintz's connections with Illinois, an Illinois forum would likely have been much more favorable for Priority Sports. While Mintz still may have pursued his suit in California, Priority Sports could have had the possibility of an alternative forum. A mandatory forum selection provision, coupled with a consent to jurisdiction clause, as well as possibly an arbitration provision, may have provided Priority with additional options to pursue. Please see our previous blog on a California federal court's recent dismissal of a declaratory suit , like Mintz's claim, based upon a Pennsylvania forum selection provision.

***Need evidence of wrongful solicitation and use of trade secrets.** Finally, this case shows that the evidence necessary to show damages and use of trade secrets can be difficult to prove without cooperating witnesses or evidence of data transmission and use, particularly where the main focus of the suit is on damages, rather than injunctive relief.

$4.38 Million Verdict In Utah Federal Court For Malicious Trade Secrets Misappropriation

By Paul E. Freehling (December 11th, 2012)

A Utah federal judge recently held that a jury's compensatory damages award of $2.92 million for misappropriating trade secrets was supported by the evidence and was not excessive. Because the jury found by clear and convincing evidence that the misappropriation was willful and malicious, the court added $1.46 in exemplary damages. The total verdict: $4.38 million. *Storagecraft Technology Corp. v. Kirby*, Case No. 2:08-CV-921 (D.Utah, Sept. 27 and Dec. 4, 2012) (appeal pending).

STC developed and obtained a copyright on a source code. The company went to considerable lengths to maintain the code's secrecy. No one could access the company's technology without signing a confidentiality agreement, obtaining a license, and agreeing to pay a royalty. Kirby, a software engineer, resigned as a STC employee in late 2004. Shortly before he quit, he informed the company that he had stored the source code and related files on his laptop and desktop. When STC's attorney communicated with him about returning this intellectual property, he responded that it would be deleted or returned. Not trusting him, the company sued him for misappropriation.

As part of the 2005 settlement of the case, Kirby represented and warranted that he had returned all of STC's intellectual property. In addition, he promised that he would not use or disclose such property, and that he would cooperate with STC in preserving it. One year later, Kirby delivered to a company he knew to be a STC competitor and lawsuit adversary his entire backup file containing the source code and 100,000 emails he had sent or received while a STC employee.

When STC learned about this delivery, it sued Kirby for misappropriation, breach of contract and copyright infringement. At trial, evidence was introduced supporting STC's claims, including a charge that Kirby was motivated by a desire to harm the company. The Utah Trade Secrets Act permits the use of a reasonable royalty as a basis for the computation of damages for trade secret misappropriation. STC's trial expert testified that a reasonable royalty for an unrestricted license to the company's source code was at least $4.5 million.

The jury discounted the expert's calculations and awarded $2.9 million in compensatory damages. Based on the jury's finding that Kirby had maliciously injured STC, the court added exemplary damages in an amount equal to 50% of the jury's award. Kirby is appealing the judgment.

In a post-trial motion, Kirby argued that the jury verdict was contrary to the clear weight of the evidence, and that the compensatory damages award "was excessive, unreasonable, and should shock the conscience of [the] Court given the lack of evidence that Kirby proximately caused any 'actual injury or loss' to STC." The court rejected Kirby's argument and stated: "The very essence" of the parties' prior settlement agreement "was Kirby's covenant to return and protect all STC Intellectual Property."

The ruling is of particular interest because, by upholding the reasonable royalties method of computing damages for misappropriation of trade secrets, STC did not have to show that Kirby actually profited from his misconduct (although there was evidence that the competitor to whom he disclosed STC's trade secrets paid him a salary of $15,000 per month for some unspecified period). Moreover, STC was not required to prove what the competitor would have been willing to pay, if anything, for use of the confidential data.

Ninth Circuit Hears Oral Argument in Rival Toy Makers' Trade Secrets Dispute

By Joshua Salinas (December 12th, 2012)

Two rival toy makers engrossed in an eight-year battle over the Bratz doll line have once again taken their fight to the Ninth Circuit. This week, a Ninth Circuit panel consisting of Chief Judge Alex Kozinski, Judge Kim Wardlaw, and Judge Stephen Trott, heard oral argument concerning an award of more than $310 million in damages and attorneys' fees against Mattel, Inc. in its dispute with MGA Entertainment, Inc.

This is the second time the case has made its way to the Ninth Circuit and to the same three-judge panel. In 2010, the same panel reversed a jury verdict that awarded Mattel nearly $100 million in damages for copyright infringement and the ownership rights to the Bratz doll brand. Previously, Chief Judge Kozinksi, writing for a unanimous panel, reversed the decision below that Bratz creator and former Mattel employee Carter Bryant had assigned the intellectual property rights in the dolls to his former employer through his employment agreement's invention assignment provision. The case was remanded for a retrial.

In a surprising turn of events, the second jury in the contentious case awarded more than $80 million in damages to MGA for Mattel's alleged trade secret misappropriation (a claim that was not tried in the first jury trial), plus attorneys' fees and treble damages for a total amount of more than $310 million.

Oral arguments began Monday in Pasadena, California. Mattel requested the court to vacate or reverse the award on grounds that MGA's trade secret counterclaim was untimely and barred by the statute of limitations. Mattel also asked the court to reverse or vacate the trade secret damages award on grounds of insufficient evidence, and reverse or vacate the attorneys' fees and costs award on grounds that Mattel's pursuit of its copyright claim was objectively reasonable.

During yesterday's oral arguments, the panel primarily focused on the timing issue. The statute of limitations for trade secret misappropriation under the California Uniform Trade Secrets Act (Cal. Civ. Code § 3426.7) is three years after the plaintiff discovers, or should have discovered, the misappropriation.

During its oral argument, Mattel explained that MGA filed its trade secret counterclaim against Mattel in August 2010, on grounds that Mattel allegedly stole trade secret information about the Bratz Doll lines during toy fairs. Mattel argued that the statute of limitations began running in 2004, when MGA had "reason to suspect" the alleged misappropriation after it hired two Mattel employees that were aware of Mattel's alleged "toy fair conduct." Specifically, Mattel pointed to MGA's prior pleadings and discovery

requests concerning the alleged toy fair conduct, which allegedly evinced MGA's "reason to suspect." Thus, Mattel argued that more than three years had passed and MGA's trade secret counterclaim was untimely and barred.

In addition, Mattel argued that the district court erred when it found that MGA's trade secret counterclaim compulsory and related back to Mattel's own trade secret claim in 2006, because the two sets of claims involved different trade secrets that were allegedly stolen at different places and times; by different actors; and through different means.

MGA opened its argument by accentuating Mattel's alleged deposition misconduct, which allegedly tolled MGA's claim. MGA also argued that its counterclaim was compulsory because Mattel's trade secrets claim concerned the same "category of documents."

Chief Judge Kozinski pressed MGA hard on its "same category of documents" position. The Chief Judge emphasized that the compulsory issue is based on the claim, not documents. For example, he explained that the same document can simultaneously support different torts and contracts claims without giving rise to compulsory counterclaims. He stated that he "didn't see how it's compulsory or anywhere related."

MGA also argued that there is a "logical relationship" between the parties' trade secret claims. Judge Trott said he is having trouble with this argument based on the definition provided in *In Re Pegasus Gold Corp*., 394 F.3d 1189 (9th Cir. 2005), which is "the same aggregate set of operative facts as the initial claim." Mirroring the Chief Judge's concerns, Judge Trott said he does not see what constellation or common nucleus of facts makes them compulsory. He said the two claims are as different as "chalk and cheese."

If the Ninth Circuit finds that the counterclaim was not compulsory, and MGA did not have reason to suspect it should have brought its counterclaim earlier, this could mean more litigation in this action in the upcoming year. In fact, Judge Wardlaw suggested that MGA refile its trade secret claim as a separate new lawsuit against Mattel.

While the ultimate outcome of this dispute is unclear, what is clear is that it does not appear to be reaching a resolution any time soon.

We will keep you apprised of any further developments.

Wisconsin Federal Court Finds That Common Law Claims Are Preempted by the California Uniform Trade Secrets Act

By Daniel Hargis (December 13th, 2012)

The case of *Illumination Management Solutions, Inc. v. Ruud* pending in the Eastern District of Wisconsin exemplifies the continuing lack of certainty on the scope of California Uniform Trade Secrets Act ("CUTSA") preemption when the claims potentially subject to preemption concern information that itself may not qualify as a trade secret but is nevertheless confidential or proprietary.

CUTSA does not preempt claims that seek "civil remedies that are not based upon misappropriation of a trade secret." Cal. Civ. Code § 3426.7(b). While this language may suggest on its surface that claims alleging misappropriation of information not rising to the level of a trade secret are not preempted, courts disagree on the issue. *Compare, e.g., Leatt Corp. v. Innovative Safety Tech., LLC*, No. 09–CV–1301, 2010 WL 2803947, at *6 and n. 5 (S.D. Cal. July 15, 2010); *Phoenix Tech. Ltd. v. DeviceVM*, No. C 09–04697, 2009 WL 4723400, at *5 (N.D. Cal. Dec. 8, 2009) with *Mattel, Inc. v. MGA Entm't, Inc.,* 782 F.Supp.2d 911, 987 (C.D. Cal. 2011); *Gabriel Techs. Corp. v. Qualcomm Inc.,* No. 08CV1992, 2009 WL 3326631, at *11 (S.D. Cal. Sept. 3, 2009).

Illumination Management, which was adjudicating the CUTSA as the case was originally filed in federal court in Los Angeles but was later transferred to the Eastern District of Wisconsin, falls into the group of cases finding such claims to be preempted. The dispute arose out of the one-time collaboration of two businesses in the lighting industry. The plaintiff, a company specializing in the development of light emitting diode technology, partnered with the Wisconsin based defendants to incorporate its technology into defendants' products. The collaboration led to the defendants becoming shareholders in the plaintiff and obtaining a seat on the plaintiff's board. Because of the relationship, the plaintiff freely shared information and technology with the defendants. The defendants are alleged to have thereafter introduced their own competing products using the light emitting diode technology. And the defendants entree into the market, according to the plaintiffs, was due to various wrongs perpetrated by the defendants, including misappropriation of the plaintiff's trade secrets and breach of common law duties owed to the plaintiff.

After the case was transferred to the Eastern District of Wisconsin, the defendants moved to dismiss the plaintiff's second amended complaint, which alleged eleven claims, including misappropriation under CUTSA and several common law claims.

In September, the court dismissed plaintiff's common law claims for breach of fiduciary duty, civil conspiracy, aiding and abetting breach of fiduciary duty, and negligent breach of the duty of care finding that the claims arose from the same nucleus of facts as the CUTSA claim and were thus preempted. *Illumination Management Solutions, Inc. v. Ruud*, No. 10–C–1120, 2012 WL 4069315 (E.D. Wis. Sept. 14 2012). The court stated that claims based on the misappropriation of information that does not qualify as a trade secret are preempted by CUTSA. Id. at *4. Recently, the court denied the plaintiff's motion for reconsideration of the dismissal order. *Illumination Management Solutions, Inc. v. Ruud*, No. 10–C–1120, 2012 WL 6060967, *1-2 (E.D. Wis. Dec. 6, 2012). The court, however, did grant the plaintiff's alternative request to amend its complaint to attempt to allege common law claims that "do not involve the misuse of trade secrets or confidential information." Id. at *3 (emphasis original).

Whether claims based on the misappropriation of information that does not qualify as a trade secret are preempted by CUTSA may one day be resolved by the California Supreme Court. But until then, Illumination Management highlights that claimants who merely assert, in the alternative to their trade secret claim or otherwise, that misappropriation of information not qualifying as a trade secret can nevertheless give rise to non-trade secret claims risk dismissal of those claims on preemption grounds.

Claimants need to be aware of the issue and, if there are valid grounds to do so, plead around the preemption defense. If there is another theory that would support a non-trade secret claim beyond a misappropriation of information theory, the claimant should plead that alternative theory if it can do so in good faith. The theory can be pled in conjunction with, but as a clearly delineated alternative to, a misappropriation of information theory. Before filing the pertinent pleading, the claimant should thus consider potential alternative theories for its non-trade secret claims, ensure there is support for the alternative theories, or if the theories can be asserted on information and belief, and draft the pleading such that it is clear that the alternative theories are distinct from a misappropriation of information theory. This is really an exercise in issue spotting and thinking creatively about one's claims.

Finally, claimants shouldn't assume they will be able to cure pleading deficiencies through amendment. Even if given leave to amend, the allegations in a prior pleading can doom a subsequent pleading. For example, at least in California, admissions in an original pleading that has been superseded by an amended pleading remain within the court's cognizance, and the alteration of such admissions by amendment designed to conceal fundamental vulnerabilities in a plaintiff's case will not be accepted the court. *See, e.g., Berg & Berg Enterprises, LLC v. Boyle*, 178 Cal.App.4th 1020, 1043 n. 25, 100 Cal.Rptr.3d 875 (2009). Similarly, a claimant may not avoid dismissal by alleging facts in an amended pleading that contradict those facts originally pled. *See, e.g., McKell v. Washington Mut., Inc*., 142 Cal.App.4th 1457, 1491, 49 Cal.Rptr.3d 227 (2006).

Trading Secrets

Tidings of Data Theft and Coal: California Federal Court Holds That Trade Secret Misappropriation Statute Preempts Claim For Misappropriation Of Confidential Non-Trade Secret Data

By Paul Freehling and Jim McNairy (December 24, 2012)

There was only coal delivered for California employers in a recent California federal decision in which the Court refused to permit a plaintiff to proceed on a tort theory for the theft of confidential information.

In a well-researched and articulate opinion, the federal court for the Northern District of California recently dismissed, as preempted by the California Uniform Trade Secrets Act (CUTSA), claims for misappropriation of non-trade secret proprietary information. Judge Koh, reasoned that those claims arose out of the same operative facts as the plaintiff's trade secret misappropriation cause of action. *SunPower Corp. v. Solarcity Corp.,* Case No. 12-CV-00694-LHK (N.D. Cal., Dec. 11, 2012) (Koh, J.).

CUTSA contains two somewhat contradictory provisions. It states that "claims based on the same nucleus of facts as trade secret misappropriation" are preempted. But it also provides that the preemption clause does not affect contractual and other claims "that are not based upon misappropriation of a trade secret." A court analyzing a complaint which alleges misappropriation of trade secrets may conclude that some of the confidential proprietary data referenced does not qualify as a trade secret because, for example, the owner failed to make reasonable efforts to maintain its secrecy. Judicial decisions are divided in such instances as to whether a cause of action for misappropriation of non-trade secret data is preempted.

Judge Koh relied primarily on a California Appellate Court opinion in which, albeit in dicta and in a footnote, the Appellate Court "emphatically reject[ed]" a Pennsylvania federal court's decision that statutory preemption does not apply. *Silvaco Data Systems v. Intel Corp.,* 184 Cal. App. 4th 210, 239 n.22 (2010) ("a prime purpose of the [Uniform Act] was to sweep away the adopting states' bewildering web of rules and rationales and to replace it with a uniform set of principles for determining when one is—and is not—liable for acquiring, disclosing, or using 'information of value'"), disapproved on other grounds, *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310 (2011).

The individual defendants in SunPower all were sales employees of the plaintiff, a manufacturer and distributor of solar panels, until they were recruited by SolarCity which also distributes solar panels. All of the individual defendants had signed confidentiality agreements with SunPower. The nine-count complaint alleged that the individual defendants misappropriated (a) trade secrets, in violation of CUTSA, and (b)

"non-trade secret proprietary information." The defendants moved to dismiss the latter claims primarily on the ground that they were superseded by the statute.

In *SunPower*, Judge Koh cited Georgia, Hawaii, Idaho, New Hampshire and Vermont Supreme Court decisions, as well as several district court opinions, that concurred with the *Silvaco* dicta and held that non-trade secret misappropriation claims are preempted. However, she also identified a half dozen other district court opinions that were in accord with the Pennsylvania federal court ruling *Silvaco* criticized. Moreover, she referenced two Ninth Circuit holdings which, "while not explicitly addressing the issue of supersession, . . . have suggested" that the Pennsylvania federal court decision is correct, but she concluded that those holdings "should not be followed to the extent they suggest that SunPower may bring a claim based on confidential or proprietary information that does not satisfy the definition of a trade secret." She reasoned that the *Silvaco* court's rationale was the more persuasive and that decisions to the contrary failed adequately to consider that rationale.

Ultimately, Judge Koh held that, in light of *Silvaco*, claims for misappropriation of proprietary non-trade secret information would be superseded by CUTSA unless (1) such information was "made property by some provision of positive law", or (2) the non-trade secret claims allege "wrongdoing that is materiall[y] distinct [] [from] the wrongdoing alleged in a [C]UTSA claim". By addressing both the nature of the information at issue and the conduct related to alleged unlawful acquisition or use of such information, Judge Koh very broadly interpreted the preemptive effect of CUTSA. In doing so, she placed a premium on careful, precise pleading.

Another issue raised by SunPower in opposition to SolarCity's motion concerned the propriety of deciding, pursuant to a Rule 12(b)(6) motion rather than delaying until the summary judgment stage, whether SunPower's trade secret and non-trade secret claims arose out of the same nucleus of facts. In several cases cited by SunPower, the courts denied Rule 12(b)(6) motions on the ground that, for purposes of deciding such motions, the plaintiffs' factual allegations must be accepted as true. However, Judge Koh was not convinced. She cited one Northern District of California decision to the contrary, and she referenced the U.S. Supreme Court's opinions in *Ashcroft v. Iqbal* and *Bell Atl. Corp. v. Twombley* in concluding that SunPower's complaint asserted implausible causes of action regarding non-trade secret information (however, she said she would grant SunPower leave to amend its complaint).

Judge Koh left no doubt concerning her resolution of the present confusing and contradictory state of California law regarding preemption by CUTSA of non-trade secret claims. She went out on a limb by relying on controversial dicta in a California Appellate Court opinion, an opinion which she candidly noted was disapproved —on other grounds—in a later California Supreme Court ruling. Her decision will be applauded and cited by defendants in that state and elsewhere, but it will be criticized by plaintiffs and employers having deal with data theft by former employees. At an early date, the legislators should consider amending the Act by removing the current inconsistency. This is particularly the case because a trade secret claim has a heightened evidentiary standard and employers may not be able to pursue such a claim (at least under a tort theory) where an employee steals data that may not rise to the level of a trade secret in light of this decision.

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

By Scott Schaefers (January 5, 2012)

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?

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.

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. v. 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.

Waiting On Nosal...Combating Data Theft Under The Computer Fraud and Abuse Act In The Ninth Circuit

By Robert Milligan (February 20, 2012)

A recent California federal court decision has permitted an employer to pursue a former employee for alleged violations of the employer's computer usage policies under the Computer Fraud and Abuse Act ("CFAA"), while an en banc Ninth Circuit panel considers the validity of such claims. The Ninth Circuit's decision in the *United States v. Nosal* provided employers with a potentially powerful tool under the CFAA to combat data theft by employees and other insiders, only to see the decision rendered non-citable in October 2011 while an en banc Ninth Circuit panel reconsiders the issue. A recent decision from federal district judge Larry Alan Burns of the United States District Court, Southern District of California, reflects a willingness to allow employers to continue to use the CFAA to combat data theft at least until the en banc panel rules in Nosal.

The case, *Platinum Logistics v. Mainfreight and Melissa Ysais*, centers around Ms. Ysais, a former sales manager at Platinum Logistics who allegedly violated a binding nondisclosure agreement by taking customer lists and rate sheets in her transition to a competitor. Platinum Logistics claims that, in taking these electronic documents without permission, Ms. Ysais violated the CFAA.

In its initial complaint, Platinum Logistics specifically cited § 1030(a)(5)(C), a subsection of the CFAA which prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss." Ruling on a motion to dismiss, the Court cited the Ninth Circuit's interpretation of § 1030(a)(5)(C) given in *LVRC Holdings LLC v. Brekka* in which access without authorization is defined as "without any permission at all." Given that Ms. Ysais accessed the documents in question while still employed at Platinum Logistics and had accessed them previously within the scope of her job, the Court granted the defendant's motion to dismiss, but without prejudice to Platinum Logistics. In his discussion on the matter, the Court provided Platinum Logistics with the opportunity to file an amended complaint, citing a different subsection of the CFAA as the potential basis for a valid claim.

According to the Court, Platinum Logistics may have a valid claim under §§ 1030(a)(2) and (a)(4), which offers legal recourse for cases where authorized access is exceeded. As interpreted by the Ninth Circuit in *Nosal,* "an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access restrictions - including use restrictions." In the case of Platinum Logistics, Ms. Ysais's alleged apparent disregard of the company's non-disclosure agreements in taking electronic documents puts her in violation of the CFAA as it is currently interpreted. Accordingly, the Court provided the plaintiff with an opportunity to amend its complaint to state this claim under the CFAA. Should the plaintiff elect to assert the CFAA claim, the Court ordered the claim stayed pending resolution of *Nosal.*

Trading Secrets

As modern computer technology continues to change the work place and how companies operate, the CFAA continues to serve as an increasingly important legal tool in preventing data theft by employees and insiders. The outcome of *Nosal* is being closely watched by employers and employees and a United States Supreme Court challenge is probably inevitable once the Ninth Circuit renders its decision.

California Federal Court Grants Summary Judgment For Facebook On Its CAN-SPAM Act, Computer Fraud and Abuse Act, And Penal Code Section 502 Claims Against Social Media Aggregator

By Robert Milligan (February 29, 2012)

For the past three years, social media platform Facebook has pursued legal action against social media aggregator Power Ventures ("Power") over what it has viewed as a blatant violation of state and federal law. Filed by Facebook in December 2008, the suit alleges violations by Power of the CAN-SPAM Act in addition to the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030) and the California Comprehensive Computer Data Access and Fraud Act (California Penal Code § 502). Facebook generally alleged that Power accessed its website in an unauthorized manner, and then utilized this unauthorized access to send unsolicited and misleading commercial emails to Facebook users.

On February 16, 2012, United States District Chief Judge James Ware of the United States District Court for the Northern District of California granted Facebook's Motions for Summary Judgment on all three counts. The Court's decision is potentially significant and groundbreaking for social media companies, like Facebook, and social media aggregators, like Power Ventures, concerning data collection by aggregators that violates social media companies' terms of service. The Court also asked for additional briefing on the amount of damages Facebook should receive and the individual liability of Power's CEO.

The decision also highlights issues regarding social media sites and spam, as well as the more significant issue of user control of their own data on social media sites. One commentator has remarked that the natural question that begs to be asked is "if Facebook users own their own data, why can't they choose the way it's accessed?" Another commentator has stated that the upshot of the decision is that "if users want to access data, they have to do so on Facebook's terms, and may not do so using a third party tool that is not a part of Facebook's developer platform. "

Power Ventures

Launched in August 2008, Power Ventures is a web service designed to offer users of multiple social platforms a one-stop solution for accessing their networks. Using login credentials disclosed by its users, Power gathers data from various sites, such as Facebook, and aggregates it on its own site. For

its part, Facebook offers its own application programming interface (API) which allows third-party developers to use Facebook user data in their applications. However, after determining that the Facebook API did not include access to all of the relevant user data they wanted, Power instead allegedly used their users' login information to access and save cached versions of Facebook pages, scraping these webpage snapshots for data. Additionally, in a "Launch Promotion," Power allegedly gathered the names of its users' Facebook friends and offered a chance at a $100 prize in return for agreeing to send them an invite to Power's service. The subsequent invitations to join were allegedly sent through Facebook's message service and used a "@facebookmail.com" address instead of a Power.com address.

CAN-SPAM Act

Passed in 2003, the CAN-SPAM Act makes it "unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading ." 15 U.S.C § 7704(a)(1). Facebook argued that Power initiated misleading messages to its users inviting them to join Power's service. Coming from the "@facebookmail.com" address, the message allegedly initiated by Power came from Facebook's servers and contained no return address where Power could be reached, nor any header information identifying Power as the initiator of the message.

As an Internet access service provider (IAS provider), Facebook is permitted to assert a cause of action (and obtain statutory damages) if it is able to establish standing under the CAN-SPAM Act, i.e. was Facebook "adversely affected" by the alleged violations. Testifying to this essential element, which the Court credited, Facebook documented its expenditures in response to Power's actions, including associated legal fees as well the cost of increased technical measures to attempt to prevent the spamming.

The Court noted that Power's spamming activity was ongoing, prolific, and did not stop after requests from the network owner. The Court reasoned that to hold that Facebook originated the emails merely because Facebook servers sent them would ignore the fact that Power intentionally caused Facebook's servers to do so, and created a software program specifically designed to achieve that effect. The Court also reasoned that the emails did not contain any return address or any address anywhere in the email that would allow a recipient to respond to Power. Thus, the Court concluded that the header information did not accurately identify the party that actually initiated the email and the header information was materially misleading. Consequently, the Court ruled in favor of Facebook, finding Power to be in violation of the CAN-SPAM Act.

Computer Fraud and Abuse Act & California Penal Code § 502

The Computer Fraud and Abuse Act is a federal law designed to, among other things, combat hacking, cracking of computer systems, and other computer-related offenses. In this case, Facebook sued Power under a subsection of the act (18 U.S.C. § 1030(a)(2)(C)) which provides that it is unlawful to

"intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[].. .information from any protected computer." Similarly, Facebook also asserted a claim under California Penal Code § 502, a state statute that aims to prevent entities and individuals from "knowingly and without permission" accessing and taking, copying, or making use of data from computers, computer systems, or computer networks. Though Power gained access to Facebook pages using login information provided by its users, the automated process by which Power obtained user data is a violation of Facebook's terms of use. As a result, Facebook argued that Power did not in fact have authorized access (under Facebook's own terms of use) to the user profiles it gathered, or the subsequent data therein, and was in violation of both § 502 as well as the CFAA.

While the Court did not agree that simply violating a network's terms of use was enough to warrant the distinction of "without permission" under § 502, it established a new standard for unauthorized access by distinguishing access which "circumvents technical or code-based barriers in place to restrict or bar a users's [sic] access." In support of this additional requirement, Facebook detailed its efforts to block Power's IP address and access, as well as the adjustment of Power's software to circumvent this measure. Additionally, Facebook pointed to emails by Power's CEO, as well as transcripts of discussions with his staff in which the CEO warns them of Facebook's potential countermeasures and the need to not be detected. Given the Power CEO's anticipation of potential blocks to Power's methods, as well as Power's actual circumvention of Facebook's IP blocks, the Court ruled that Power did in fact access Facebook's servers without permission and was in violation of California Penal Code § 502. Similarly, after crediting Facebook's showing of Power's violation of § 502 and considering Facebook's costs to attempt to thwart Power's unauthorized access, which were in excess of the $5,000 minimum damage or loss threshold mandated by 18 U.S.C. § 1030, the Court also found Power to be in violation of the CFAA.

Conclusion and Takeaways

In response to the decision, interested parties have voiced differing views. Facebook's lead litigation counsel has been quoted by Bloomberg News as saying: "We will continue to enforce our rights against bad actors who attempt to circumvent Facebook's privacy and security protections and spam people." The EFF has criticized the decision stating that the case "demonstrates the difficulties facing those who seek to empower users to interact with closed services like Facebook in new and innovative ways."

Though successful in proving that Power accessed its site without permission, Facebook's victory may be bittersweet for the social networking giant. Previously, Facebook relied heavily on its incredibly robust terms of use to safeguard itself from what it viewed as abuse of its service. Now, given the Court's standard for what constitutes access "without permission," Facebook, as well as other Internet based services, must focus even more heavily on incorporating protective measures into its website's code and allocate more resources to promptly respond to threats from outsiders like Power. Monitoring a network the size of Facebook's for unauthorized access may be a daunting technical task and the security investigation costs significant, yet failing to do so may cost even more to a service dependent upon users who may expect privacy and security. Companies that traffic in secured information should be sure to invest in comprehensive protective measures designed to keep unauthorized users out,

whatever their purpose. Crafting a comprehensive terms of use that explicitly outlines what is acceptable is still important to protecting a company from misappropriation or abuse as it helps to establish clear boundaries for authorized access. However, while a strong terms of use is necessary, it is not sufficient to gain the full protections of the CFAA and California Penal Code § 502 for social networking services, such as Facebook, at least according to this Court.

Colorado Federal Court Rules That Former Employer Stated A Claim Against Former Executive and His New Employer Under The Computer Fraud Abuse and Act Regardless Of Differing Circuit Interpretations Of The Act

By Robert Milligan (March 9, 2012)

In its order denying defendants' motion to dismiss in *SBM Site Services, LLC v. Garrett, et al.*, Case No. 10-cv-00385, a Colorado federal court identified a circuit split over the interpretation of "unauthorized access" under the Computer Fraud and Abuse Act and then found a former employer had stated a CFAA claim against a former executive and his new employer regardless of the different circuit interpretations based upon his post-termination computer activities. The case is significant because it provides employers with authority that the CFAA should apply in cases where an employee steals or destroys company data on a company computer after his or her termination.

Pertinent Allegations

In its ruling, the court laid out the pertinent allegations which it accepted as true for purpose of ruling on defendants' motion. According to the complaint, defendant John Garrett, formerly the Senior Vice President/Chief Business Development Officer at SBM, a janitorial, recycling, and moving services company, worked remotely from home using two desktop computers and two laptop computers provided to him by SBM. He used these SBM-provided devices to remotely access SBM's computer system. Prior to his move to Able, a direct competitor of SBM, Garrett allegedly had his administrative assistant download numerous SBM files from its network, had them burned to a cd, and then had them sent to him.

According to the amended complaint, on January 4, 2010 Garrett informally notified SBM that he was resigning effective January 22, 2010. SBM then informed Garrett that he would need to return all SBM property, including computers, records and other confidential information, before his departure. After failing to return the company computers at an initial meeting on January 26, 2010, SBM scheduled another meeting for January 29, 2010 to collect the items. Garrett allegedly canceled this second meeting and did not return the last of his company computers until February 16, 2010, over two weeks after starting his new job at Able. Garrett began his employment with Able on January 28, 2010 and SBM alleges that Garrett loaded SBM's confidential information onto a laptop provided to him by Able. Upon examination of the returned laptop, SBM allegedly found that the hard drive had been encrypted

to prevent access in addition to being "intentionally erased." SBM asserted several claims against Garrett and Able, including violation of the CFAA.

CFAA and Circuit Split

As with most cases where the CFAA is invoked, the question of what constitutes unauthorized access is central to the arguments made by both sides. Section 1030(a)(5)(C) of the CFAA makes it unlawful to "intentionally access[] a protected computer without authorization and as a result of such conduct, cause[] damage and loss." Garrett argued that because he was authorized to access the laptop while he was employed by SBM, he cannot have accessed the laptop without authorization.

The court acknowledged that the Tenth Circuit has yet to address what constitutes "unauthorized access" for purposes of the CFAA. The court analyzed differing interpretations of the provision made by the Seventh and Ninth Circuits.

In its interpretation of what constitutes "unauthorized access," the Seventh Circuit applied agency principles in *International Airport Centers, LLC v. Citrin* to determine that an employee's access was unauthorized from the moment he decided to quit and had undertaken actions in violation of his duty of loyalty to his employer. According to the decision, access is only authorized within the agency relationship between employer and employee. This agency relationship relies on loyalty as well as transparency, and violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship. Under the Seventh Circuit's approach, whether access to a computer was "unauthorized" depends upon the status of the agency relationship between the employer and employee.

The Colorado federal court noted that the Ninth Circuit has taken a more restrictive view of what constitutes "unauthorized access" for purposes of the CFAA. In *LVRC Holdings LLC v. Brekka,* the Ninth Circuit determined that "authorization" depends on actions taken by the employer and "[i]f the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA." In other words, unless an employer rescinds an employee's right to use or access a computer, the employee arguably has authorized access to all systems and files within the scope of their position. Thus, the onus is on the employer to end an employee's right to access by explicitly informing them of such. It is notable that the Colorado federal court's decision does not address the exceeds authorized access section of the CFAA, which provides an alternative theory of liability under the CFAA. An en banc panel of the Ninth Circuit is presently considering that section in *U.S. v. Nosal* and will issue a decision soon.

Colorado Federal Court's Analysis: Post-Termination Activities Key

Forgoing to determine which circuit interpretation to follow, the Colorado federal court ruled that SBM had stated a claim under the CFAA under either standard. Since Garrett allegedly accessed SBM's protected computer systems both after he had decided to quit as well as after he was asked to return all computer equipment, the court found that SBM did in fact have a valid claim for violation of the CFAA. The court reasoned that SBM had notified Garrett that he was required to return all company

property at the time he ended his employment. SBM explicitly revoked Garrett's access to the laptop as of his last day as an employee. He allegedly failed to return his equipment, including a laptop, on his last day and canceled a follow up meeting to collect the equipment. He retained the laptop for approximately three weeks after he terminated his employment. When he returned the laptop, it had allegedly been intentionally erased. The court found that it was reasonable to infer that Garrett accessed the laptop after his last day of employment. The court distinguished cases cited by defendants that Garrett's access was not "unauthorized" because they involved the use or alleged misuse of computer provided equipment during the duration of defendant's employment. In this case, Garrett allegedly retained Plaintiff's laptop for three weeks after his employment ended, including more than two weeks after he started his employment with Able.

The court reasoned that there can be no question that, under either the Seventh or the Ninth Circuit's interpretation of "unauthorized access," Garrett's access to the laptop became unauthorized when his employment ended and SBM requested the return of the laptop. The court also found that SBM had stated a claim against Able. The court found that Garrett was an agent of Able and it was reasonable to infer that Garrett accessed SBM's laptop during the time that he was employed with Able and in the scope of such employment.

Takeaways

With computer access becoming an integral and essential aspect of conducting business in the modern world, issues dealing with how employees access and utilize a company's computer resources are very important, and companies must employ clear and conspicuous computer usage policies with employees, including contractual agreements to return all company property upon termination, in order to effectively protect company property and data. Company computer log-in prompts should remind employees of their obligation to follow computer usage policies. Companies should consider clearly defining when an employee's computer access is without authorization, exceeds authorization, and is without permission, and only permit the employee access to computer data and servers which is essential to perform their job functions. Lastly, should there be any delay in the return of a company computer upon termination of an employee who may pose a threat to company data security, companies should consider having the computer forensically imaged to detect any computer fraud or abuse by the employee. If any is detected, this new federal decision indicates that the employer may have a viable CFAA claim against the employee.

Minnesota District Court Dismisses Computer Fraud and Abuse Act Claim Brought Against Former Employee Based Upon Narrow Interpretation Of Act

By Robert Milligan and Joshua Salinas (March 21, 2012)

In another decision that underscores the circuit split regarding the interpretation of the Computer Fraud and Abuse Act's (CFAA) language on authorized access, the Honorable Judge David Doty of the United States District Court for the District of Minnesota has dismissed an employer's claim that its former employees violated the Act. The case, *Walsh Bishop Associates, Inc. v. O'Brien*, CIV. 11-2673 DSD/AJB, 2012 WL 669069 (D. Minn. Feb. 28, 2012), concerns three former officers of the Minneapolis based architectural firm Walsh Bishop. The court held that since the defendants had authorized access to all of the electronic files they purportedly took, they could not be liable under the CFAA for their use or misuse of the files.

According to the court's decision, Keith O'Brien, Ian Scott, and David Serrano sat on Walsh Bishop's executive committee and had "access to the highest level of confidential and proprietary information of [Walsh Bishop]." In June 2011, the three incorporated a separate entity, also a named defendant, WBA Partners, Inc. The three allegedly used WBA Partners, Inc. name on a $7 million proposal while still working at Walsh Bishop. Additionally, in August 2011 Scott allegedly sent a Walsh Bishop customer list to his personal email and Serrano allegedly sent a drawing he had prepared for Walsh Bishop to his personal email.

All three purportedly met with competing firms during this time about switching firms and bringing their clients with them. Thereafter, defendants' employment with Walsh Bishop terminated at an unknown date. Walsh Bishop subsequently sued defendants claiming a violation of the CFAA and a variety of other state and federal statutes, in addition to common law claims.

Walsh Bishop's CFAA claim specifically referenced Section 1030(a)(2) of the Act, which holds a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from a protected computer" liable for imprisonment and a fine. Although the CFAA is largely a criminal statute, an amendment to the Act passed in 1994 allows its application in civil suits.

Walsh Bishop contended that Scott and Serrano violated the CFAA when they emailed company documents to themselves "in a manner contrary to [Walsh Bishop's] interests and use policies." Walsh Bishop derived its argument from the Ninth Circuit case *United States v. Nosal,* which expanded the interpretation of "exceeds authorized access" to include violations of a company's "computer access restrictions - including use restrictions." (*United States v. Nosal*, 642 F.3d 788 (9th Cir. 2011), reh'g en banc granted, No. 10–10038, 2011 WL 5109831 (9th Cir. Oct. 27, 2011)). *Nosal* departed from the Ninth Circuit authority determined "authorization" based on the actions taken by the employer. (See e.g., *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In *Brekka*, the Ninth Circuit

narrowly interpreted the CFAA and placed the onus on the employer to explicitly rescind the employee's right to use or access a computer.

The defendants moved to dismiss Walsh Bishop's CFAA claim on grounds that Walsh Bishop authorized their computer access "at the highest levels," and, thus they could not exceed authorized access.

In his decision to grant Defendant's motion to dismiss, the court noted that the Eight Circuit has yet to determine whether the CFAA imposes civil liability on employees who access information with permission but for an improper purpose. The court cited several Minnesota District Court cases that adopted a more narrow view of the CFAA that *focused on the scope* of access rather than misuse or misappropriation of information. The court found that this narrow interpretation correctly applied the language and purpose of the statute more than Nosal.

First, the court highlighted the plain language of the section 1030(a)(2), which concerns access and not the use of information. He stated that had Congress intended to target use of information, it would have included the appropriate language. (See e.g. § 1030(a)(1)).

Second, the court stated that the legislative purpose and history support the plain meaning of the statute because Congress enacted the CFAA to apply to persons who abused computer technology without access. The court emphasized that Congress never intended to provide a federal cause of action for state-law breach of contract, trade secret, or other business-tort claims.

Finally, the court addressed Walsh Bishop's argument that the defendants' acts were unlawful because they violated Walsh Bishop's computer-use policies. The court first explained that he could not consider the computer-use policy because Walsh Bishop failed to attach the policy in its complaint. The court stated that even if he considered the computer-use policy, the policy only proscribed *certain uses* of information, not defendants' *scope of access*. The court highlighted the fact that Walsh Bishop granted defendants broad access to its computer systems and expressly granted access to the areas of the systems it alleged defendants used with an improper purpose. Therefore, since the defendants had access to all of the files they purportedly took, the court ruled that they cannot be held liable under the CFAA for their use or misuse of said files.

Walsh Bishop is unfortunately at the mercy of court's decision to use the more narrow interpretation of the CFAA, similar to the Ninth's Circuit interpretation in *Brekka*, over the more employer friendly precedent established by the Seventh Circuit in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) and the Ninth Circuit in *Nosal.*

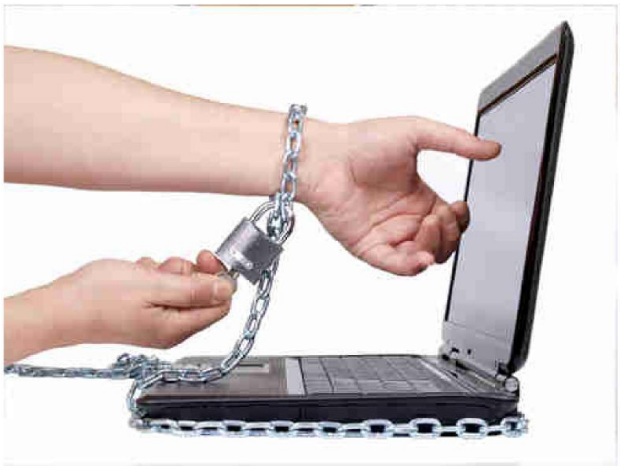
Although Walsh Bishop implemented explicit computer and data use restrictions, its policies restricted only employees' use of information and not access to information. This alleged deficiency subjected Walsh Bishop's claim to the court's interpretation of the statutory language of the CFAA and corresponding circuit split.

Lastly, the court declined to exercise supplemental jurisdiction over Walsh Bishop's remaining state-law claims, but dismissed the claims without prejudice so that Walsh Bishop could bring an action in Minnesota state court.

This case is important because it reminds companies to be vigilant in advancing their own computer use and access restriction policies at every opportunity. Employers should implement policies that explicitly define both the employee's access to information and the appropriate use of information. In addition to a comprehensive and clear computer use and access policies, companies should consistently remind employees of their duty to adhere to such policies. For example, this can be done through a prompt that appears whenever the employee logs on to a protected computer system. This constant reminder can go a long way in discouraging any behavior not in the best interests of a company and provide evidentiary support should the employer need later to sue the employee for violation of the CFAA or similar state laws.

Ninth Circuit En Banc Panel Tells Employers That Computer Fraud and Abuse Act Is Only To Combat Hacking, Not Employee Trade Secret Misappropriation: United States Supreme Court May Need To Resolve Circuit Split

By Robert Milligan (April 20, 2012)



On Tuesday, April 10, 2012, a Ninth Circuit en banc panel released its highly anticipated decision in *United States v. Nosal* and affirmed the judgment of the district court dismissing criminal counts against a former employee of a headhunter firm accused of violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq. by conspiring with employees of the former employer to log on to the employer's confidential database and send proprietary files to a competitor.

The opinion, authored by Chief Judge Alex Kozinski, and supported by a majority of the 11-judge court, made the following general statements in its introduction:

> Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website?
>
> This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

The Court then went on to reject the federal government's interpretation of the CFAA, finding that the statute was meant to punish hacking, not misappropriation of trade secrets. To find otherwise, Judge Kozinski reasoned would "criminalize any unauthorized use of information obtained from a computer" and "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."

"Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights," Kozinski wrote. "Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you could be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement."

The Court acknowledged that the Eleventh, Fifth, and Seventh Circuits permit employers to pursue CFAA claims against employees who violate computer use policies or violate duties of loyalty to their employer. The Court reasoned though:

> "We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty. See *United States v. Rodriguez,* 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid "making criminal law in Congress's stead." *United States v. Santos*, 553 U.S. 507, 514 (2008).
>
> We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead. For our part, we continue to follow in the path blazed by *Brekka*, 581 F.3d 1127, and the growing number of courts that have reached the same conclusion.

The Ninth Circuit concluded that because Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of "without authorization, or exceeds authorized access" under 18 U.S.C. § 1030(a)(4).

Because Nosal's alleged accomplices had permission to access the company database, they did not "exceed authorized access" under the CFAA, the Court held. "The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations," Kozinski added. "But we shouldn't have to live at the mercy of our local prosecutor."

In a powerful dissent, Judge Barry Silverman wrote:

> This case has nothing to do with playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything

> to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts. The indictment here charged that Nosal and his co-conspirators knowingly exceeded the access to a protected company computer they were given by an executive search firm that employed them; that they did so with the intent to defraud; and further, that they stole the victim's valuable proprietary information by means of that fraudulent conduct in order to profit from using it. In ridiculing scenarios not remotely presented by this case, the majority does a good job of knocking down straw men - far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy.
>
> The majority also takes a plainly written statute and parses it in a hyper-complicated way that distorts the obvious intent of Congress. No other circuit that has considered this statute finds the problems that the majority does.

It remains to be seen whether the federal government will seek Supreme Court review. There is clearly a circuit split on this important issue. While purportedly committing a federal crime by violating a company's computer policies by playing sudoku or watching March Madness seems laughable, the majority's decision leaves employers in the Ninth Circuit, and particularly California, with less options than those in other circuits that recognize CFAA claims (both civil and criminal) for wrongful access of company computers to steal company data for competitive purposes. We will provide additional insight on the implications of the Court's decision in later posts. As a preliminary matter, companies operating in the Ninth Circuit should reevaluate the scope of access that they provide their employees on their computer systems and limit access to highly valuable information to only those who need to know.

New York Federal District Court Strikes Down Application of the Computer Fraud and Abuse Act to ISP Throttling Case

By Robert Milligan (April 26, 2012)

As Internet traffic has exploded in the last decade, Internet Service Providers (ISP) - the companies who build and profit from providing the requisite infrastructure - have had to strategically maintain their networks to satisfy demand under increasingly tightening technological constraints. One way ISPs do this is by employing a practice called "throttling," or limiting heavy users' access to Internet servers to free up bandwidth for others. When one subscriber to an ISP's service makes heavy demands to the network, such as downloading large amounts of videos, other users in the area suffer from decreased speed; throttling is one way of preventing this sort of problem. ISPs typically reserve their right to throttle in their terms and of service with customers.

While ISPs argue that throttling is a necessary practice, others argue that it amounts to the arbitrary limiting of access to a vital communications tool by a corporate entity and constitutes a dangerous overreach of power. Left without regulatory recourse, net neutrality advocates - or those opposed to the practice of throttling - have turned towards the application of other laws in their battle against ISP throttling.

In *Serrano v. Cablevision Systems Corp.*, No. 09-CV-1056 (DLI) (MDG), a class action suit filed in the United States District Court for the Eastern District of New York, Plaintiffs Alyce Serrano and Andrea Londono alleged violations of the Computer Fraud and Abuse Act (CFAA) as well as various state law claims in relation to ISP throttling. According to their complaint, ISP Cablevision "wrongfully limited Plaintiffs' use of certain peer-to-peer ("P2P") applications without authorization, and thereby caused damage to Plaintiffs' computers." Specifically, Plaintiffs cited 18 U.S.C. § 1030(a)(5)(A)-(C), a section of the CFAA related to damages caused by "the transmission of a program, information, code, or command...without authorization" or "intentionally access[ing] a protected computer without authorization."

The first key to successfully arguing a violation of the CFAA is proving that any access or action to a protected computer system was done "without authorization." To Cablevision's credit, Serrano and Londono both signed "Terms of Service" and "Acceptable Use Policy" documents at the time of their service installation and after subsequent work orders. These documents included provisions for

Cablevision to reserve “the right to protect the integrity of its network and resources by any means it deems appropriate. This includes but is not limited to...putting limits on bandwidth.” The agreements also allow them to do so “without prior notification.”

The Court found that Plaintiffs’ claims arising under the CFAA were “defeated by the clear language of the Terms of Service and the Acceptable Use Policy.” The Court found that based on Plaintiffs’ assent to these valid and enforceable provisions, “Plaintiffs cannot now claim that Cablevision acted ‘without authorization’ when it re-stricted their bandwidth.”

Although Serrano and Londono argued that these contracts were vague and ambiguous and should not be considered valid, the Honorable Judge Dora L. Irizarry ruled that they were in fact proper and could be dutifully enforced. Judge Irizarry cited New York law related to agreements made over the internet, or so-called “click-wrap” contracts, in ruling them valid “as long as the consumer is given a sufficient opportunity to read the...agreement, and assents thereto after being provided with an unambiguous method of accepting or declining the offer.” As all such requirements were met in Cablevision’s case, Judge Irizarry ruled that the contracts, and therefore Cablevision’s right to authorized access of Plaintiffs protected computer systems for the purposes of throttling, were in fact legal and granted Cablevision’s motion for summary judgment.

For all of its wide-ranging applicability to legal matters in the digital space, the CFAA does not appear to be of much use in preventing ISP throttling. Arguing that an ISP does not have authorized access to regulate its own networks may be nearly impossible to assert given their financial right to the infrastructure as well as their responsibility to protect its functionality for all users. Coupled with the robust Terms of Service and Acceptable Use Policies likely employed industry wide, ISPs are not likely to be vulnerable to this type of CFAA claim.

It will be interesting to see how the issue of ISP throttling is addressed in future cases and possible legislation. ISPs argue that if they are not allowed to throttle heavy users, all users will eventually suffer from a decrease in Internet speed. As more Internet users trend towards heavy use, the problems may become more pronounced over time. With ISPs struggling to build out next generation networks to handle increased usage, costs could be passed on to consumers in new forms, including multi-tier pricing systems based on bandwidth usage similar to those being introduced by cellular data carriers. While the vast majority of Americans may never be subject to bandwidth throttling, the latitude ISPs are given in establishing this practice will set the stage for how ISPs are able to regulate the networks of tomorrow.

U.S. v. Nosal Update: Solicitor General and DOJ Still Deciding Whether To File Writ Of Certiorari With United States Supreme Court

By Robert Milligan (May 9, 2012)

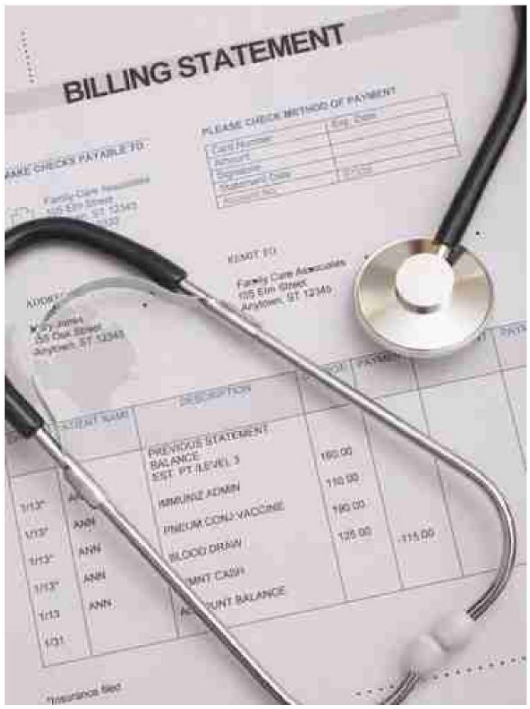
According to a recent filing with the California federal district court in the *United States v. Nosal* case, the Solicitor General, in consultation with the Criminal Division of the Department of Justice and the United States Attorney's Office, is still deciding whether to file a writ of certiorari with the United States Supreme Court.

The writ would challenge the Ninth Circuit's recent decision in the case which circumscribes the use of the Computer Fraud and Abuse Act to primarily hacking activities, rather than violations of employer computer usage policies or internet service providers' terms of service/use, and request that the Supreme Court resolve the current circuit split. We previously discussed the Court's decision and its impact. Other legal commentators such as John Marsh, Ken Vanko, and Nick Akerman have weighed in on the decision. The parties' stipulation indicates that the government's deadline to file the writ is July 9, 2012.

Should your company be interested in taking a side in the dispute, including joining a letter to the Solicitor General or participating in an amicus filing, please contact your Seyfarth attorney contact or submit your interest here.

Michigan Federal Court Adopts Narrow Interpretation of Civil Liability Under Computer Fraud and Abuse Act

By Robert Milligan (May 30, 2012)



The U.S. Circuit Courts of Appeals are currently split over how broadly the Computer Fraud and Abuse Act ("CFAA") should be interpreted. A recent decision out of the Eastern District of Michigan highlights this split and examines the ways in which the courts have interpreted the statute before deciding to adopt a narrow interpretation of civil liability under the CFAA.

On May 14, 2012, Judge Marianne O. Battani of the Eastern District of Michigan decided the case of *Ajuba International, LLC v. Saharia*. As a condition of his employment, Mr. Saharia, the defendant, signed an employment agreement with the plaintiffs, along with a non-compete agreement prohibiting him from competing with Ajuba International or soliciting any of its employees. Once the agreement expired, Saharia entered into a new agreement with Ajuba International's subsidiary, Ajuba India. Under the terms of this agreement, Saharia acted as Ajuba India's president. Unbeknownst to the plaintiffs, however, at the same time, Saharia had established his own company, AGS India, to compete directly with their company. Allegedly, Saharia then hired multiple key management personnel from AGS India, interfered with the plaintiffs' business relationships to advance his own interests, and misappropriated trade secrets and other confidential information. The plaintiffs sued in federal court alleging a number of causes of actions, including a violation of the CFAA.

The dispute between the parties over whether a CFAA violation actually occurred highlights an ongoing circuit split over the statute's prohibition of unauthorized use. Under the CFAA (18 U.S.C. §1030(a)(5)(c)), it is a crime for a current or former employee to intentionally access a protected computer issued or owned by their employer "without authorization" or in a manner that "exceeds authorized access" leading to damage and loss. However, how the phrases "without authorization" and "exceeds authorized access" are interpreted varies between the circuits.

Some courts, including the Ninth Circuit, have construed the terms of the statute in a narrow manner. In *LVRC Holdings L.L.C. v. Brekka*, the court found that an employee's misuse or misappropriation of an employer's confidential or proprietary information is not "without authorization" as long as the employer has given permission to the employee to access this information. Similarly, federal district courts in the

Southern District of New York and the District of Arizona, adopted narrow approaches in *Orbit One Communications v. Numerex and Shamrock Foods Co v. Gast*, respectively. In both cases, the courts held that the CFAA prohibits improper access of computer information, but did not prohibit misuse or misappropriation. As such, once an employee receives authorization to access the employer's computer, he or she does not violate the CFAA if he proceeds to subsequently use that information improperly.

By contrast, other courts, including the First, Eleventh, Fifth and Seventh Circuit, have interpreted the CFAA more broadly, finding that it prohibits violations of an employer's computer use restrictions, or a breach of the employee's duty of loyalty to the employer, which stems from the agency doctrine. Under this approach, "an employee accesses a computer without authorization whenever, without the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty." *Guest-Tek Interactive Entm't, Inc. v. Pullen*, 665 F. Supp. 2d 42, 45 (D. Mass. 2009).

In examining this particular case, Judge Battani found that the Sixth Circuit has yet to address the meaning of either "without authorization" or "exceeds authorized access" within an employment context, however, in other contexts, the court had taken the narrow approach. Similarly, two separate district courts within the Sixth Circuit had both confronted the circuit split, and each had adopted the narrow approach. As such, Judge Battani chose to adopt the narrow approach in this case, finding that even if misappropriation occurred, because the initial access was authorized, it was not in violation of the CFAA.

Judge Battani relied on three main principles in adopting the narrower interpretation of the CFAA: first, the legislative history was consistent with such a finding; second, the statutory canon of avoiding absurd results and the rule of lenity find in favor of such a holding; finally, the plain meaning of the statute compels a narrow interpretation. Similarly, the court's holding suggests that the broader interpretation is not based on statutory authority suggesting that misappropriation is included under the CFAA, nor is there any reason to suggest that Congress intended to interpret the CFAA so broadly as to convert a violation of the duty of loyalty into a federal offense.

The Solicitor General is presently deciding whether to seek Supreme Court review of the Ninth Circuit's decision in *U.S. v. Nosal*, which reached a similar result as Judge Battani in *Ajuba International, LLC v. Saharia.*

U.S. v. Nosal Update: Solicitor General Still Deciding Whether To Seek Supreme Court Review of Important Ninth Circuit Computer Fraud and Abuse Act Decision

By Robert Milligan (July 12, 2012)

The Solicitor General obtained a thirty day extension on the July 9, 2012 deadline to file a petition for a writ of certiorari with the United States Supreme Court on the Ninth Circuit's controversial *U.S. v. Nosal* decision, which limits the use of the federal Computer Fraud and Abuse Act. According to the extension request, the Solicitor General "has not yet determined whether to file a petition for a writ of certiorari in this case. The additional time sought in this application is needed to assess the legal and practical impact of the court's ruling and, if a petition is authorized, to permit its preparation and printing."

A writ petition would challenge the Ninth Circuit's recent decision which circumscribes the use of the Computer Fraud and Abuse Act to primarily outsider hacking activities, rather than violations of employer computer usage policies or internet service providers' terms of service/use, and request that the Supreme Court resolve the current circuit split. We previously discussed the Court's decision and its impact.

Should your company be interested in taking a side in the dispute, including joining a letter to the Solicitor General or participating in an amicus filing, please contact your Seyfarth attorney contact or submit your interest here.

Another Michigan Federal Court Adopts Narrow Interpretation of Civil Liability Under Computer Fraud and Abuse Act

By Paul E. Freehling (July 24, 2012)

A U.S. District Court in Michigan recently granted partial summary judgment in favor of two individuals who were sued by their former employer, Dana Ltd., for violating the Computer Fraud and Abuse Act, 18 U.S.C. §1030 *et seq.*

The individuals admitted that, prior to their departure from Dana but after accepting employment with a competitor, they accessed and copied numerous Dana files and then erased or obliterated the files they had copied. Notwithstanding contrary authority, the court held that the CFAA only prohibits unauthorized access to an employer's confidential data, regardless of motive, and the employees had the right to access Dana's secret information. The CFAA also prohibits unauthorized alteration of computerized data, but the judge ruled that Dana failed to prove that it permanently lost significant information. Further, it was held that only officers and directors have a fiduciary duty to their employer, and these employees were neither officers nor directors. *Dana Ltd. v. American Axle & Mfg. Holdings, Inc.*, Case No. 1:10-CV-450 (E.D.Mich., June 29, 2012).

Reviewing inconsistent federal court decisions as to whether the CFAA is violated by an employee who, though authorized to access confidential information, does so for personal reasons, the court sided with the opinions emphasizing that the statute addresses only unauthorized access and says nothing about an employee's motive. Additionally, the court said leniency toward employees is required since the CFAA is primarily a criminal statute. Thus, the ruling on summary judgment was favorable to the employees. The ruling is also consistent with another Michigan district's court decision on the issue that we previously blogged on.

The CFAA also prohibits unauthorized alteration of information stored in a computer. However, Dana backed up its files. It also allowed and/or required employees to delete or destroy duplicate copies of documents taken and not returned, and arguably that is what the individuals did. Moreover, the individuals denied destroying, and Dana had no evidence that they destroyed, either original files or information of importance.

Dana was successful in defeating summary judgment motions directed to its allegations that the individuals breached their confidentiality agreements and misappropriated Dana's trade secrets and

that their new employer committed unfair competition and tortious interference. Contested issues of material facts prevented a pre-trial determination of these claims.

Sooner or later (unless Congress intervenes first), the U.S. Supreme Court will have to resolve the split among federal appellate courts regarding the CFAA's scope – that is, whether an employee's authorization to access the employer's computer system automatically terminates when the system is used to injure the employer or contrary to computer usage policies. The Fifth, Seventh, and Eleventh Circuits have found liability under those theories. One wonders what the Supremes will make of it all and whether they will again overturn their friends from the Ninth Circuit.

Solicitor General Decides Not To File Petition For Review In *United States v. Nosal*: Circuit Split On Computer Fraud And Abuse Act Remains

By Robert Milligan and Joshua Salinas (August 3, 2012)

The Solicitor General indicated yesterday that he will not file a petition for a writ of certiorari with the Supreme Court in *U.S. v. Nosal.*

It was anticipated by some legal commentators that a Supreme Court decision in *Nosal* may resolve a deepening split between the Circuit Courts regarding the proper interpretation of the statutory language in the Computer Fraud and Abuse Act (CFAA) and its applicability to factual scenarios where employees steal company data in violation of computer usage policies or in breach of their loyalty obligations.

Earlier this spring, a Ninth Circuit en banc panel in *Nosal* adopted a narrow interpretation of the CFAA and found that an employee's violation of his/her employer's computer usage policies was not a violation of the CFAA. The Court focused on whether the employee originally had access to the information, not whether the employee misused the employer's confidential information in violation of usage policies.

Last week, the Fourth Circuit in *WEC Carolina Energy Solutions v. Miller* joined the Ninth Circuit and adopted this narrow interpretation of the CFAA. Please see John Marsh's and Ken Vanko's blogs on the case.

On the other side, the Fifth, Seventh, and Eleventh Circuits have adopted a broader interpretation of the CFAA based on either common-law agency principles or computer usage policies. Under the agency theory, when an employee accesses a computer to further interests adverse to the employer, such actions terminate his or her agency relationship and, thus the employee loses any authority to access the computer. Under the computer usage theory, a violation of a computer usage policy can serve as a basis for holding an employee liable under the CFAA, Thus, an employee who is authorized to access a company computer, but uses that access to steal or damage valuable company data in violation of a computer usage policy, would be liable for his or her wrongful conduct.

The Supreme Court has yet to decide a CFAA case since the statute's inception in 1984. With the Solicitor General refraining from filing a petition in *Nosal,* a resolution of the circuit split may lie with a

statutory fix by the legislature or possible review of the Fourth Circuit's decision in *WEC Carolina Energy Solutions v. Miller.* No such fix, however, appears imminent.

Earlier this week, Senator Patrick Leahy (D-VT) proposed an amendment to the Cybersecurity Act of 2012 (S3413), that would in effect adopt the Ninth Circuit's narrow interpretation of the CFAA.

Yesterday, the cybersecurity bill failed to obtain the required amount of votes required to move the legislation forward. With Congress on August recess and its focus turning towards the upcoming November elections, any cybersecurity legislation is not expected to be voted on until next year.

As of now, an employer's protection under the CFAA against rogue employees that steal valuable company data may simply depend on which jurisdiction they are in and/or the genius of counsel.

Employers Beware: Fourth Circuit Adopts Narrow Interpretation of Computer Fraud and Abuse Act

By Jessica Mendelson (August 6, 2012)

On July 26, 2012, the Fourth Circuit Court of Appeals decided *WEC Carolina Energy Solutions LLC v. Miller,* holding that departing employees are not liable under the Computer Fraud and Abuse Act ("CFAA") for mere violations of a company computer use policy. The Fourth Circuit's decision solidifies the circuit split on whether employees who violate computer use policies and/or engage in disloyal conduct by stealing company data can be liable under the CFAA.

Mike Miller was an employee of WEC Carolina Energy Solutions ("WEC"). During his employment, Miller was provided with a computer and cell phone from which he could access the company's intranet which housed confidential, proprietary, and trade secret information. Prior to resigning in 2010, Miller allegedly downloaded a number of confidential documents, which he then proceeded to email to himself. Miller began to work for a competitor, Arc Energy Services ("Arc") and allegedly used WEC's confidential information in a sales presentation for them. WEC's computer use policies, which Miller had agreed to comply with as part of his employment, prohibited employees from downloading confidential and proprietary information to a personal computer. Based on his actions, WEC sued Miller, alleging that he had violated the CFAA.

The U.S. District Court for the District of South Carolina held that the violation of company usage policies regarding the downloading and use of confidential and proprietary information did not on its own violate the CFAA. WEC appealed to the Fourth Circuit, which affirmed the District Court's holding. According to the Fourth Circuit, the CFAA prohibits unauthorized acts of altering and obtaining information from a protected computer. In this case, however, Miller had permission to access the information at the time he downloaded it. As a result, his later use of the information was not in violation of the CFAA.

In holding that Miller's actions did not violate the CFAA, the Fourth Circuit partially agreed with the Ninth Circuit's *Nosal* ruling, which has been previously covered by this blog. The Fourth Circuit criticized the previously vacated three-judge panel opinion in Nosal, stating that even under that interpretation, an employee could not be found liable for permissibly accessing information and using that information in an impermissible manner. The Fourth Circuit also declined to follow the Seventh Circuit, which had previously held in *International Airport Centers LLC v. Citrin* that employees who access company computers in violation of their fiduciary duties to the company violate the CFAA.

In its holding, the Fourth Circuit utilized a strict construction approach. Judge Floyd found that the CFAA was "primarily a criminal statute designed to combat hacking," and as such, civil liability should be limited. The court defined the phrase "exceeds authorization" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." Similarly, "without authorization" is "when an individual gains admission to a computer without approval," while "exceeds authorized access" meant the individual has approval to access a computer but his access. . . falls outside the bounds of his approved access." In this case, the court found neither definition applied to Miller's conduct, since all he had done was improperly use information that was validly accessed during his employment.

John Marsh has astutely pointed out on his blog that there may still be some life left in the CFAA for employers. The Fourth Circuit concluded that an employee "exceeds authorized access" when he has approval to access a computer but uses that access to obtain or alter information outside the bounds of his approved access. Applying these definitions, the Fourth Circuit found that WEC did not forbid Miller's "use" of information that was validly accessed in the first place. Marsh questions whether the result may have been different if the policy had forbid accessing information for purposes other than furthering WEC Carolina's business.

The Fourth Circuit's decision, along with the recent Ninth Circuit decision in *Nosal*, substantially limits the use of the CFAA against departing employees. It will be interesting to see if Supreme Court review is sought. We will continue to keep you apprised of future developments in the rapidly changing CFAA landscape.

California Federal District Court Distinguishes Ninth Circuit's Nosal Decision and Finds that Computer Fraud and Abuse Act Claims Are Available for Violations of Employers' "Access" Restrictions

By Johaua Salinas (August 14, 2012)

On June 19, 2012, a district court for the Northern District of California distinguished the Ninth Circuit's recent *U.S. v. Nosal* decision and allowed an employer to bring a claim under the Computer Fraud and Abuse Act ("CFAA") against a former employee for alleged violations of a verbal computer access restriction. (*Weingand v. Harland Financial Solutions*, 2012 U.S. Dist. LEXIS 84844 (N.D. Cal. June 19, 2012). The decision alleviates some of restraints imposed by Nosal on employers who want to bring CFAA claims against departing employees that steal valuable company data.

Plaintiff Michael Weingand worked as a Senior Field Engineer at Defendant Harland Financial Solutions. On November 4, 2010, Harland notified Weingand that it was terminating his employment. The next day, after learning of the termination of his employment, Weingand allegedly emailed Harland's H.R. Manager, requesting permission to copy his "personal files" on his Harland laptop to a USB flash drive. Harland agreed and let him access his Harland laptop at Harland's offices on November 6, 2010 at approximately 1:00 p.m.

Weingand later brought action against his former employer Harland for wrongful termination and employment retaliation.

During discovery, Harland learned through computer forensic analysis that Weingand allegedly accessed and copied over 2,700 business files belonging to Harland, its clients, and third-party software vendors; some files containing confidential, proprietary, and copyrighted information. Harland also discovered that Weingand's alleged unauthorized access of these files allegedly occurred on November 6, 2010 between 1:11 p.m. and 1:41 p.m.–the same date and time Harland gave Weingand permission to copy his personal files from his old work computer.

In light of these alleged facts, Harland moved to amend its answer to add counterclaims against Weingand for, inter alia, violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

Weingand opposed Harland's motion on grounds that, inter alia, Harland's CFAA counterclaim would be futile and subject to a motion to dismiss. In particular, Weingand contended that Harland handed the

computer to Weingand without restriction. Moreover, Weingand contended that Harland's proposed CFAA counterclaim contained no allegations as to what directions, limitations, or restricted authorization were stated to Weingand when we was handed the computer. Further, Weingand argued that Harland's "verbal authorization" regarding access to only personal files was irrelevant because the only authorization which the statute speaks is "code" authorization (i.e. whether someone is literally blocked from certain files by some security measure such as a password).

The Court rejected Weingand's arguments, granted Harland's motion, and allowed Harland to amend its answer to add the CFAA counterclaim. The Court reasoned that "[Weingand] received permission to access Harland's computer system based on his representations that he wanted to get his 'personal files' after his termination, but he had no authority with respect to the additional files he accessed." "Thus, the counterclaim creates at least a reasonable inference that his authorization extended only to accessing and copying said 'personal files' and that he exceeded that authorization." *Weingand*, 2012 U.S. Dist. LEXIS 84844, *6.

This post-*Nosal* decision has several significant takeaways:

(1) Computer access restrictions/policies may remain viable for CFAA claims in the Ninth Circuit post-*Nosal*

One of the important holdings from Nosal was that violations of an employer's computer use policy do not constitute violations under the CFAA. Weingand recognized, however, that *Nosal* precluded applying the CFAA to violating restrictions on use, but not rules regarding access. In fact, Weingand allowed a claim under the CFAA based on the employer's mere verbal restriction on access (i.e. that the employee could only access personal files). This holding remains consistent with the Ninth Circuit's prior decision in *LVRC Holdings LLC v. Brekka*: "The plain language of the statute therefore indicate that authorization depends on actions taken by the employer." Thus under *Weingand*, an employer's computer access policies may remain viable post-*Nosal* to bring CFAA claims against employees that violate those policies and steal company data.

(2) Physical access to a computer does not equal "authorization"

The mere fact that an employee is granted physical access to a computer does not necessarily mean the employee is immune to CFAA claims. The Court rejected Weingand's argument that he had "authorization" simply because he had physical access to the computer. The Court noted that while the Nosal opinion uses the phrase 'physical access,' "[*Nosal*] was concerned only with the distinction between access and use, not any distinction between different types of authorization pertaining to access." The Court went on: "Indeed, *Nosal* ... suggests that one need not engage in such rigorous technological measures to block someone from accessing files in order to limit their authorization." Thus, an employer can communicate its computer access restrictions to employees and remain protected under the CFAA, without having to physically block certain files every time that employee's authorizations change.

This also remains consistent with *Brekka*, where the Ninth Circuit stated that if a former employee accesses information without permission, even if his prior log-in information is still operative as a technical matter, such access would violate the CFAA.

While *Nosal* substantially limits employers' use of the CFAA against departing employees that steal company data, it may not be as broad of a limitation as anticipated.

Weingand has since moved to dismiss Harland's CFAA counterclaim pursuant to FRCP Rule 12(b)(6). The hearing is set for August 31, 2012. We will follow the decision to see if the Court provides any further discussions regarding Nosal, the CFAA, and employers' use of the CFAA to stop data theft by employees.

Federal Court Clerk Arrested For Allegedly Sharing Confidential Information With Gangs

By Jessica Mendelson (August 28, 2012)

In a shocking scandal, a federal court clerk has been accused of leaking confidential files, including information disclosing details of contemplated law enforcement raids on Armenian street gangs.

As reported by the ABA, Nune Gevorkyan ("Gevorkyan"), a district court criminal intake clerk, and her husband, Oganes Koshkaryan ("Koshkaryan") were arrested and charged with conspiring to obstruct justice, a violation of Title 18, United States Code Sections 371 and 1512. The charges were filed in the US District Court for the Central District of California, and if convicted, both face up to twenty years in prison.

The Eurasian Organized Crime Task Force (EOCTF), a law enforcement group comprised of nine different local law enforcement agencies in Los Angeles County, as well as the FBI, U.S. Secret Service, and the U.S. Immigration & Customs Enforcement, first initiated an investigation of several high profile members of the Armenian Power gang in 2006. The Armenian Power gang, an organized crime syndicate which primarily includes members of Armenian descent, is believed to be involved in a variety of criminal activities, including kidnapping, extortion, bank fraud, identity theft, credit card fraud, distribution of narcotics and various other criminal acts.

The FBI alleges that Gevorkyan accessed sealed indictments prior to February 2011 raids across Southern California which led to the arrests of over 70 associates of the Armenian Power gang. After looking at the indictments Gevorkyan allegedly passed the information on to her husband, Oganes Koshkaryan ("Koshkaryan"). Koshkaryan allegedly acted as an intermediary, promising clients he could get confidential information from the courts in exchange for cash.

The FBI first learned of the leaks after a defendant who was seeking a reduced sentence informed them that the raids were known to some of the gang members who were arrested. The cooperating defendant told the FBI that he had fled his home prior to the arrests because of the information Koshkaryan allegedly had provided to him. The defendant later surrendered. A second defendant also fled for his or her safety based on Koshkaryan's alleged information.

On at least two occasions, Koshkaryn alleged delivered information from the sealed court records to an FBI informant. This past month, the informant allegedly asked Koshkaryan about a person currently

under investigation, and was told the person would be arrested soon. Koshkaryan provided additional information regarding another defendant, and was paid $2000. Record searches completed by FBI allegedly confirmed that Gevorkyan had accessed sealed court documents pertaining to the ongoing investigations. Specifically, checks of electronic court records allegedly confirmed that Gevorkyan had accessed the sealed court records pertaining to the named individuals shortly after the undercover had delivered the names to Koshkaryan.

According to a story in the Glendale News-Press, law enforcement officials view the arrest of Gevorkyan and Koshkaryan as exposing a major "betrayal within the system." According to the story, law enforcement officials are concerned that "organized crime is infiltrating areas we wouldn't have expected," putting officer's safety in danger, and allowing defendants under investigation to possibly destroy evidence and threaten criminal investigations. The EOTCF has already had to move up operations for fear that the suspects might flee or destroy incriminating evidence.

The arrest of Gevorkyan and Koshkaryan may be emblematic of a more widespread FBI crack down on insider threats. In recent years, the FBI has put an increasing premium on detecting such threats and preventing the significant harm such threats cause. These threats are often difficult to detect because an insider, as an employee with legitimate access, may not initially appear to be doing anything wrong. However, such insiders can cause significant damage by stealing company information or products to benefit another organization. The FBI has provided detailed tips on its website to detect insiders who may compromise company assets.

We will continue to keep you apprised of future developments in this case, as well as other FBI efforts to reduce the growing threat posed by rogue insiders. The case also highlights why some legal commentators and courts believe that the Computer Fraud and Abuse Act should be broadly construed to prevent insider data theft.

Update: California Federal District Court Reaffirms that Computer Fraud and Abuse Act Claims are Available for Violations of Employers' "Access Restrictions" Despite Ninth Circuit's *Nosal* Decision

By Joshua Salinas (September 13, 2012)

Last month we blogged about a district court for the Northern District of California that distinguished the Ninth Circuit's recent *U.S. v. Nosal* decision and allowed an employer to bring a counterclaim under the Computer Fraud and Abuse Act ("CFAA") against a former employee for alleged violations of a verbal computer access restriction. (*Weingand v. Harland Financial Solutions,* 2012 U.S. Dist. LEXIS 84844 (N.D. Cal. June 19, 2012). Recently, the court reaffirmed its conclusion regarding *Nosal* concerning the employee's subsequent motion to dismiss that CFAA counterclaim.

Defendant employer Harland Financial Solutions alleged that it verbally authorized plaintiff and former employee Michael Weingand to return to its offices after the termination of his employment to copy his personal files from his prior work computer. A dispute arose, however, when Weingand allegedly "accessed, without authorization, over 2,700 business files," some containing confidential, proprietary, and copyrighted information. (See our previous blog post for further details regarding the background of this case).

As discussed in our previous post, the court granted Harland's motion for leave to amend its answer to assert a counterclaim against Weingand for violations of the CFAA.

Harland subsequently amended its answer to assert the CFAA counterclaim. Weingand then moved to dismiss the claim for "failure to state a plausible claim for relief." (FRCP 12(b)(6)).

On August 29, 2012, the court denied Weingand's motion to dismiss. The court noted that it already rejected a bulk of Weingand's arguments in the prior motion for leave to amend. The court acknowledged, but declined to adopt, Weingand's argument that verbal authorization could not be the sort of authorization cover by the CFAA:

Notably, the court reiterated its prior conclusion concerning *Nosal*:

> "Although *Nosal* clearly precluded applying the CFAA to violating restrictions on use, it did not preclude applying the CFAA to rules regarding access."

Additionally, the court noted that many of the issues raised by Weingand concerning the scope and nature of his authorization, what constituted "personal" files, and whether he exceeded Harland's authorization, were factual questions appropriate for summary judgment – not a motion to dismiss.

The court denied Weingand's motion to dismiss because Harland alleged specific details about Weingand's alleged unauthorized access, including when, where, and what Weingand allegedly accessed and copied.

The court's reassertion that *Nosal* does not preclude employers' "access restrictions" is significant because it reaffirms that *Nosal* may not be as broad of a limitation for employers that seek to use the CFAA against departing employees that steal valuable company data. After Nosal, it was feared that employers would have no recourse under the CFAA against employees that violate clear and explicit computer, network, and information security policies.

The court allowed Harland to proceed with its CFAA claim based on a mere verbal access restriction. This holding remains consistent with the Ninth Circuit's prior decision in *LVRC Holdings LLC v. Brekka*: "The plain language of the statute therefore indicate that authorization depends on actions taken by the employer." Thus under *Weingand*, an employer's computer access policies may remain viable post-*Nosal* to bring CFAA claims in the Ninth Circuit against employees that violate those policies and steal valuable company data.

"Click Fraud" Allegations Found Insufficient Under Computer Fraud and Abuse Act, But Personal Jurisdiction Found Where Defendant Company's Website Deliberately Targeted Consumers Within the Forum State

By Joshua Salinas and Jessica Mendelson (September 19, 2012)

A federal district court for the Northern District of California recently held in a "competitor click fraud" case that a mere assertion of a violation of the Computer Fraud and Abuse Act claim without sufficient factual details regarding any inside or outside "hacking" is insufficient to establish subject matter jurisdiction over the action. (Incorp Services Inc. v. IncSmart.Biz Inc., No. 11-CV-4660-EJD-PSG, 2012 WL 3685994 (N.D. Cal. Aug. 24, 2012) The case also presented a novel personal jurisdiction issue involving alleged online false advertising where neither the defendants nor the plaintiff resided in California. The court found that personal jurisdiction existed because the defendant company's website deliberately targeted California consumers and continuously exploited the California marketplace.

Background

Incorp Services Inc. ("Incorp") is a Nevada-based corporation that provides a variety of company formation and registration services, including registered agent services across the country. Incorp expended resources to advertise its services on Microsoft, Google, and Yahoo! search engines. These search engines use a "pay-per-click" model that charges advertisers each time a user clicks on the advertiser's ad and subsequently deducts those charges from the advertiser's ad budget. The search engine stops providing advertising space when the advertiser's advertising budget is depleted.

A rampant problem with this pay-per-click advertising model is "competitor click fraud," a fraudulent scheme where companies - who are also advertising on the same websites as their competitors - repeatedly click on their competitors ads to drain their competitor's advertising budget. As a result, companies can potentially "clean" the Internet of their rivals' advertisements by exhausting their rivals' advertising budgets.

Incorp filed a lawsuit in the Northern District of California last year under the Computer Fraud and Abuse Act ("CFAA") alleging that it was the victim of this aforementioned fraud. Incorp alleged that a group of unknown Doe Defendants engaged in a campaign of repeatedly clicking on Incorp's online

ads, with no actual interest in learning about Incorp or purchasing Incorps' services. Incorp alleged that the Defendants conducted this campaign in bad faith with the intent of deleting Incorp's advertising budget to obtain a more prominent position in search engine results and consequently drive more potential customers to Defendants' website.

Incorp later identified the IP addresses associated with the alleged click fraud and amended its complaint to add IncSmart.Biz, Inc. ("IncSmart") as a defendant and to include claims against IncSmart for, inter alia, false advertising under the Lanham Act. Incorp alleged that IncSmart falsely advertised that IncSmart provides registered agent services for states where IncSmart does not have the necessary qualifications or did not obtain the necessary certifications to conduct business.

Incorp also amended its complaint to add officers of IncSmart as defendants, as well as one of the officer's elderly mother. All of these individual defendants were residents of Nevada and had no meaningful personal ties to the State of California. Neither individual defendant owned or leased any real or personal property in California, nor had they ever owned or been required to pay taxes in California.

Accordingly, IncSmart and the individual defendants filed motions to dismiss the amended complaint for lack of personal jurisdiction and improper venue, or alternatively, a transfer of venue. Specifically, they contended that Nevada was the appropriate forum and not California.

As a preliminary matter and before reaching the personal jurisdiction issue, the court decided to first analyze the existence of subject matter jurisdiction for the CFAA claim.

Subject Matter Jurisdiction

The court noted that it may dismiss an action for lack of subject matter jurisdiction where the court lacks a statutory or constitutional basis for deciding the case. In this case, Incorp pled the following: "In clicking on Incorp's online ads without having an actual interest in Incorp's website or services, Defendants exceed their authorized access to the Search Engines' protected computers...." (emphasis added). Relying on *United States v. Nosal*, 661 F.3d 1180 (9th Cir. 2011), which has been previously discussed in greater detail in this blog, the court found that Incorp's CFAA claim required a showing of additional facts to establish subject matter jurisdiction.

"The Court observes that there are no direct or clear allegations of 'hacking' in this passage-being, broadly, 'the circumvention of technological access barriers,' not violation of use restrictions." In other words, the court held that clicking online ads "without having an actual interest" does not constitute "exceeds authorized access" under the CFAA. The court also held that if Incorp was contending that Incorp's online activity violated any terms of use policies, it was insufficient to state a claim under the CFAA in light of the *Nosal* decision that violations of "use restrictions" are not violations under the CFAA. As such, the court granted Incorp leave to amend with respect to the CFAA claim so that Incorp could clarify and reallege how IncSmart's conduct violated the CFAA.

Personal Jurisdiction

The court then addressed personal jurisdiction. Under the Fourteenth Amendment's Due Process Clause, the court may exercise personal jurisdiction over a defendant who has "certain minimum contacts with the forum, such that maintenance of the suit does not offend traditional notions of fair play and substantial justice." Incorp did not contend that the court has general jurisdiction, and therefore, the court addressed specific jurisdiction.

The traditional test for establishing specific jurisdiction involves a three-prong test:

1. The non-resident defendant must have sufficient minimum contacts, i.e. "purposefully direct his activities" toward the forum state or purposefully avail himself of "the privilege of conducting activities in the forum." A split has arisen between the circuits concerning analysis under this prong when the minimum contacts are online – the *Calder* effects test, the *Zippo* sliding scale test, and the totality-of-circumstances test. The Ninth Circuit has followed the *Calder* effects test, which requires that the defendant allegedly must have (i) committed an intentional act, (ii) expressly aimed at the forum state, (iii) causing harm that the defendant knows is likely to be suffered in the forum state. Applying this analysis, the court in this case found that IncSmart allegedly used a highly interactive website to offer California specific services to California residents. The court found that this suggested a deliberate intent to access and sell to California consumers, and that IncSmart "continuously and deliberately exploited" the California marketplace with its website. The court held that IncSmart could reasonably expect to be subject to litigation in California.

2. The claim must arise out of the defendant's forum-related activities. Here, the court found that the claim arose from IncSmart's activities via its website, which specifically targeted California consumers.

3. The exercise of jurisdiction must be reasonable. Finally, the court found that IncSmart failed to present a compelling case that rendering jurisdiction would be unreasonable, and that requiring the case to be refiled in an alternate forum would merely delay the resolution of the case. As a result, the court denied the motion for lack of jurisdiction over the corporation and some of its officers. The court granted the motion with leave to amend, however, with respect to one of the officer's elderly mother because she was not connected to IncSmart's website and there was no evidence of any personal jurisdiction.

Improper Venue/Transfer of Venue

Regarding venue, the court concluded that the Defendants failed to establish the necessary burden required to transfer the case to Nevada. In particular, the court noted that Incorp's choice of forum should be overturned sparingly, and the Defendants failed to show an inconvenience regarding the location of witness and/or documentary evidence. Thus, no transfer of venue was needed.

Takeaways

(1) Are click fraud claims viable under the CFAA after *Nosal*?

Some commentators anticipated that the CFAA may represent the future in effective click fraud deterrence. This would become increasingly valuable as more advertising dollars are moving from traditional print and television to online advertising. In fact, Microsoft was the first to bring civil action for click fraud under the provisions of the CFAA a few years ago. (*Microsoft Corp. v. Lam*, No. C09-0815 (W.D. Wash. filed June 15, 2009). Microsoft contended that the fraudulent clicks at issue violated its terms and conditions, and, thus exceeded authorized access by violating these use restrictions. Unfortunately, no substantive rulings came out of the case as the parties reached a settlement prior to any motion practice.

This case seems to suggest that click fraud claims based on violations of terms of use policies may not be viable under the CFAA after *Nosal.* The court in this case allowed Incorp to amend its CFAA claim, but it remains unclear how click fraud can constitute activity "without authorization" or "exceeding authorized access" under the statute. One positive note for click fraud victims is that the court's reliance on Nosal may limit its holding to jurisdictions that follow the Ninth Circuit's narrow interpretation of the CFAA regarding violations of use restrictions or terms of use policies.

(2) Highly interactive websites that deliberately target a forum state may establish personal jurisdiction

Moreover, this case reaffirms the use of the *Calder* effects test within the Ninth Circuit for analyzing minimum contacts online. As companies continue to expand and increase their presence and business activities online, it is important to recognize that certain online activities may establish personal jurisdiction that may not otherwise exist. As demonstrated in this case, district courts within the Ninth Circuit when analyzing personal jurisdiction will look into the interactivity of a party's website and/or how the party's online activities deliberately target a specific forum. Thus, even if a party is not "physically present" in a particular forum, the party's may not be able to use the Internet as a digital shield to hide from the court's jurisdiction.

New Federal Legislation Proposed To Amend Computer Fraud and Abuse Act To Address Unauthorized Cloud Computing Activities

By Jessica Mendelson (October 9, 2012)

On September 19, 2012, Senators Amy Klobuchar (D-MN) and John Hoeven (R-ND) introduced the "Cloud Computing Act of 2012." The bill is a bipartisan effort to amend the Computer Fraud and Abuse Act ("CFAA"). If the bill passes, it would purportedly provide greater civil and criminal protections under the CFAA against unlawful computer activites related to cloud computing than currently exist. The introduction of the bill was delayed until this year after Senator Orrin Hatch (R-Utah) withdrew his support for the original bill in mid-2011.

Cloud computing was defined in the previous press statement involving Klobuchar's bill as the "use of remote data centers to take over the task of computing from the personal computer." Social media websites commonly use such cloud computing, and more recently, businesses have increased utilizing it to increase productivity and lower IT costs.

Under the terms of the proposed legislation, federal agencies would be required to publish periodic reports about their progress in shifting computer infrastructures toward cloud computing. Additionally, federal agencies would have to comply with the Office of Management and Budget's ("OMB") Federal Cloud Computing Strategy, and submit periodic reports to the OMB and the Office of Electronic Government and Information Technology about their compliance efforts. These reports would also require a "three year forecast of the plans of the agency relating to the procurement of cloud computing services and support relating to such services."

The bill defines "cloud computing service" as "a service that enables convenient on demand network access to a shared pool of configurable computing resources (including networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or interaction by the provider of the service." This definition comports with that of the National Institute of Standards and Technology's definition of the term. Similarly, a cloud computing account is defined as "information stored on a cloud computing service that requires a password or similar information to access and is attributable to an individual." Under this definition, a single user can have multiple cloud computing accounts.

Passage of the bill would amend the CFAA to provide an additional, separate offense or claim for unauthorized access of a cloud computing account. Essentially, accessing a cloud computing account without authorization or in excess of authorization would become a criminal offense and as well as provide civil liability. Specifically under the bill "if the protected computer is part of a cloud computing service, each instance of unauthorized access of a cloud computing account, access in excess of authorization of a cloud computing account, or attempt or conspiracy to access a cloud computing account without authorization or in excess of authorization shall constitute a separate offense."

According to a press statement, Klobuchar previously indicated under the existing terms of the CFAA, if a cloud service has millions of individual accounts, and a hacker were to take a few dollars from each, the hacker cannot be prosecuted for a felony because the law addresses the individual attacks, and not the aggregate effect. According to the press statement, such security breaches can cost the public up to $1 trillion annually.

The bill provides for presumed loss. Specifically, it provides "[i]f an offense under this section involves a protected computer that is part of a cloud computing service, the value of the loss of the use of the protected computer for purposes of subsection (a)(4), the value of the information obtained for purposes of subsection (c)(2)(B)(iii), and the value of the aggregated loss for purposes of subsection (c)(4)(A)(i)(I) shall be the greater of (1) the value of the loss of use, information, or aggregated loss to 1 or more persons; or (2) the product obtained by multiplying the number of cloud computing accounts accessed by $500."

Critics of the bill argue that it defines cloud computing too broadly. Legal critics have criticized the bill's definition of cloud computing, calling it incoherent and "co-extensive with the Internet generally." The Cloud Computing Act of 2012 applies to a protected computer which acts as part of a cloud computing service. The phrase "protected computer" is defined broadly by the CFAA to include any computer "used in or affecting interstate. . . commerce or communication." Critics argue that under this definition, every computer connected to the internet would constitute a "protected computer" since such computers can be used to access websites involved in interstate commerce.

The bill has also been criticized for its failure to add "meaningful protection" to the already confusing CFAA. Opponents suggest it is unclear "what problem this bill purports to solve" and question whether there have been cases where "the CFAA underprotected a cloud computing service or this legislation would have changed the outcome." They argue the bill simply increases the CFAA's complexity without much benefit, and the proper fix for the CFAA would be to "reduce the law's length, organize it better, and reduce its implications for user's ordinary Internet activity." Others argue that the proper approach is to allow for voluntary methods, rather than legislation.

The bill, presently in committee, has a long road to travel in order to become law. We will continue to keep you apprised of future developments with this bill, as well as other legislation pertaining to the CFAA.

Pennsylvania Federal Court Dismisses Employee's Computer Fraud and Abuse Act Claim Based Upon Employer's Alleged Improprer Access of LinkedIn Account: No Cognizable Damages

By Jessica Mendelson and Robert Milligan (October 12, 2012)

Ownership of company social media accounts has recently become a hot topic in the legal industry, and with its decision in *Eagle v. Morgan*, 2012 WL 4739436, E.D.Pa., October 04, 2012 (NO. CIV.A. 11-4303) this past week, the Eastern District of Pennsylvania has added fuel to the fire.

Edcomm, a banking education company, was initially run by Dr. Linda Eagle. In 2010, Sawabeh Information Services Company ("SISCOM") purchased the outstanding common shares of Edcomm. While she was president of the company, Dr. Eagle established an account on LinkedIn. Another employee assisted her in maintaining the account, which was used "to promote Edcomm's banking education services; foster her reputation as a businesswoman; reconnect with family, friends, and colleagues, and build social and professional relationships." Edcomm's general, informal policy was that when an employee left the company, the company would, in effect, "own" the account, and could "mine" the incoming traffic and the information on the account, as long as its actions did not rise to the level of stealing an employee's identity.

Eagle initially remained the CEO of the company, but was allegedly fired by the defendants in June 2011. Sandy Morgan was appointed interim CEO. Edcomm changed the password for Eagle's LinkedIn account and replaced her name and photo with that of Sandy Morgan and blocked Eagle's access to the account. Eagle initiated this lawsuit in July 2011. Defendant Edcomm counterclaimed, and in December 2011, this court dismissed Edcomm's own CFAA claims against Eagle. For additional background, see our prior post on this case here. In July 2012, defendants filed a motion for summary judgment.

On October 4, 2012, the U.S. District Court for the Eastern District of Pennsylvania granted defendants' motion for summary judgment on Eagle's Computer Fraud and Abuse Act and Lanham Act claims. The court denied summary judgment with respect to the state claims asserted by Eagle.

The court dismissed the CFAA claim, finding Eagle had not shown a legally cognizable loss or damages suffered during the brief period in which she could not access her LinkedIn account. Eagle alleged she had missed out on professional opportunities because she lacked access to her account. However, according to the court, typically CFAA damages are limited to cases where a plaintiff lost

money because her computer was inoperable or damaged, neither of which was the case here. Instead, Eagle alleged loss of potential business opportunities. According to the court, such speculative losses are "simply not compensable under the CFAA." The court further objected to Eagle's failure to quantify damages: Eagle provided "absolutely no evidence in support" of her damages claims.

In addition, the court dismissed the Lanham Act claim for failure to show a likelihood of confusion. Here, the defendants had switched the name and photo on the account, replacing Eagle's name and image with that of Morgan. Although it may have diverted Eagle's contacts, the defendants did not try to "pass off" Morgan as Eagle, nor did they suggest Eagle endorsed her in any capacity. As such, defendants' actions would merely serve to divert Eagle's contacts, rather than confuse them.

The court retained jurisdiction over Eagle's state law claims. The case is scheduled to go to trial on October 16. Among the claims that will be addressed at that time are invasion of privacy by misappropriation of identity, tortious interference with contract, unauthorized use of name in violation of Pa. C.S. § 8316, misappropriation of publicity, identity theft under Pa. C.S. § 8316, conversion, civil conspiracy, and civil aiding and abetting. Ultimately, the court's resolution of the conversion claim may resolve the ownership issue regarding the LinkedIn account.

This case is emblematic of significant controversies faced by the courts and the legislature with respect to social media. The courts have begun to grapple with issues such as whether social media accounts and followers can be owned, misappropriated, converted, transferred, or assigned, who may be liable when someone loses access to their social media accounts and followers, what damages are recoverable, and what is a personal social media account versus a company social media account. These issues have already arisen in cases such as *Phone Dog*, *Christou v. Beatport, LLC* and *Piggy Paint*, and will likely continue to arise in the future.

As social media disputes have become more prominent in the courts, the issues have become a hot topic in the state and federal legislatures. As of now, the current legislative debate on social media is primarily focused on prohibiting the turnover of user names and passwords for personal social media accounts by employees and prospective hires. California recently joined Maryland and Illinois in passing legislation prohibiting employers from requiring access to employees' and prospective hires' "personal" social media. "Personal" is not defined, however, in the California statute and "social media" has a very broad definition that may encompass any "personal" digital information. In the future, the larger issues are likely to focus on the extent to which companies can assert ownership interests in social media accounts, including the passwords, contacts, and other information contained in the accounts, defining the distinction between between personal and work accounts, and developing appropriate protections to ensure that company trade secrets and confidential information are not leaked on "personal" social media without invading privacy and other legal protections.

The takeaway message from this case is to be proactive and develop social media policies and agreements concerning these issues before the need actually arises. Agreements and policies should establish who owns the company social media account, and specify a procedure for returning login information upon termination. Employees should be reminded of the agreements and policies at the

time of termination and employers should ensure that they obtain the relevant usernames and passwords. Additionally, the company should register or create the account, and change the password at the time of termination in order to avoid confusion. Agreements and control over the account are key in such disputes, as it speaks to who actually owns the account. Please also see Eric Goldman's informative and insightful blog entry on this new decision.

We will continue to keep you apprised of future developments in this case and similar social media ownership/trade secret issues.

Hacking Into Personal E-Mail Account Not a Violation of the Stored Communications Act According to South Carolina Supreme Court

By Molly Joyce (October 23, 2012)

On October 10, 2012, the Supreme Court of South Carolina found in *Jennings v. Jennings, et al.*, that a defendant who allegedly hacked into a plaintiff's personal e-mail account to retrieve messages that were already read by the plaintiff was not liable under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701.

The Defendant allegedly hacked into plaintiff's Yahoo! account once she learned that plaintiff was allegedly cheating on his wife. At issue in Jennings was whether the hacked e-mails – which were single copies of e-mails on the Yahoo! server and not downloaded or saved to another location – were in "electronic storage" under the SCA. While all of the Justices agreed that the e-mails at issue were not in electronic storage under the statute's definition, and therefore, not protected under the SCA, their rationale in reaching their conclusion diverged and resulted in a 2-2-1 decision.

Section 2701(a) of the SCA proscribes accessing an electronic communication while it is in "electronic storage." The SCA defines "electronic storage" as

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication. 18 U.S.C. § 2510 (17).

The lower court held that the e-mails were in "electronic storage" because they were stored for backup protection pursuant to subsection (B) of Section 2510 (17). On appeal, Broome argued that the plaintiff needed to establish that the e-mail met both subsections (A) and (B) to constitute electronic storage. The Supreme Court's decision, written by Justice Hearn, noted that although the Department of Justice espoused Broome's interpretation of Section 2510(17), called the "traditional interpretation," it was not one favored by the majority of courts that have considered the topic, which have instead found that subsection (A) or (B) must be met. In any event, plaintiff only argued that his e-mails were in electronic storage pursuant to subsection (B), and therefore the court found that it was unnecessary to determine whether to adopt the traditional interpretation or the interpretation recognized by most courts.

In discussing the applicability of subsection (B), the Justice Hearn relied upon Merriam-Webster's definition of "backup," which is "one that serves as a substitute or support." The court concluded that Congress's use of the word "backup" necessarily presupposes the existence of another copy to which the e-mail would serve as a substitute or support. The court found that because the plaintiff's e-mails were a single copy of the communication, they could not have been stored for backup protection, and thus, not protected by the SCA.

Chief Justice Toal, on the other hand, in his separate concurring opinion, disagreed with Justice Hearn's reliance upon the dictionary definition of "backup," arguing that an e-mail message on an internet service provider's website could be considered stored for "support" in the event the user needs to retrieve it. Instead, he argued that the traditional interpretation advanced by the DOJ (requiring that both subsections (A) and (B) are met for it to be considered in "electronic storage") should be adopted. In his view, an e-mail is in electronic storage only if it has been received by a recipient's service provider but has not yet been opened by the recipient. Because the e-mails at issue had already been received, opened and read by the plaintiff when they were retrieved by Broome, they fell out of the scope of electronic storage under the statute.

A third opinion written by Justice Pleicones concurred in result but noted that it was also necessary to consider that, in addition to the fact the e-mails at issue were not in temporary storage during the course of transmission (subsection A), they were also not copies made by plaintiff's service provider for purposes of backup (subsection B), and therefore not protected by the SCA.

Given that the Justices could not agree even amongst themselves on the basis for their decision, it's not surprising that other courts considering the applicability of the SCA have reached differing results, most notably the Ninth Circuit in the case of *Thoefel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). In *Thoefel*, the court found that e-mail messages which were delivered to the recipient, read, and stored by the internet service provider were in "electronic storage" under the SCA.

The Justices in *Jennings* were quick to acknowledge that even if Broome did not violate the SCA, her alleged actions weren't necessarily acceptable either. Justice Hearn said that "this should in no way be read as condoning her behavior. Instead, we only hold that she is not liable under the SCA because the e-mails in question do not meet the definition of 'electronic storage' under the Act." Similarly, Chief Justice Toal noted that the SCA, which was enacted in 1986, "is ill-fitted to address many modern day issues, but it is this Court's duty to interpret, not legislate."

The *Jennings* decision has led commentators to express frustration with the SCA's lack of protection for webmail and information stored in the cloud. Most agree that Supreme Court review of the SCA or even a new federal statute addressing this type of activity is necessary to protect information stored using today's technology. While the Computer Fraud and Abuse Act might be another possible avenue for plaintiff Jennings, plaintiffs oftentimes are unable to prove the requisite amount of damages under the CFAA, which was recently demonstrated in the case of *Eagle v. Morgan, et. al.*, no. 11-4303 (E.D. Penn. Oct. 4, 2012). Because this issue is far from resolved, employers (and, yes, even scorned lovers) shouldn't necessarily view the *Jennings* decision as a green light to hack into one's personal e-mail.

Employer Petitions U.S. Supreme Court to Resolve Computer Fraud and Abuse Act Circuit Split

By Robert Milligan and Joshua Salinas (November 2, 2012)

As anticipated, the issue regarding the application of the Computer Fraud and Abuse Act ("CFAA") against employees who violate their employer's computer use policies and steal valuable company data may be headed to the U.S. Supreme Court. Last week, WEC Carolina Energy Solutions LLC ("WEC") filed a petition for writ of certiorari before the Supreme Court, asking the Court to determine whether the CFAA applies to employees who violate employer-imposed computer access and data use restrictions to steal company data.

Petitioner WEC provides specialized welding and related services to the power-generation industry. Respondent Mike Miller was employed by WEC as a project Manager in Field Services. WEC issued Miller a laptop computer for use in his employment, along with access to WEC's computers and servers and numerous confidential and trade secrets documents stored therein. WEC allegedly had a clear company policy prohibiting any unauthorized use of its confidential information and trade secrets, including a prohibition against downloading confidential and proprietary information to an employee's personal computer.

Miller resigned from WEC and went to work for a competitor, Arc Energy Services ("Arc"). Immediately before his resignation, however, Miller allegedly downloaded a substantial number of WEC's confidential documents and emailed them to his personal email account. These confidential documents allegedly included highly valuable information regarding WEC's past and pending customer proposals, pricing information, and quotation worksheets. Miller allegedly incorporated this information into a sales presentation on behalf of Arc for a potential customer regarding two power plant projects; Arc was subsequently awarded those projects.

WEC brought action against Miller for, inter alia, violation of the CFAA. WEC contended that Miller lacked and/or exceeded his authorization to download WEC's confidential documents because WEC's company policies prohibited any downloading of these documents to his personal computer.

The Fourth Circuit Court of Appeals in *WEC Carolina Energy Solutions LLC v. Miller,* 2012 WL 3039213 (4th Cir. 2012), affirmed the district court's dismissal of the claim and held that departing employees are not liable under the CFAA for mere violations of a company computer use policy. In doing so, the Fourth Circuit adopted the Ninth Circuit's narrow interpretation of the CFAA , thus

widening a split between the federal circuits on whether employees who violate company policies and/or engage in disloyal conduct by stealing company data can be liable under the CFAA. Please see John Marsh's and Ken Vanko's blogs, as well as our previous blog, on the case.

On the other side, the Fifth, Seventh, and Eleventh Circuits have adopted a broader interpretation of the CFAA based on either common-law agency principles or computer usage policies. Under the agency theory, when an employee accesses a computer to further interests adverse to the employer, such actions terminate his or her agency relationship and, thus the employee loses any authority to access the computer and certainly access to steal company data. Under the computer usage theory, a violation of a computer usage policy can serve as a basis for holding an employee liable under the CFAA, Thus, an employee who is authorized to access a company computer, but uses that access to steal or damage valuable company data in violation of a computer usage policy, would be liable for his or her wrongful conduct.

Earlier this spring, a Ninth Circuit en banc panel in *U.S. v Nosal* adopted a narrow interpretation of the CFAA and found that an employee's violation of his/her employer's computer usage policies was not a violation of the CFAA. The Solicitor General declined to file a petition for writ of certiorari in that case.

As of now, an employer's protection under the CFAA against rogue employees that steal valuable company data may simply depend on which jurisdiction they are in and/or the genius of counsel.

WEC's petition does not necessarily mean the Supreme Court will hear the case. In fact, the Court's website provides that it receives over 10,000 petitions each year but only grants and hears oral argument in about 75-80 cases (<1 %).

The fact that the Supreme Court has yet to decide a CFAA case since the statute's inception in 1984, along the deepening circuit split, may influence the Court's consideration of the petition. We will continue to keep you apprised of future developments in the rapidly changing CFAA landscape.

Plaintiffs Retain Home Field Advantage in Email Hacking Action But Nebraska Federal Court Dismisses Computer Fraud and Abuse Act Claim

By Marcus Mintz (November 13, 2012)

Corporate espionage in the sports industry? The owners of the Indoor Football League's Omaha Beef recently asserted serious allegations against rival team, the Allen Wranglers, the League commissioner, and the Beef's former coach, now coaching for the Wranglers.

In *Gridiron Management Group LLC v. Allen Wranglers*, No. 8:12-cv-3128, 2012 WL 5187839 (D. Neb. Oct. 18, 2012), Plaintiffs asserted that the Beef's former coach, Defendant Patrick Pimmel, at the commissioner's direction, hacked the Yahoo! email accounts of one of the Beef's owners and its day-to-day manager, Plaintiff Jeffrey Sprowls. Plaintiffs filed their lawsuit in Nebraska federal court, asserting claims for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Stored Communications Act 18 U.S.C. §2701, as well as for violations of Nebraska statutes and business tort claims.

Plaintiffs allege that sometime in 2011, Pimmel, at the commissioner's direction, began using unauthorized means to gain access into the Plaintiff's electronic accounts. They allege that this allowed Pimmel to gain unauthorized access to Plaintiff's electronic accounts on more than one hundred separate occasions. After gaining access to Sprowls's accounts, Pimmel allegedly viewed private electronic communications and disseminated them to the commissioner. Plaintiffs claim that the commissioner did not warn or inform Plaintiffs that those accounts had been accessed.

Texas-based Pimmel moved to dismiss the action for lack of personal jurisdiction, for improper venue, alternatively, to transfer venue, and to dismiss the CFAA count. Pimmel contended that since becoming the Wranglers' head coach, he has not resided in or conducted business in Nebraska and has maintained little or no physical contract with the state. The court was not persuaded by Pimmel's arguments that the action did not belong in Nebraska. It expressly found that because Pimmel was alleged to have hacked into email accounts maintained by Nebraska residents on computers located in Nebraska, he could have reasonably expected that "the brunt of the injury resulting from his actions would be felt in Nebraska" and that personal jurisdiction existed over Pimmel because he should reasonably have anticipated being hauled into court in Nebraska after hacking into computers located there over 100 times. Similarly, the court held that although "[n]othing indicates that any of the Defendants were ever physically present in Nebraska," Pimmel was alleged to have reached across

state boundaries by hacking into Plaintiffs' Nebraska-based computers. Accordingly, after taking all uncontroverted allegations in the complaint as true, the court found that venue was also appropriate in Nebraska and denied Pimmel's motion to dismiss for improper venue and refused to transfer venue to Texas. In sum, the physical presence of Plaintiffs' computers trumped Pimmel's lack of physical connection with Nebraska.

Pimmel's sole victory was obtaining dismissal, albeit without prejudice, of Plaintiffs' claim for violation of the CFAA. The court found that although Plaintiffs pled sufficient facts to establish unauthorized access to a protected computer, Plaintiffs failed to allege facts demonstrating any damages as a result of Pimmel's access. The court noted that, for purposes of the CFAA, "damage" does not "encompass harm from the mere disclosure of information and is not intended to expansively apply to all cases where a trade secret has been misappropriated by use of a computer." Finding Plaintiffs' allegations insufficient, the court dismissed the CFAA count, although without prejudice, permitting Plaintiffs another opportunity to establish damages for sustaining a claim under the CFAA.

Arizona Federal Court Issues Significant Computer Fraud and Abuse Act and Trade Secret Preemption Decision

By Paul Freehling (November 26, 2012)

According to a recent Arizona federal court decision, (a) an employee who had the right to access his employer's confidential emails did not violate the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, by downloading 300 such documents to his personal computer and sharing them with a recently terminated employee; (b) an employer may pursue either a misappropriation claim under the Arizona Uniform Trade Secrets Act (AUTSA), or statutorily pre-empted causes of action based on the same facts; and (c) a rule to show cause is appropriate where the defendants violated a 48-hour deadline to return the employer's confidential documents. *Food Services of Amer. Inc. v. Carrington*, No. CV-12-00175-PHX-GMS (D. Ariz., Nov. 8, 2012).

Because of the holding in *U.S. v. Nosal*, 676 F.3d 854, 863-64 (9th Cir. 2012), the *Carrington* case defendants cannot be sued in the Arizona federal court for a CFAA violation (of course, both individuals may be liable for non-CFAA causes of action). *Nosal*, which is binding on that court, held that an employee who was authorized to access the employer's computerized records did not violate the CFAA by downloading and distributing them to unauthorized persons. Some other circuit courts of appeal decisions conflict with *Nosal*. See, e.g., several cases cited there — including *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (breach of duty of loyalty terminates authorization to access employer's computer data and, therefore, violates CFAA) — and criticized.

The AUTSA pre-empts all claims based on the same facts as the misappropriation cause of action (regardless of whether what was misappropriated was a trade secret or merely confidential information). However, according to the court in Carrington without citation of authority, pre-emption means that the employer must choose whether to sue for an AUTSA violation or for pre-empted claims. This holding is puzzling. Several cases hold that causes of action pre-empted by a uniform trade secrets act are abrogated. See, e.g., *CDC Restoration & Constr. v. Tradesmen Contractors, LLC,* 274 P.3d 317 (Utah App. 2012) (the "preemption provision [in a UTSA] has generally been interpreted to abolish all free-standing alternative causes of action for theft or misuse of confidential, proprietary or otherwise secret information").

In response to their ex-employer's motion for entry of a rule to show cause why the defendants should not be held in contempt for late production of the employer's documents, the defendants asserted that they had located and produced the documents only a few months after expiration of the deadline for doing so. They professed to having committed a "relatively minor technical infraction" as a result of "a misunderstanding between counsel and defendants." The court was unforgiving because the "defendants' response fails entirely to comprehend the serious nature of violating a court order." That ruling contains a loud and clear message concerning the potential adverse consequences to a party for failing to produce misappropriated confidential documents as ordered by a court, no matter how abbreviated the time allowed for doing so.

In sum, the *Carrington* decision should send shivers down the spine of a former employee who misappropriated his employer's proprietary information. In some circuits the former employee may escape CFAA liability for misdeeds occurring before termination, but regardless he may be hit with an expensive lawsuit and a monetary judgment.

Mississippi Federal District Court Allows Computer Fraud and Abuse Act Claim To Proceed Against Former Employee

By Jessica Mendelson (December 18th, 2012)

A recent Computer Fraud and Abuse Act ("CFAA") case from the Southern District of Mississippi further muddies the water with respect to the circuit split regarding the application of the law against former employees who violate computer usage policies or violate their duties of loyalty to their employers by stealing company data from company computer systems.

Unified Brands, Inc. ("Unified"), a manufacturer and marketer of food service equipment, purchased another company, Intek, in 2010. Michael Teders ("Teders"), who had previously been an executive of Intek, entered into employment contracts with both Intek and Unified during the purchase period. Under the terms of the agreement, Teders was prohibited from working for any business which sold or produced steam cooking equipment for a year. In August 2010, Teders began working as Unified's National Sales Manager, and signed another agreement pledging to maintain the confidentiality of Unified's proprietary information for a two year period. Teders also signed one year non-compete and non-solicitation agreements. In December 2010, Teders allegedly "secretly negotiated a position with AEC," a competitor in the steam cooking equipment industry. Prior to announcing his resignation, Teders allegedly accessed the laptop Unified Brands had provided him with, and downloaded confidential and proprietary information. Furthermore, Teders allegedly solicited Unified's customers in violation of his employment agreement with Unified.

In February 2011, Unfied sued Teders in the Southern District of Mississippi, alleging various causes of action, including violations of the Computer Fraud and Abuse Act ("CFAA"), the Mississippi Uniform Trade Secrets Act (MUTSA), negligent supervision, and tortious interference with business relationship. The defendants moved to dismiss for lack of personal jurisdiction and failure to state a claim.

Jurisdiction

AEC moved for dismissal on the grounds of lack of personal jurisdiction under Rule 12(b)(2) of the Federal Rules of Civil Procedure. Here, the court found that subject matter jurisdiction was based on both federal question and diversity jurisdiction. In federal question cases, the court must look to service of process provisions giving rise to the federal question. Under the CFAA, a federal court may exercise

personal jurisdiction "over only those defendants who are subject to the courts of the state in which the court sits." *Point Landing, Inc. v. Omni Capital, Int'l, Ltd.*, 795 F. 2d 415, 419 (5th Cir. 1986). The analysis is similar for diversity of citizenship cases, where the court conducts a two-step analysis: (1) the forum state's law must provide for assertion of jurisdiction, and (2) the state law must comport with the Fourteenth Amendment's Due Process Clause.

In addressing the first step, the court looked to Mississippi's Long Arm Statute, which allows a court to exercise personal jurisdiction over non-resident persons and business entities that have made a contract with a Mississippi resident that is to be performed in whole or part in the state, have committed a tort in the state, or who do business in the state. Here, Unified argues that personal jurisdiction can be exercised over AEC and Holder because they committed a tort within the state, namely tortious interference with business relationship. The court found AEC and Holder did more than simply hire a competitor's employee: Teders was still employed with Unified, and yet he was actively negotiating his future employment with AEC and Holder. As such, there was sufficient evidence to establish a prima facie showing that the tortious interference occurred in Mississippi, since at least some of the damage and loss occurred in that state.

In addressing the second step, the court looks to whether state law complies with the Fourteenth Amendment. To make such a showing, the court must show that the defendant has purposefully availed himself of the benefits and protections of the forum state by establishing minimum contacts with the forum state, and that the exercise of jurisdiction doesn't offend traditional notions of fair play and substantial justice. Here, the court found that the nexus between Mississippi and the allegedly injured business relationship was the employment contract between Unified and Teders, which are governed by Mississippi law. Teders was allegedly soliciting clients while still employed with Unified, which satisfied the due process requirement. Additionally, exercising jurisdiction would not be unreasonable because the defendants directed business activities into Mississippi, which had an interest in litigating the case because the tortious interference occurred within its borders.

Ultimately, the court found a prima facie showing of jurisdiction, but emphasized that the plaintiff must still prove jurisdictional facts at trial or pretrial evidentiary by a preponderance of the evidence.

Motion to dismss for failure to state a claim: The Computer Fraud and Abuse Act

The most notable ruling here is the court's decision regarding the CFAA claim. Unified alleged that Teders violated the CFAA by intentionally accessing a computer without authorization and obtaining information from a protected computer. AEC and Holder argued Teders downloaded confidential information from a computer he was authorized to access. Despite the defendants' argument, the court found there was sufficient evidence to assert a plausible CFAA violation. According to the court, several courts have recognized that "once an employer is working for himself or another, his authority to access the computer ends, even if he or she is still employed at the present employer." Here, the pleadings alleged Teders was unauthorized to access the computer, since he was acting on his own behalf, which the court found was sufficient to assert a CFAA claim.

Interestingly, this case seems to rely on the rationale of the agency theory, which is followed by the Seventh Circuit, as opposed to the computer usage theory followed by the Fifth and Eleventh Circuits. Cases following the agency theory are becoming increasingly rare these days. See our post on *WEC Carolina Energy Solutions* for additional information on this circuit split.

Under the agency theory, which is based on common law agency principles, when an employee accesses a computer to further interests adverse to the employer, such actions terminate his or her agency relationship and, thus the employee loses any authority to access the computer. The Seventh Circuit applied agency principles in *International Airport Centers, LLC v. Citrin* to determine that an employee's access was unauthorized from the moment he decided to quit and had undertaken actions in violation of his duty of loyalty to his employer. According to the decision, access is only authorized within the agency relationship between employer and employee. This agency relationship relies on loyalty as well as transparency, and violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship. Under the Seventh Circuit's approach, whether access to a computer was "unauthorized" depends upon the status of the agency relationship between the employer and employee.

Under the computer usage theory, also known as the intended usage theory, a violation of a computer usage policy can serve as a basis for holding an employee liable under the CFAA. Thus, an employee who is authorized to access a company computer, but uses that access to steal or damage valuable company data in violation of a computer usage policy, would be liable for his or her wrongful conduct. For additional information, see Shawn Tuma's post on the subject. The computer usage theory has been applied in the Eleventh and Fifth Circuits, while the agency theory's application has generally been limited to the Seventh Circuit. However, the Southern District of Mississippi's decision suggests that the agency theory may still have some life left. It will be interesting to see how the case progresses as it moves toward the summary judgment stage, and we will continue to keep you apprised of future developments.

Virginia Federal Court Finds For Employer on Fidicuary Duty Claim Against Former Employee

By Michael Baniak (December 19, 2012)

A Virginia federal court district court recently issued a significant decision awarding lost profits to an aggrieved employer for breach of fiduciary duty by a former employee. The Court found that the ex-employee was not able to deduct his services for the company as an expense against the damages award. Further, the Court found that the employer's CFAA claim failed becuase there was not a sufficient showing of loss. *Ritlabs, SRL v. Ritlabs, Inc*., 2012 WL 6021328 (E.D. Va. 11/30/12).

Ritlabs SRL ("SRL") sued its CEO and part owner Demcenko, for alleged self-dealing through another company he formed (co-defendant), Ritlabs, Inc. ("INC"). The host of counts included breach of fiduciary duty of loyalty, violation of the Computer Fraud and Abuse Act (CFAA), and tortious interference with contractual relations. In a nutshell, Demcenko, while still the director (essentially CEO) of SRL, allegedly formed a rival Internet technology and software company INC with his wife. He then entered into a license agreement between SRL and INC to exclusively sell SRL's software in the US, with a non-exclusive worldwide. As the Court determined, Demcenko did not obtain approval from his SRL co-owners, nor advise them of his ownership interest in INC, or that he was cancelling a software distributorship agreement between SRL and another company, which he then entered into on behalf of INC.

Needless to say, his co-owners did not take kindly to Demcenko's activities, and sued. Plaintiff ultimately moved for summary judgment as to all of its claims, which resulted in the Court's grant of the same generally across the board, along with summary judgment against Defendants on all counterclaims. The Court imposed constructive trusts, issued restraining orders, and ordered an accounting and disgorgement proceeding. A bench trial ensued as to damages, and it is here that interesting tidbits reside.

The breach of fiduciary duty was the big-ticket item, based upon Demcenko's diversion of corporate opportunities to himself (through INC). SRL went for INC's gross revenue, without reduction for any expenses, as well as for some other smaller amounts. SRL also sought punitive damages in the way of costs and attorney's fees.

Applying Virginia law, a plaintiff is entitled to what it would have received "but for" the breach of fiduciary duty, so as to "deny Defendants the fruits of their scheme." Accordingly, the Court determined

that damages should therefore be calculated on the basis that Demcenko was operating INC for the constructive benefit of SRL; ergo, SRL was entitled to only profits, not gross revenue. In what might be seen as a bit of chutzpah by some, the Defendants sought to deduct amounts received by Demcenko for his "services". The Court was not buying it, however, and concluded that collecting a salary for breach of one's duty of loyalty, and while he was still receiving a salary from SRL, was not appropriate as a deductible expense.

As for damages under the CFAA, the Court noted that civil liability, and responsibility for compensatory damages or other relief, requires a showing of CFAA qualifying "loss" aggregating at least $5000. 18 U.S.C. section 1030(g). The bar for loss is not terribly high, as any reasonable cost to the "victim," including the cost of responding to the offense, damage assessment, restoration, revenue lost "or other consequential damages incurred because of interruption of service" will suffice. But here, the Court did not find the necessary nexus with damage incurred because of interruption of service for the bulk of what SRL was toting up on this count. That left an amount below $5000 total, which the Court noted was below the jurisdictional threshold, and divested the Court of jurisdiction. The previous judgment as to liability was thereby vacated for "lack of subject matter jurisdiction."

As for costs and attorneys fees, the elimination of the CFAA count removed that as a basis for a fee award. And as for punitive damages, upon which SRL further predicated its costs and attorneys fees, "the Plaintiff did not include a prayer for punitive damages in its Complaint, and should not be considered now." Nonetheless, the Court reviewed the evidence, and concluded that SRL did not meet its high burden for punitive damages. It was in this discussion that what might otherwise have seemed to be a fairly open and shut case revealed some nuances, such as his former partners having some favorable knowledge of Demcenko's plans to open a US branch, and "that the affairs of SRL were at times accompanied by rather unorthodox self-driected transactions by each of the owners."

Non-Competes & Restrictive Covenants

Pennsylvania Federal Court Salvages Customer Lists as Basis for UTSA Claim, But Shreds Liquidated Damages Provision and Rejects Fiduciary Claim

By Rebecca Woods (February 3, 2012)

In the most recent ruling in long-running litigation styled *AMG National Trust Bank v. Ries*, NO. 06-CV4337, 09-cv-3061 (E.D. Pa.) (decided Dec. 29, 2011), the Eastern District of Pennsylvania partially granted the defendant Stephen Ries's motion for summary judgment, jettisoning the plaintiff's breach of fiduciary duty claims and plaintiff's request for liquidated damages, but permitting the case to proceed for alleged breach of a restrictive covenant in his employment agreement.

Ries sought to have the court declare that the liquidated damages clause in the AMG non-compete agreement was unenforceable. The liquidated damages clause provided for payment of ten times the most recent annual gross fee income of the AMG client with whom defendant violated the non-compete. The court held that, as a matter of law, ten years worth of projected client fees per violation was an "unreasonably large and incredibly disproportionate estimate of the presumed actual damages caused by breaching a two-year restrictive covenant." The court noted in a footnote that other courts had held that even limiting the liquidated damages multiplier to the number of restricted years constituted an unreasonable penalty. The court also held, however, that notwithstanding the unenforceable liquidated damages clause, AMG had provided sufficient evidence that it had suffered actual damage such that summary judgment on the claim was not warranted.

The court also granted the summary judgment motion as to AMG's breach of fiduciary duty claim. Declining to resolve a choice of law issue because there was no conflict, the court concluded that the fiduciary duty claim was a mere duplicate of the breach of contract claim and thus was barred by either Colorado's economic loss rule or Pennsylvania's "gist of the action" rule. AMG had failed to identify any duty owed by defendant that was not grounded in his contractual obligations.

Finally, the court rejected summary judgment as to AMG's customer lists claim. Conceding that customer lists are "at the very periphery of the law of unfair competition" (quotation omitted), the court ruled in AMG's favor, invoking prior Pennsylvania case law noting that customer data may qualify as a trade secret if it is not basic, widely available information, albeit collected as a result of the employee's efforts. Instead, the employer seeking to protect such information must demonstrate that the data was collected by the employee only by virtue of the employee's position, with the help of the employer (time, expense, and efforts), while the employee was subject to a confidentiality agreement. A factor in the court's conclusion also appeared to be that AMG limited its claim to customers with whom Ries did not allege a close relationship. Ries's use of customer list data for customers with whom he had not worked at AMG appeared to make it easier for the court to conclude that this was information the jury could hold was properly subject to protection.

New York Federal Court Finds That Anti-Raiding Clause Is Subject to Rule of Reasonableness Under New York Law

By David Monachino (February 7, 2012)

In *Renaissance Nutrition, Inc. v. Jarrett*, 2012 WL 42171 (WDNY) (January 9, 2012), Renaissance, a vitamin and pre-mix company serving the dairy industry, alleged that two former top-level employees violated a five year "non-recruitment" or "anti-raiding" clause. In short, Renaissance alleged that these employees resigned in tandem with plans to develop a rival company, Cows Come First, and then actively recruited three other former Renaissance employees to join them in their new venture. The former employees moved for summary judgment arguing, in part, that the non-recruitment clause was invalid, because it did not protect a legitimate business interest. Renaissance responded by arguing that New York courts have upheld recruitment clauses like the one at issue here and that the clause was proper in scope because it only limited the defendants from purloining its employees not from engaging in business generally.

After noting that there appeared to be only one New York case discussing the applicable standard for enforcing a non-recruitment covenant (and no appellate authority), the District Court decided to apply the "overriding requirement of reasonableness" used to analyze non-compete covenants in New York. In its "reasonableness" analysis, the District Court required that Renaissance make "an enhanced showing" that its interests in protecting its client relationships outweigh the former employees' interests in free competition, by demonstrating that: "(1) the employees diverted by defendants posed a substantial risk that if they left, their customers would follow, (2) the departed employees would engage or did engage in competitive business with Renaissance, and that (3) it provided substantial resources and assistance in cultivating the customer base such that it would be unfair to allow employees to steal those customers to compete with it." The District Court ultimately held that Renaissance had a legitimate interest in the protection of client relationships developed at its expense and denied defendants' motion for summary judgment.

Illinois Appellate Court Holds That Illinois Supreme Court Non-Compete Decision In Reliable Fire Applies Retroactively

By Jessica Mendelson (February 11, 2012)

On February 3, 2012, the Appellate Court of Illinois, Second District reversed and remanded the Winnebago County Circuit Court's decision in *Hafferkamp v. Llorca* in a significant unpublished non-compete decision. The Second District held that the trial court failed to properly apply the Illinois Supreme Court's standard set in *Reliable Fire Equipment v. Arredondo* to determine whether the non-compete agreement was valid.

The defendant in this case, Leah Llorca, worked at a hair salon owned by the plaintiff, Mary Hafferkamp. As part of the terms of her employment, Llorca signed a non-compete agreement. Llorca later left Hafferkamp's hair salon, and joined a competing business, located in the geographic area excluded by the non-compete agreement. Hafferkamp sued to enforce the contract, and the trial court held the agreement unenforceable. The trial court's holding was based on *LSBZ, Inc. v. Brokis*, 237 Ill. App. 3d 415 (1992), which provided the correct enforceability test at the time of the trial court's ruling. The LSBZ test required the court to determine whether the promisee had a legitimate business interest in enforcing the agreement, and found that such an interest only existed in two cases: when the employee acquired confidential information from the employer, or where the employer had near permanent customer relations. The court here found that neither criteria was met, and thus the agreement was found unenforceable. Hafferkamp then appealed the case to the Second District.

After the trial court's decision in *Hafferkamp v. Llorca* was made, but prior to the Second District's ruling, the Illinois Supreme Court issued a significant ruling on non-compete agreements. This decision, in the case of *Reliable Fire*, clarified the standard for determining the enforceability of non-compete agreements. According to the Supreme Court, for an agreement to be enforceable, it must be analyzed under a three-pronged rule of reason test. The covenant would only be enforced if doing so was (1) not greater than necessary to protect a legitimate business interest of the promisee, (2) would not be "injurious to the public," and (3) would not cause "undue hardship to the promisor." *Reliable Fire*, 2011 IL 111871 at ¶ 17. Additionally, the court found that whether an interest was considered a "legitimate business interest" needed to be determined based on the totality of the circumstances. Id.

Basing its holding on the Illinois Supreme Court's decision, the Second District reversed and remanded *Hafferkamp v. Llorca* for the *Reliable Fire* test to be applied. By using the *LSBZ* holding as the basis for its decision, the trial court had not considered the totality of circumstances in determining whether Hafferkamp's business interests were legitimate, and thus, the Second District chose to remand the case.

According to the Second District, the "decision in *Reliable Fire* should apply both retroactively and proactively, since the Supreme Court "did not expressly limit the application. . . to prospective cases

only." *Hafferkamp v. Llorca,* 2011 IL App (2d) 100353 at ¶17. The court's reasoning for this was that *Reliable Fire* did not create a new test, but simply clarified a convoluted test to prevent misapplication. Additionally, the court found that failing to implement *Reliable Fire* retroactively could lead to inconsistent rulings depending on the filing date of the case, even if the facts of the case did not warrant such rulings.

The Second District's ruling is of note for future Illinois cases, in that it suggests that *Reliable Fire's* test for the enforceability of a non-compete clause applies to cases filed prior to the date on which Reliable Fire was decided.

One legal commentator, Kenneth Vanko of non-competes.com, has remarked that the Second District's ruling is consistent with *Reliable Fire* because the Illinois Supreme Court "really did nothing to change the law but only rejected the appellate courts' gloss on the applicable non-compete test."

Oregon Federal Court Permits Declaratory Relief Suit To Proceed In Race To Judgment Non-Compete Dispute

By Robert Milligan and Joshua Salinas (February 13, 2012)

In light of Valentine's Day, a blog involving two competitors specializing in heart rhythm therapy seems fitting. The Oregon district court case is *Biotronik, Inc. v. Medtronic, USA, Inc.,* No. 03:11-cv00366-HU, 2012 WL 14031 (D. Or. Jan. 4, 2012), where the Honorable Judge Michael H. Simon, found the amount in controversy for federal diversity jurisdiction satisfied, even though the plaintiff sought only declaratory relief and did not claim damages exceeding $75,000.

The interesting aspect of this case is that Judge Simon determined the value of the amount in controversy based on the plaintiff's potential liability for defendants' allegations in a separate out-of-state lawsuit.

The Parties and Background Facts

Plaintiff Biotronik, Inc. and Defendants Medtronic USA, Inc. and Medtronic, Inc. (collectively "Medtronic") are competitors in the cardiac rhythm management device ("CRMD") industry. CRMDs electrically stimulate the heart to pump blood when the heart is unable to keep a steady beat. Inherent in this highly competitive and technologically complex market is the necessity to have skilled salespeople with a great deal of technical knowledge. Thus, companies such as Medtronic retain noncompetition and non-solicitation agreements to protect the training and resources they invest in their employees.

A dispute arose when several employees left Medtronic to work for Biotronik. Medtronic believed former employee Rory Carmichael had wrongfully solicited these employees and caused them to leave for Biotronik.

Medtronic sued Carmichael in Minnesota state court, alleging that he solicited Medtronic's employees, on behalf of and/or for the benefit of Biotronik, in breach his Employment and Separation Agreements with Medtronic. At the time of the alleged solicitations, Carmichael was not yet an employee of Biotronik. Medtronic did not join Biotronik in the Minnesota action because Medtronic allegedly lacked sufficient evidence to sue for tortious interference with contract.

Biotronik's Declaratory Relief

Biotronik formally hired Carmichael while the Minnesota action was still pending, and immediately brought a declaratory relief action against Medtronic in Oregon state court. Biotronik sought two declarations:

1. "Biotronik has the right to employ Carmichael, free from any Post-Termination Obligations relating to noncompetition and non-solicitation that are set forth in the [Employee Agreement] and the Parties' Agreement; and

2. "Biotronik did not cause any violation of any of the Post-Termination Obligations set forth in [Carmichael's Employee Agreement]."

Medtronic removed the case to federal district court based on diversity of citizenship; Biotronik was an Oregon corporation and Medtronic a Minnesota corporation. Medtronic then moved to dismiss the case for improper jurisdiction, or in the alternative, transfer to Minnesota. Medtronic hoped to transfer the case to Minnesota, which has a stronger policy in enforcing noncompetition and non-solicitation agreements compared to Oregon.

Biotronik on the other hand moved to remand the case back to Oregon state court and maintain any "home field advantage," contending that the amount in controversy did not exceed the $75,000 requirement for federal jurisdiction.

Determining the Amount in Controversy

Judge Simon stated that when a removed lawsuit seeks declaratory or injunctive relief, the amount in controversy is measured by the value of the "object of litigation." (See *Hung v. Wash.State Apple. Adver. Comm'n,* 432 U.S. 333 (1977)). The object of litigation here was Biotronik's potential liability to Medtronic – the value of liability if Biotronik was in fact found liable in the Minnesota action for causing Carmichael to wrongfully solicit Medtronic's employees.

The value of that potential liability was the liquidated damages provision in Carmichael's Separation Agreement, which required Carmichael to repay Medtronic all post-termination compensation and additional consideration he received from his Employment and Separation Agreements. Judge Simon found the amount in controversy satisfied because the amount of these repayments would exceed $75,000.

Judge Simon found federal diversity jurisdiction satisfied, but denied Medtronic's request for dismissal or transfer.

Important Takeaways

1. Noncompetition and non-solicitation cases often involve a "race to the courthouse" to file first and secure the home forum and applicable state law because states differ in their policies toward the enforcement of non-compete clauses.

2. Plaintiffs seeking to avoid the removal of their declaratory relief actions to federal court, and potentially face dismissal or transfer, should narrow the language of their declarations to restrict the scope of their potential liability. Judge Simon noted that Biotronik's first declaration regarding its mere ability to employ Carmichael would not have satisfied the amount in controversy requirement. Biotronik's broad language in its second declaration, however, opened the door and allowed Judge Simon to consider Biotronik's potential liability for causing "any violation of any of [Carmichael's] Post-Termination Obligations."

3. Defendants seeking to remove a plaintiff's declaratory relief actions to federal court, to ultimately dismiss or transfer the case, should anticipate this strategy when initiating any early lawsuits. While the ideal strategy for employers is to file actions in one's own state first, the new employer is usually in the best position to know when the alleged breacher/employee is officially hired. Moreover, while there may not be sufficient evidence to join the new employer in an initial lawsuit, as in Medtronic's case, the scope of the allegations concerning the new employer in a complaint or other pleadings may help expand the scope of the new employer's potential liability. Thus, if the new employer's later declarations are too broad, the allegations in the early lawsuit may help widen the scope of potential damages to satisfy the amount in controversy for federal diversity jurisdiction, and help assist in a future motion to dismiss or transfer.

Former Pharmacy Benefit Management Executives Sued For Alleged Violations Of Customer Non-Solicitation Agreements In Wisconsin Federal Court

By Justin Beyer (February 15, 2012)

Thompson Reuters (Healthcare) Inc. sued three former executive employees, all formerly working for Thompson Reuters in its pharmacy benefits management and consulting division of its healthcare services arm, in the United States District Court for the Eastern District of Wisconsin on Monday and immediately filed a motion for partial summary judgment against the former executives for a declaration that their non-solicitation agreements are enforceable under Wisconsin law.

According to the complaint, all three former employees were originally employed by Trivantage Pharmacy Strategies, LLC, a private company located in Milwaukee, Wisconsin, which Thompson Reuters acquired in 2009.

As alleged in the complaint, Trivantage was in the business of providing pharmacy benefit management consulting and auditing services to assist companies in lowering their healthcare costs, and specifically lowering their pharmacy costs. Prior to Thompson Reuters acquisition of Trivantage, one of the employee defendants was allegedly a co-founder of Trivantage and had served as its Vice President of Business Development and the other two individual defendants served as Vice Presidents of Consulting Services. Between the three defendants, they were allegedly responsible for identifying potential clients, marketing Trivantage's services, developing and maintaining relationships with Trivantage's customers and prospective customers, and developing relationship with the appropriate personnel for each customer, for the purpose of establishing goodwill and maintaining customer relationships.

According to the pleadings, during the course of their employment with Trivantage, each of the defendants also executed various employment agreements, which, among other things, prohibited them from soliciting Trivantage's customers; specifically, one of the individual defendants agreed not to solicit Trivantage's customers for two years and the other two individual defendants agreed not to solicit for 18 months. Also included in each of the various agreements was an assignment clause, in which each of the defendants agreed that their non-solicitation agreement was assignable to any Trivantage successor.

In April 2009, Thompson Reuters entered into an agreement to purchase Trivantage, according to the complaint. Before the deal was executed, one of the individual defendants allegedly entered into a separate deal with Trivantage, through which Caldwell allegedly reaffirmed his non-solicitation obligations in exchange, in part, for receiving five percent of the net proceeds from Thompson Reuters' acquisition of Trivantage. Thompson Reuters attached an unexecuted copy of the alleged agreement to its complaint and claims that its agreement with that individual defendant constitutes an alleged oral contract.

For the following two years, the defendants continued to be employed by Thompson Reuters, performing the same functions that they had performed at Trivantage. In mid-2011, Thompson Reuters discovered that the defendants were not allegedly devoting their full energies to Thompson Reuters and suspected that the defendants were setting up and/or operating a new business. Specifically, Thompson Reuters claims that one of the individual defendants stopped logging his sales efforts into Thomson Reuters' computer system, the other two individual defendants allegedly exchanged emails that seemed to indicate that they were brainstorming about the name for a new company, and, on at least one occasion, according to the complaint, the individual defendants or one of their associates appear to have funneled a Thomson Reuters' payment to an unauthorized vendor.

Subsequently, Thompson Reuters terminated the individual defendants in August 2011. After their termination, Thompson Reuters sent a letter to each of the defendants reminding each of their non-solicitation agreements, but each defendant responded claiming that their non-solicitation agreement was unenforceable.

Also after terminating the defendants, Thompson Reuters allegedly discovered that the defendants, in May 2011 and while still in Thompson Reuters' employ, incorporated Remedy Analytics, a business which is competitive to Thompson Reuters and which is operated from two of the individual defendants' home. In November 2011, Thomson Reuters further learned that the defendants, through Remedy Analytics, were allegedly soliciting and attempting to poach certain Thompson Reuters' clients.

Interestingly, Thompson Reuters does not seek injunctive relief against the defendants in the complaint, instead seeking a declaration that the non-solicitation agreements are enforceable and seeking money damages for breaches of contract. In addition to filing its complaint, Thompson Reuters filed a motion for partial summary judgment seeking an immediate ruling from the court that the non-solicitation agreements are enforceable.

This case is worth watching as it addresses significant issues such as the enforceability of the non-solicitation agreements under Wisconsin law, including whether the court will enforce non-solicitation agreements acquired through a stock purchase agreement. Also, should the Court find that the restrictive covenants are enforceable, the amount of damages, if any, recovered, by Thompson Reuters should be interesting to follow.

A New York Court Holds that Employee Choice Doctrine Does Not Apply to Equitable Relief in a Non-Compete Matter

By David Monachino (March 2, 2012)

Employers often condition the payment of post-employment or deferred compensation on a departing employee's compliance with a noncompete agreement. New York is one of the few states that specifically allow for such an arrangement under the "employee choice" doctrine. This doctrine holds that an employee who chooses to voluntarily resign and violate his or her noncompetition obligations can be deemed to have waived any legal right to post-employment compensation, but does not require the agreement to pass the test of "reasonability" to which noncompete agreements in New York are generally subject. The employee choice doctrine is based on the premise that a resigning employee is given the choice of either preserving his or her right to compensation by refraining from engaging in competitive employment, or forfeiting that right by choosing to compete with a former employer.

A New York court has recently declined to allow the employee choice doctrine to apply to applications for equitable relief. In *Richard Manno & Co., Inc. v. Manno*, 2012 WL 488252 (N.Y.Sup., Suffolk Co. Feb. 6, 2012), respondent, Anthony Manno, was employed by the petitioner, a company which manufactures and sells steel fasteners and machined parts in the United States. In October of 2010, the petitioner and respondent entered into a severance agreement, which, in part, provided for future lump sum payments as well as monthly and other periodic payments for designated terms. The payments were conditioned upon certain post employment obligations by Mr. Manno, a violation of which would contractually result in the forfeiture of future payments.

The petitioner claimed that in or about January of 2011, respondent violated the severance agreement by forming a competing company and sought injunctive relief in aid of arbitration for monetary damages. The New York court denied the application assuming, without so finding that the subject severance agreement contains a non-compete restrictive covenant, it "would not be enforceable without regard to the standards of reasonableness which covenants not to compete are regularly measured." The court also noted that the "[a]pplication of the reasonableness standard is consistent with [a prior Court of Appeals decision that noted] that the 'employee choice doctrine' exception is applicable only in cases involving economic relief and not to those for injunctive relief."

New Ninth Circuit Case Aids Departing Employees In Non-Compete and Non-Solicit Disputes Involving Race To Judgment

By James D. McNairy (March 5, 2012)

Contractual choice of law provisions often seek to apply the law of the state that, when applied by a court to the contract at issue, is most likely to result in favorable interpretations, application, and/or enforcement of those provisions in the contract most valued by the contracting parties. However, when the law chosen is of a state different than the state in which the contract appears to be headed for litigation, the parties to the contract may "race" to get their respective lawsuits on file and obtain a judgment in the jurisdiction that they perceive most favorable to their position.

Given the patchwork of laws from state-to-state concerning the enforceability of non-compete and non-solicitation agreements, choice of law provisions in agreements containing such clauses is often a significant strategic consideration.

The Ninth Circuit's recent decision in *Ruiz v. Affinity Logistics Corp.*, 2012 WL 388171 (9th Cir. February 8, 2012), likely will be applied in "race to judgment" cases to argue that the law of the state with the greatest connection to the negotiation, subject matter, and performance of the underlying contract should be applied to the issues in suit. In *Ruiz*, the Ninth Circuit held that a contractual choice of law provision calling for the application of Georgia law was unenforceable because California had a materially greater interest than Georgia in the outcome of the case. See Seyfarth's One Minute Memo for a fuller description of *Ruiz*.

The *Ruiz* court analyzed five factors in determining whether California had a materially greater interest than Georgia in determining the issues in suit: (1) the place of contracting, (2) the place of negotiation for the contract, (3) the place of performance, (4) the location of the subject matter of the contract, and (5) the domicile, residence, nationality, place of incorporation, and place of business of the parties. The Ninth Circuit's factors, which are somewhat reminiscent of a "minimum contacts" analysis used to determine personal jurisdiction, place an emphasis on tying the chosen law to the state where the parties actually spent most to their time creating, entering into, and performing the contract.

While only time will tell, it is likely that the five factors applied in *Ruiz* will be used by litigants in the Ninth Circuit to argue against the enforceability of choice of law clauses applying the law of a state

where the functional connections set forth in *Ruiz* do not exist. Given this, parties may do well when drafting choice of law provisions to, where possible, choose the law of a state where the functional connections set forth in *Ruiz* may be satisfied.

Trading Secrets

Massachusetts Court Finds IT Consultant's Non-Compete Agreement Unenforceable Due to "Material Change" in Employment Relationship

By Kate Perrelli, Erik Weibust, and Ryan Malloy (March 6, 2012)

In *Grace Hunt IT Solutions, LLC v. SIS Software, LLC, et al.*, Judge Lauriat of the Business Litigation Session of the Massachusetts Superior Court recently held that an IT consulting firm could not enforce non-compete agreements against employees who left after the company decreased their base salaries and implemented a new compensation structure in which employees could earn bonuses based on billable hours that equaled or exceed the amount of their previous base salaries, because the change materially affected the employment relationship.

Plaintiff Grace Hunt IT Solutions, LLC ("Grace Hunt") provides software management consulting services. Pursuant to an Asset Purchase Agreement effective September 30, 2011, Grace Hunt became the successor and assignee of Grace Hunt, LLC, of which defendants John S. Joyce, George Olsen, and Robert Remick were all employees. Pursuant to the purchase, defendants became employees of Grace Hunt.

Defendants Joyce and Olsen had previously signed non-compete agreements with Grace Hunt, LLC. After the purchase, Grace Hunt sent the individual defendants offer letters outlining the terms of their employment, each of which included a provision stating that they would be required to sign a new non-compete agreement.

They were also told that the Grace Hunt planned to implement a different compensation structure and change eligibility for fringe benefits. According to the defendants, their base salary was decreased by 20 percent, but they were informed that they could earn the difference through bonuses based on billable hours. The individual defendants signed and returned their offer letters, but they refused to sign the non-compete agreements that accompanied those letters.

In late October 2011, SIS Software, LLC ("SIS"), a software consulting company based in Georgia, contacted Joyce about opening a Boston office. Knowing that Olsen and Remick were unhappy at Grace Hunt, Joyce forwarded them SIS's contact information. SIS made all three employment offers and, in early December, they all resigned from Grace Hunt. Each defendant informed certain clients

that they were leaving Grace Hunt, though they claim that they did not encourage clients to switch consultants. According to Grace Hunt, several clients ultimately moved their business to SIS.

On January 6, 2012, Grace Hunt filed a breach of contract claim against all defendants in the Superior Court, alleging that, while still employed by plaintiff and shortly thereafter, the individual defendants communicated with and solicited its clients on behalf of SIS. Additionally, Grace Gunt sought to enforce the defendants' original non-compete agreements against them.

Judge Lauriat found that, although the original non-compete agreements sought to protect a legitimate business interest (customer goodwill), they were nonetheless unenforceable because, under Massachusetts law, non-compete agreements are voided by "material changes" in employment relationships between employees and employers. In making a determination as to whether there was such a material change in the relationship, "courts have considered it extremely significant that the employer sought to have the employee[s] sign a new non-compete agreement."

The Court concluded that defendant Remick could not be bound by the terms of the non-compete agreement because he never signed any employment or non-compete agreement with Grace Hunt, LLC. As to Joyce and Olsen, sufficient evidence suggested that the change in their compensation plan was significant. That their fringe benefits were better, Judge Lauriat held, is "immaterial" because "under the new compensation plan, Joyce and Olsen would have made significantly less, at least until there was sufficient work to enable them to bill enough hours to be eligible for bonuses."

The case serves to warn employers that any material change in the employer-employee relationship, including a compensation package modification, may void a non-compete agreement.

California Federal Court Ships California Employee's Declaratory Relief Action Seeking To Invalidate His Non-Compete To Pennsylvania

By Jessica Mendelson (March 8, 2012)

On February 27, 2012, a California federal judge for the Northern District of California, decided the case of *Hegwer v. American Hearing and Associates*, finding that the alleged illegality of a non-compete clause in an employment agreement involving a California employee has no bearing on a legal forum selection clause. Accordingly, the Court transferred the employee's declaratory relief action to Pennsylvania federal court.

Plaintiff Jay Hegwer initially filed suit against his former employer, Defendant American Hearing and Associates alleging three state claims: declaratory relief, fraud, and unfair business practices.

According to the court's decision, Hegwer had been searching for a job in early 2010, and contacted a corporate recruiter, John Frank, who passed his resume to David Young, the regional manager for AHAA. Young contacted Hegwer to arrange an interview, and at the time, Hegwer advised him that he required a salary of $150,000. Young and Frank both informed Hegwer that the associate manager position they were considering him for paid a base salary of $100,000 per year, but that he could expect to earn $50,000 in commissions annually. Hegwer was hired as an associate manager, and signed an employment agreement containing a provision stating that all litigation arising out of or related to the agreement would take place in Chester County, Pennsylvania. The agreement also contained an arbitration clause, a non-solicitation/non-competition clause, and a choice of law clause specifying the agreement was governed by Pennsylvania law.

According to the decision, soon after he was hired, Hegwer went to Pennsylvania for a training session led by another employee, Deonda Weldon ("Weldon"). Weldon allegedly told Hegwer that only one company employee actually made any sort of commission, and that if he truly expected to make $50,000 in commissions, he should just "quit now." In June, Hegwer was terminated for allegedly sexually harassing a fellow trainee, a claim he believes was fabricated by Weldon.

Hegwer filed suit in California state court, in Marin County. AHAA removed the case to federal court on the basis of diversity jurisdiction, and then moved to have the case dismissed for improper venue, or to be transferred to Pennsylvania.

Hegwer argued that the forum selection clause should not be enforced because the other provisions of the employment agreement, including the arbitration, non-compete and non-solicitation clauses, were unenforceable under California law. The court dismissed this argument, finding that whether other provisions of the agreement were unenforceable was irrelevant to the enforceability of the forum selection clause. Hegwer also argued that the enforcement of the forum selection clause would prevent him from having his day in court, since the case would be sent to arbitration. The court found this argument speculative and unpersuasive.

Finally, Hegwer argued that he would not be able to pursue the case if it took place in Pennsylvania, because of the extensive travel costs. The court found that given Hegwer currently resides in Wyoming, the cost would be similar to travel to either Pennsylvania or California, and as a result, Hegwer had failed to show that enforcement would deprive him of his day in court.

Ultimately, the court found the forum selection clause was enforceable, and venue was improper in California. The court relied on *M/S Bremen v. Spata Off-Shore Co*., where a forum selection clause is considered unreasonable, and thus, unenforceable if: the inclusion of the clause was a product of fraud, undue influence, or an imbalance of power, (2) the forum is so gravely difficult and inconvenient that the party challenging the clause will for all practical purposes be deprived of its day in court, or (3) the clause would contravene a strong public policy of the forum where the suit was brought. 407 U.S. 1, 15 (1972). Here, Hegwer failed to show the clause was gravely inconvenient, and therefore the case was transferred to the Eastern District of Pennsylvania.

The court's ruling in *Hegwer* is in line with traditional rulings on the subject. The courts have routinely rejected notion that "expense or inconvenience of prosecuting an action in the designated forum" rises to the level of depriving one's day in court. *R.A. Argueta v. Banco Mexicano*, 87 F. 3d 320 (9th Cir. 1996).

Texas Appellate Court Voids, As Contrary to Fundamental Texas Law, Incentive Compensation Contract Imposing A Substantial Penalty For Post-Employment Competition With The Ex-Employer

By Paul E. Freehling (March 13, 2012)

Under Texas law, a restraint on competition without reasonable time and geographical limitations is unenforceable. Although New York generally disfavors an unreasonable non-competition covenant, there is an exception under the employee-choice doctrine. A recent Texas appellate court panel, applying Texas law, reversed a lower court order declaring valid under New York law an employment contract provision imposing a substantial penalty on a 30-plus year Exxon Mobil employee based in Texas who retired and then went to work for a competitor. *Drennen v. Exxon Mobil Corp*., No. 14-10-01099-CV (14th Tex. App., Feb. 14, 2012).

Over the years, Drenner was the recipient of incentive compensation in the form of 73,900 shares of restricted Exxon Mobil stock registered in his name and "earnings bonus units" which entitled him to share in the company's earnings under certain circumstances. The incentive program allowed Exxon Mobil to cancel an incentive award to anyone who engaged in activity detrimental to the interests of the corporation as determined by the program administrator. A choice-of-law provision designated New York law although there was an exception for certain foreign nationals which provided for accommodation of "local laws, tax policies, or customs" of the foreign countries.

Shortly before Drenner retired, Exxon Mobil requested him to notify senior management if, within two years, he intended to accept a position with a competitor. Complying, he notified his former supervisor that he was considering acceptance of a senior officer position with Hess Corporation, a competitor of Exxon Mobil.

The supervisor warned Drenner that a consequence would be loss of all of his incentives. Nevertheless, he accepted a position as senior vice president of Hess whereupon Exxon Mobil cancelled his restricted stock and earnings bonus units. He sued Exxon Mobil in a Texas state court, seeking a declaration that the cancellation was unlawful. The trial court ruled against him, and he appealed. The only issues involved questions of law.

Under the employee-choice doctrine, New York courts hold that an employee is not unreasonably restrained if the employee is free to choose between (a) preserving economic benefits by refraining from competition, and (b) risking forfeiture of those benefits by exercising his right to compete. The Texas appellate court held "that under New York law, the detrimental activity provisions [of the incentive program] are covenants not to compete and are enforceable under the employee-choice doctrine." The court cited a Texas statute which, by contrast, provides that "a noncompetition agreement is enforceable [only] if it contains limitations as to time, geographical area, and scope of activity to be restrained that are reasonable and do not impose a greater restraint than is necessary to

protect the goodwill or other business interest of the employer." Continuing, the court held that "Because Exxon Mobil's detrimental activity provisions meet none of these requirements, they are unenforceable under Texas law." The dispositive question was which state's law applies.

The court concluded that Texas has a materially greater interest that New York in the determination of enforceability. First, Exxon Mobil is headquartered in Texas, Dreener lives and worked there, and he signed the agreements in that state. "Second, issue of whether non-competition agreements are reasonable restraints upon employees who live and work in this state is a matter of fundamental Texas public policy." Third, "the rationale underlying [the employee-choice] doctrine has been rejected by both the Texas legislature and the Texas Supreme Court." Finally, Exxon Mobil's contention that it has a strong interest in uniform application of its employment agreements was refuted by the exception for accommodation of local laws and policies for foreign nationals, and "If creating this exception does not significantly impede Exxon Mobil's operations, we conclude that making the same accommodation for a long time Texas resident, whose work was in Texas and who signed the agreements in Texas, similarly would not be excessively disruptive."

This case teaches that choice-of-law provisions may have to yield to the law of a different state whose fundamental public policy is paramount. Further, the decision reinforces the principle that a substantial loss of benefits as a price for competing is the equivalent of a non-competition clause.

Fireworks Fly, California District Court Enjoins Former Pyrotechnics Company Employee From Soliciting Former Employer's Customers

By James D. McNairy (March 30, 2012)

On March 21, 2012, in the case of *Pyro Spectaculars, Inc. et al. v. Souza*, Case No. 12-CV-00299-GGH, Magistrate Judge Gregory G. Hollows of the USDC for the Eastern District of California (Sacramento Division), issued and order preliminarily enjoining a former Account Executive for a pyrotechnics company from soliciting the customers of his former employer. There are several notable aspects of this decision:

Employee Mobility vs. Protection of Trade Secrets

In analyzing the "public interest" considerations involved in potentially issuing a preliminary injunction, the court weighed the competing public interests related to California's strong public policies favoring on the one hand employee mobility, and on the other hand, protection of trade secrets. The court decided to issue a time-limited injunction intended to prevent misuse of Plaintiff's trade secrets while allowing lawful competition. In so doing, the court made some statements useful to California employers:

- Given that Defendant was subject to a non-solicitation agreement, the court took care to not run afoul of Business and Professions Code section 16600, which presumes that contracts restraining one's right to engage in a lawful business, trade or profession are void. Specifically, the court granted a "narrow, time-limited non-solicitation restriction&to prevent defendant's misuse of [Plaintiff's] trade secret information in competing with [Plaintiff]." The court found the non-solicitation restriction particularly justified given Defendant's alleged surreptitious downloading of Plaintiff's information, use of wiping software to cover his tracks, and failure to account for several thumb drives notwithstanding the court's order that he do so.

- As to the likelihood of irreparable harm element required for injunction, the court observed that "damage to a business's goodwill is often very difficult to calculate". This is a useful finding for rebutting arguments that damages are sufficient to address a plaintiff's alleged harm and thus injunctive relief should be denied. This may be particularly so where customer list trade secrets are at issue because the goodwill of

> customer relationships is often closely related to, if not bound up with, the at issue trade secrets.

The Viability of "Customer Lists" as Trade Secrets: Defendant argued that Plaintiff's customer lists did not constitute trade secret information

The court found that, although several information components that comprised Plaintiff's trade secrets were publicly available, the software used by Plaintiff provided a "virtual encyclopedia" of specific Plaintiff customer, operator, and vendor information allowing a competitor to solicit Plaintiff's clients "more selectively and more effectively without having to expend the effort to compile the data". See *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1522 (1997). Appealing to common sense, the court also noted, if Plaintiff's customer list was so readily available, "why was it necessary for defendant to surreptitiously download, retain, and funnel...[Plaintiff's] information to his new employer in the first place."

Trade Secrets Retained in One's Memory May Serve as a Basis to Enjoin Solicitation of a Company's Competitors

Defendant's other questionable conduct caused the court to be "skeptical" that an injunction requiring defendant to merely return Plaintiff's information "will be sufficient to protect against misuse of [Plaintiff's] trade secrets." Importantly, the court further found that:

> This skepticism is reinforced by the fact that defendant's probable misappropriation thus far has "so tainted defendant's base of knowledge that it would be very difficult, at least over the next several months, for defendant to separate his general pyrotechnics information and skills from [Plaintiff's] legitimate trade secrets when competing with [Plaintiff].

While California court's do not recognize the so-called "inevitable disclosure" doctrine, the *Pyro Spectaculars* court's injunction and above reasoning is not an articulation of that doctrine. The inevitable disclosure doctrine as applied in its purest form may be used in the absence of any wrongdoing by defendant to enjoin defendant from assuming employment with a competitor because allowing defendant to do so would cause defendant to "inevitably disclose" his former employer's trade secrets due to the similarity of the duties defendant will have in his new job relative to the duties of his prior job. See *Pepsico v. Redmond*, 54 F. 3d 1262 (7th Cir. 1995).

In contrast, here the court found that, based on evidence of record, Defendant's conduct was so unreliable and that his probable misappropriation had "so tainted his base of knowledge" that defendant would not be able to segregate his general knowledge and skills from Plaintiff's legitimate trade secrets when competing with Plaintiff.

Although such reasoning and related injunction appear powerful indeed, the court tempered this aspect of its reasoning by imposing the qualification in the injunction that Defendant was enjoined only from initiating contact with Plaintiff's current customers. If Defendant's alleged bad acts have "so tainted

defendant's base of knowledge that it would be very difficult...for defendant to separate his general pyrotechnics information and skills from [Plaintiff's] legitimate trade secrets", query whether the initiating contact limitation is sufficient to fully protect Plaintiff's trade secrets?

Perhaps anticipating this, the court noted that Plaintiff could use ongoing discovery to monitor compliance wit the preliminary injunction and seek damages if evidence showed any use by defendant and/or his new employer of Plaintiff's trade secrets.

The court's decision provides some comfort to California employers that there are at least some rules, even in California, to protect employers from former employees who steal company data and embark on campaigns to flip valuable customer relationships.

For Whom the Employment Agreement Tolls: New York State Appellate Court Applies Equitable Tolling Doctrine In Non-Compete Dispute

By David Monachino (March 31, 2012)

An important procedural issue that often arises in a non-compete dispute is the idea of equitable tolling. This doctrine essentially allows a court to toll, or stay, the time remaining on a non-compete agreement during the period in which the employee is in breach. Equitable tolling, however, is not always available, and the remedy is highly dependent on what state's law governs the agreement. A New York Appellate Court recently upheld the doctrine where the agreement expressly provided for equitable tolling.

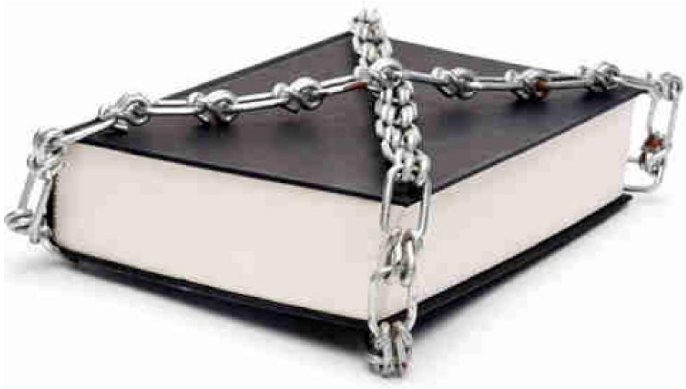
In *Delta Enterprise Corp. v. Cohen*, Delta Enterprise Corp. manufactures and sells furniture and other products for infants, toddlers and children. Its longtime employee, Ralph Cohen was the co-head of the Toddler Furniture Division when he left the company in early 2010. Delta alleged that Mr. Cohen misappropriated confidential information from Delta, and started a competing business while he was still employed with Delta in violation of a two year non-compete and non-solicit agreement.

Delta sued Mr. Cohen nearly a year later after he left Delta and obtained both temporary and preliminary injunctive relief from the trial court prohibiting him from, among other things, engaging "in business with any of the factories with which Delta conducted business" and "interfering with or disrupting any relations between Delta and any of its customers, licensors, employees or vendors...." for two years after the end of his employment.

Although successful in the lower court, Delta appealed the decision arguing that the tolling provision in its employment agreement should be enforced from any period in which Mr. Cohen was in violation of the employment agreement and not just from the end of his employment. The New York Appellate Division (First Department) agreed and modified the preliminary injunction to extend two years from the date of issuance of the temporary restraining order or resolution at trial, whichever is earlier.

Employer Who Sued Former Employees to Enforce Non-Competition Clauses Did Not Violate Indiana's Blacklisting Statute

By Paul E. Freehling (April 3, 2012)



Indiana and several other states statutorily prohibit employers from "blacklisting" former employees, that is, attempting to prevent them – whether they were discharged or resigned – from obtaining subsequent employment. Responding recently to certified questions from the U.S. District Court for Southern Indiana, the Indiana Supreme Court held that former employer Loparex, LLC did not violate the statute when it sued (unsuccessfully) for an injunction to enforce a non-competition agreement signed by two ex-employees, one who was terminated and another who left voluntarily. *Loparex, LLC v. MPI Release Technologies, LLC*, 2012 WL 955426 (Ind. Sup. Ct. Mar. 21, 2012). In reaching that result, the Supreme Court rejected its almost century-old decision in *Wabash R.R. Co. v. Young,* 162 Ind. 102, 69 N.E. 1003 (1904).

Loparex makes "release liner" products such as nametags with peel-off backings, window films, and roofing underlayment. The formulas involved in these products allegedly are trade secrets. Odders and Kerber were employees of that company who had in-depth knowledge of its confidential information. Both were subject to one-year non-compete agreements. Odders was discharged and went to work for MPI, a competitor of Loparex. Kerber resigned from Loparex and also commenced employment with MPI.

Loparex asked the Southern District of Indiana federal court to enjoin Odders and Kerber from working for MPI (initially, Loparex requested injunctive relief from MPI too, but later withdrew the request). Odders and Kerber denied wrongdoing and counterclaimed for damages, including attorneys' fees, contending that their ex-employer violated the Indiana Blacklisting Statute, Ind. Code §22-5-3-2, by filing the lawsuit. The district court overruled Loparex's motion to dismiss the counterclaim and granted summary judgment to Odders and Kerber on the company's complaint. Then, the federal court certified three questions to the Indiana Supreme Court each of which that court now has answered in the negative: Does an ex-employer violate the Blacklisting Statute by suing to enforce non-competition agreements signed by former employees? Is the decision in *Wabash R.R. Co. v. Young* still good law? Are attorneys' fees recoverable as compensatory damages in a suit for violating the Blacklisting Statute?

A number of states besides Indiana have blacklisting laws. The Supreme Court made specific reference to statutes in Arizona, Iowa, Kansas, North Carolina, Ohio, and Oklahoma. According to the court, the majority of cases arising under those statutes hold that the employer's conduct, whatever it happened to be, was not prohibited, and the principle to be gleaned by from the few decisions against employers is that they incur liability only where they act "with the wrongful intent to inhibit or prevent [former] employees from obtaining future employment." The court continued: "Simply put, a lawsuit – successful or not – to protect trade secrets or seeking to enforce a noncompetition agreement does not, on its own, fall within that scope." The court added that filing baseless or sham actions to restrain employees' subsequent employment may constitute common law torts such as malicious prosecution and abuse of process, and may violate Federal Rule of Civil Procedure 11 and state counterparts, and antitrust laws.

Turning to the *Young* decision, the court pointed out that the title of the Indiana Blacklisting Statute mentions protection of discharged employees but is silent regarding employees who resign. The law's text, however, safeguards employees who leave their positions voluntarily as well as those who are fired. At the time *Young* was decided, in 1904, Article 4, Section 19, of the Indiana Constitution mandated that statutes "embrace but one subject and matters properly connected therewith; which shall be expressed in the title." Because the title of the Blacklisting Statute made no reference to employees who resigned, in Young the Indiana Supreme Court invalidated the portion of the blacklisting statute that concerned them.

The holding in *Young* has been relied on many times since 1904, but in several other cases courts have found ways to distinguish it. According to the Supreme Court in *Loparex*, the rationale for the ruling in *Young* – whether it was right or wrong in 1904 – has been undermined by subsequent amendments to the Constitution and because "a good many cases analyzing challenges to statutes under Section 19 have employed a more accommodating approach than that taken in Young." So, in response to the certified question, the Indiana Supreme Court held that *Young* "is no longer stare decisis on the question of whether an employee who voluntarily leaves her employment may pursue a claim under the Blacklisting Statute."

The court had little trouble rejecting the proposition that an employee who prevails in a blacklisting case is entitled to attorneys' fees as part of compensatory damages. After summarizing the American and British rules on attorneys' fee awards, the Supreme Court held that "there is nothing about the language, history, or nature of Indiana's Blacklisting Statute that points to anything other than application of the American Rule."

Employers in Indiana, and perhaps other states with blacklisting laws, can breathe a bit easier now that the Indiana Supreme Court clearly has held that, under that state's law, filing a lawsuit to enforce a non-competition agreement – whether the plaintiff is or is not successful, and whether the defendant is an employee who was fired or who resigned – does not constitute blacklisting.

Colorado Federal Court Decision In Non-Compete Dispute Demonstrates Importance Of Drafting Enforceable Forum Selection Provisions In Business Transactions

By Robert Milligan (April 6, 2012)

As part of the process of acquiring of a business and retaining key employees of the acquired business, multiple agreements surrounding the parameters and contingencies of the transaction are often drafted, including asset purchase agreements and employment agreements. These agreements sometimes overlap in scope and ensuring that all material aspects of the deal align in the documents is crucial in maintaining the effectiveness of any singular business transaction. In an order denying defendant's motion to dismiss in a non-compete dispute involving a former key executive of the purchaser, the Honorable Judge R. Brooke Jackson of the United States District Court for the District of Colorado illustrated the importance of congruity within these sorts of agreements, particularly forum selection provisions. The bottom line is that special care needs to given in the drafting of these documents so that the non-compete provisions and forum selection provisions remain consistent.

The case, *Robert Stuart v. Marshfield Doorsystems, Inc.* Civil Action No. 12-cv-00454-RBJ, 2012 WL 872766 (D. Colo. March 14, 2012), concerns a dispute over agreements signed during defendant's acquisition of plaintiff's company and retention of his employment services. In 2004, Stuart and his business partner David Cox sold Consolidated Fiber, LLC, which deals in the manufacturing and selling of commercial and residential doors, to Marshfield Doorsystems. By the terms of the Asset Purchase Agreement ("APA"), Stuart and Cox received $2 million each and agreed to stay with the company and sign separate employment agreements. The APA included reference to unsigned employment agreements that were attached as exhibits and incorporated by reference.

The APA included a non-competition clause that barred them from joining a competing business for 24 months after the termination of their employment agreements. Additionally, the APA stipulated it would be governed by Delaware law, where Marshfield is incorporated, and that "any dispute, controversy or claim arising out of or relating to" the APA would be settled through arbitration in Chicago, IL. Any dispute not able to be settled through arbitration would then be settled in an applicable court in Chicago.

In concordance with the APA, Stuart signed an Employment Agreement with Marshfield that had him under contract for a five year "Initial Term." Per the Employment Agreement's "Renewal Terms" the contract was extended automatically at the end of the Initial Term for one year every year unless terminated by either party through 45 days advance notification. Stuart's Employment Agreement contained a non-competition clause largely identical to the one found in the APA, but, in contrast with the APA, provided that any and all disputes "arising out of or related to" the Employment Agreement were to be resolved by a court trial without a jury. Moreover, the Employment Agreement contained a merger clause stating that it "merges and supersedes all prior and contemporaneous discussions, agreements and understandings of every nature between the parties hereto relating to...employment." The APA and Employment Agreements were apparently executed on the same day.

After the Initial Term had passed, in addition to three subsequent Renewal Terms, Stuart informed Marshfield on January 9, 2012 that he intended to resign approximately four weeks later. A few days after this, Stuart informed Marshfield that upon his departure, he would be joining TruStile Doors, LLC in Denver, CO. Marshfield terminated Stuart's employment on January 17, 2012 and cited the non-competition clauses of the APA and his Employment Agreement in insisting he quit his job with TruStile Doors, which Marshfield considers a competitor. Marshfield also informed TruStile Doors of Stuart's agreements and pressed them to terminate his employment.

On February 22, 2012, Stuart filed a complaint in federal court in Denver, Colorado against Marshfield seeking a declaration that the non-competition agreements are not enforceable, or that they were waived, or that they were not violated, as well as an injunction against Marshfield from interfering with his employment at TruStile Doors. In response, Marshfield requested arbitration through the American Arbitration Association to settle the arbitrable aspects of the dispute in Chicago, per the APA. Marshfield also filed a complaint against Stuart in the United States District Court for the Northern District of Illinois, Eastern Division, seeking an order from the court for arbitration as well an injunction barring Stuart from working at TruStile Doors. Similarly, Marshfield filed a motion to dismiss Stuart's complaint filed in the Colorado federal action due to improper venue based on the forum selection clause found in the APA, as well as motion to transfer venue based upon forum non conveniens.

In denying Marshfield's motion to dismiss, the court determined that the Employment Agreement is a "stand-alone contract with no forum selection clause" that has governed the employment relationship since its signing. Additionally, due to the language of the merger clause providing that it "merges and supersedes all prior..,agreements," the Court ruled that the Employment Agreement merges and supersedes any inconsistent provisions in the APA.

The Court reasoned:

> Because it requires a court trial, it is not governed by the APA's arbitration clause. Because it has no forum selection clause, Mr. Stuart is not precluded from instituting a lawsuit outside Chicago. . . .

> Marshfield argues that the parties clearly intended that any disputes under the APA would be resolved by arbitration or litigation in Chicago. However, while the APA so provides in general, the Employment Agreement does not. **The parties could have put an arbitration clause and a forum selection clause in the Employment Agreement, but they did not.**
>
> Marshfield argues that the Employment Agreement was incorporated into and became a part of the APA. I do not agree. The APA incorporated by reference its exhibits which, as relevant here, were facsimile forms of employment agreements. Mr. Stuart was required to agree to an actual employment agreement in substantially the same form as the facsimiles, which he did. **However, as indicated above, the Court finds that the actual Employment Agreement by its plain language stands on its own as an independent contract.**" (emphasis added)

Accordingly, the court denied the motion to dismiss on grounds of improper venue. The court also denied Marshfield's request to transfer the case to the Northern District of Illinois. The court reasoned that neither party had significant contract with Colorado or Illinois. Delaware law could be determined and applied by either court. The court stated that there was no basis to find that it would be difficult or expensive to obtain or present relevant evidence in Colorado or that either party would not receive an equally fair trial or enforcement of judgment would be more difficult in either forum. The court noted that arguably that there could be duplicative litigation and inconsistent outcomes but that it would not interfere with the current Illinois action and that "by insisting on litigating in Colorado, Mr. Stuart has chose to run the risk of having to litigate in two places."

When dealing with complex transactions such as the acquisition of an entity, companies should be sure to place a high premium on attention to detail, including non-compete and forum selection provisions. Ensuring that all aspects of a deal, from purchase agreements to employment contracts, have been carefully drafted with every potential contingency accounted for can be a tedious task. However, doing so can save a company significant money by mitigating the number and impact of future disputes. Contract provisions such as a forum selection clause may appear trivial until they are forgotten. In the case of *Stuart v. Marshfield*, consistent forum selection provisions in the APA and Employment Agreement would likely have allowed Marshfield to secure a favorable forum for all disputes between the parties, extinguished Stuart's attempt to secure a perceived more favorable forum, and provided Marshfield with greater certainty and less expense in the enforcement of the non-compete provision against Stuart.

Sale of Business "Good Will" and Subsequent Competition with Purchaser May Subject Seller to Perpetual Restrictions on Contacting Former Customers and Clients

By Paul E. Freehling (April 12, 2012)

A recent Second Circuit Court of Appeals decision provides guidance regarding New York law concerning permissible and impermissible competitive conduct by the seller of a business, including its "good will," who – without giving a non-compete covenant – thereafter goes into competition with the purchaser. The Second Circuit was aided by New York's highest court which answered certified questions concerning the proper interpretation of the so-called "*Mohawk* doctrine." The Second Circuit held that, in perpetuity, the seller may not disparage the purchaser, may not actively solicit former clients/customers but may respond truthfully to factual questions posed by them on their own initiative, may not provide the new employer with information that is proprietary to the purchaser but may assist in developing a plan to attract former clients/customers, and may attend meetings with them but must take a largely passive role. *Bessemer Trust Co., N.A. v. Branin*, Docket Nos. 08-2462-cv(L) and 08-2677-cv(XAP) (2d Cir., Apr. 5, 2012).

Defendant Branin sold the assets of his investment portfolio management business to Plaintiff Bessemer Trust. The assets included client accounts and "good will." He did not give Bessemer a non-compete covenant. After the sale, Branin worked for Bessemer for a short time, but then resigned and joined competitor Stein Roe Investment Counselors. Branin made no promises to Stein Roe that his clients would follow him, but communicated his hope that 80 % of the $2.3 million in revenue he had been generating for Bessemer would transfer to Stein Roe within a year. Before leaving Bessemer, Branin did not inform any of his clients of his impending move.

After Branin commenced employment with Stein Roe, he did not initiate contacts with his former clients. When they asked why he had left Bessemer, he gave mostly benign responses (for example, that Stein Roe's method of dealing with clients is "more appropriate for my training and experience"). Bessemer sued Branin when the large Palmer family account that he had been managing for 15-20 years transferred to Stein Roe.

The Palmer family's representative had called Branin and inquired about his reasons for leaving Bessemer. When Branin gave his standard answer, the representative requested a meeting to discuss how the account would be managed if it was moved to Stein Roe. Branin helped Stein Roe prepare by providing information about the Palmer family and the family's investment philosophy. Branin attended the meeting between the Palmer family and Stein Roe, but took a passive role, apart from making introductions and occasionally amplifying a point. Afterwards, the Palmer family invited Branin to their home to make a specific proposal. Branin accepted the invitation and, while there, told them that Stein Roe's fees would be the same as Bessemer's and that the president of Stein Roe would be the number two person on the account. The Palmer family transferred their account to Stein Roethe next day.

Relying on *Mohawk Maintenance Co. v. Kessler,* 52 N.Y.2d 276, 283, 419 N.E.2d 324, 328 (1981) – "the vendor is not at liberty to destroy or depreciate the thing which he has sold; there is an implied covenant on the sale of 'good will' . . . not to solicit the customer which he has parted with; it would be a fraud on the contract to do so" – the district court held that Branin had violated New York law with regard to the Palmer account and awarded Bessemer $1.25 million. Both parties appealed.

The federal appellate court initially concluded that under New York law, the principles set forth in Mohawk were unclear as applied to the facts of the Bessemer-Branin litigation. Accordingly, the Second Circuit certified several questions about the Mohawk doctrine to the New York Court of Appeals. Based on the answers, the federal appellate judges concluded that the district court judge erroneously focused on Branin's intentions rather than his actions. Therefore, the district court's judgment for Bessemer was vacated, and the case was remanded for further proceedings.

This decision teaches that the buyer of a personal services business (and other purchasers of "good will") should insist on a covenant not to compete from the seller. Bessemer's failure to do so has cost the company millions of dollars in lost revenue and enormous legal fees (there have already been five published opinions over the course of the litigation's six years, and it isn't over). Under the rules articulated by the New York Court of Appeals, some of which may be a bit naïve (is it believable that sellers of "good will" with long-standing business relationships will forego all meaningful communications with former clients/customers in perpetuity?), absent a covenant future sales of "good will" followed by the seller's entry into competition could generate similar fact-intensive and expensive lawsuits.

Washington Appellate Court Finds That Employer's Threatening Letter, Relying In Part On Inevitable Disclosure Doctrine, to Former Employee's Prospective Employer Is Not Actionable

By Jessica Mendelson (June 16, 2012)

In *Moore v. Commercial Aircraft Interiors*, 2012 WL 1947890 (Wash. Ct. App., May 29, 2012), a Washington Appeals Court held that a former employee suing his former employer for tortious interference with business expectancy must show actual evidence and not simply conclusory statements of his alleged former employer's improper purpose, in order to recover.

Robert Moore ("Moore") worked for Commercial Aircraft Interiors ("CAI") from 2003 until his voluntary resignation in 2008. Moore never signed a non-compete agreement with the company, but did sign a nondisclosure agreement intended to protect CAI's confidential, proprietary, and trade secret information.

A few months after his resignation from CAI, CAI began merger negotiations with a competitor, Volant Aerospace Holdings LLC ("Volant"). The companies hired Moore as an "independent consultant" to assist with negotiations. As part of his employment, Moore signed contracts with both companies prohibiting the disclosure of trade secrets, finances or "other know-how" to third parties.

After a few months, negotiations between the parties broke down. Moore went back to work at CAI., but was laid off by about three months later. Later that year, Moore applied to Volant, which seriously considered hiring him, but was hesitant to do so without CAI's blessing. As a result, Volant's president wrote to CAI asking for the company's acknowledgement that hiring Moore was not objectionable and would not violate any legal agreement. CAI responded, via counsel, that the company opposed Moore's hiring, and that as a Volant employee, Moore could not "avoid the use of or disregard the infinite knowledge he possesse[d] of CAI's confidential information and trade secrets." CAI threatened litigation for unfair competition if Volant were to hire Moore.

As a result of the letter, Moore failed to obtain employment with Volant, and sued CAI, alleging tortious interference with a business expectancy and blacklisting. The trial court granted summary judgment for CAI, finding Moore had failed to state sufficient evidence that CAI had acted in bad faith or with malice. Moore appealed to the Court of Appeals, which affirmed the summary judgment.

In affirming the trial court's ruling, the Court of Appeals found the burden was on Moore to establish the elements of tortious interference. To do so, he would need to prove the existence of five elements: "(1)existence of a valid contractual relationship or business expectancy, (2) that defendants had knowledge of that relationship, (3) an intentional interference inducing or causing a breach or termination of the relationship or expectancy, (4) that defendants interfered for an improper purpose or used improper means, and (5) resultant damage.

Here, however, the court found Moore failed to show improper means or purpose. Although Moore argues CAI's threat of litigation provided sufficient proof, the court found "threatened lawsuits may constitute an interference by improper means only where the interferor has no belief in the merit of the litigation or threatens litigation only to harass the third parties and not to bring his claim to definitive adjudication." Here, the burden of proof was on Moore to show the litigation was not in good faith, and the two sworn declarations provided were merely conclusory, and as such, insufficient evidence.

Similarly, the court dismissed Moore's argument that CAI failed to act in good faith, because their reasons for legal action relied on the inevitable disclosure doctrine, rather than any actual threat of trade secret disclosure. This doctrine, which, in some jurisdictions, prevents an employee from going to work for a competitor by demonstrating the employee would inevitably disclose trade secrets, has never been expressly adopted by the Washington courts. The court rejected Moore's argument, finding the inevitable disclosure doctrine irrelevant, since the case at issue did not allege trade secret misappropriation, and neither party sought an injunction.

Similarly, the court dismissed Moore's claim of blacklisting, finding the only evidence Moore could provide to support the claim were the statements from his own conclusory declarations, which were insufficient to support a claim.

Ultimately, the court found the evidence suggested CAI was simply asserting in "good faith, an arguable interpretation of existing law" which did not make the company liable for tortious interference or blacklisting. Here, no evidence showed threatened frivolous litigation based on a desire to harass or harm Moore according to the court.

Moore v. Commercial Aircraft Interiors provides some important lessons for both employers and employees regarding cases where an employee leaves to work for a competitor. From an employer's perspective, this ruling seems to suggest a former employer has some leeway in the types of litigation threats made against a former employee who tries to work for a direct competitor so long as they rely on "arguable interpretation[s] of existing law."

New Hampshire Enacts New Law Requiring Disclosure of Non-Compete and Non-Piracy Agreements Prior To Job Offer And Change In Job Classification

By Ryan Malloy and Robert Milligan (June 17, 2012)

The New Hampshire legislature recently passed a new state law that will require the disclosure of non-compete and non-piracy agreements to potential employees prior to making offers of new employment and to existing employees with an offer of change in job classification. Governor Lynch signed the bill on May 15, 2012. Under the new law, any agreement that is not in compliance with the law shall be void and unenforceable.

The new law is effective July 14, 2012. Employers using non-compete and/or non-piracy agreements must plan accordingly. We previously alerted our readers to this legislation after New Hampshire's House recommended the bill in March. The full text of the law can be found here. The law has some similarities to Oregon's non-compete statute which also has pre-offer disclosure requirements.

Some legal commentators have noted that New Hampshire courts generally look with disfavor on non-compete agreements and they have criticized the new law for its lack of clarity concerning the meaning of non-piracy agreements. Based upon the statutory language, it is unclear whether non-piracy agreements means non-solicitation clauses or also includes non-disclosure clauses. Additionally, "change in job classification" is not defined under the law. "Change in job classification" could mean promotion, lateral move, demotion, or change in title. Case law or additional legislation will need to further define the statutory language.

Employers conducting business in New Hampshire will want to take this new law into account and comply in the hiring and employment process with New Hampshire employees.

A Business Entity That Changes Its Corporate Structure Risks Expiration Of Its Employees' Covenants-Not-To-Compete And Confidentiality Agreements

By Paul E. Freehling (June 25, 2012)

A business entity changing its form, but not its operations, will want to protect non-competition and confidentiality agreements with its employees from expiring as a result of the transaction. Because those covenants usually are viewed as non-assignable personal service contracts, they may be unenforceable by the surviving entity, absent each employee's express consent, if the covenants are seen as pertaining solely to the disappearing company which executed them. The agreements remain viable only if the rights and obligations they contain, as well as the agreements themselves, are deemed to have passed to the survivor by operation of law.

Suppose, for example, that there is a planned transaction whereby a partnership will be incorporated, or a corporation will be converted to an LLC, or a subsidiary will be merged into its parent. If the entity that will disappear has employee non-compete or confidentiality agreements, in a minority of jurisdictions the survivor will be precluded from enforcing the covenants on the ground that the survivor is not the company that executed and is named in them. Courts there refuse to rewrite contracts and hold that a personal services agreement expires if it identifies a specific contractual party that is merged out of existence as a consequence of the merger. However, this result might be different if the agreement explicitly binds "successors." Courts are divided as to whether enforceability is supported, on a theory of implied consent, merely because the contracting employees continue their employment with the successor after the transfer of assets; to be absolutely safe, the surviving entity which wants its employees to be bound should enter into new covenants with the employees. As reported on John Marsh's blog Trade Secret Litigator, the Ohio Supreme Court recently held that a covenant not to compete will not be extended to the new company after a merger if the covenant's language fails to specifically assign its rights to the new company.

Many jurisdictions find continuing viability for non-compete and confidentiality agreements after the transaction in the instance of (a) an automatic transfer of assets, (b) no modification of the employee's duties or benefits, and (c) no changes in the operational structure. These courts hold that all of the predecessor's contracts are assumed by the successor, and they should be enforceable as written. Further, the employer has experienced nothing more than a technical revision, and employees have no legitimate cause to complain about what is little more than a change in the employer's name.

Trading Secrets

Even in jurisdictions hostile to the efforts of a successor-by-merger to enforce its predecessor's covenantsnot-to-compete, the successor should be permitted to enforce the predecessor's confidentiality agreements. It would be a travesty if, simply because of a change in an employer's organizational structure, a high-level employee was deemed to be free to resign, go to work for a competitor, and abdicate his or her commitment not to disclose the former employer's trade secrets.

Delaware Chancery Court Rules That Former Employees Are Not Indispensable Parties in Non-Compete Case

By Ryan Malloy (July 22, 2012)

On July 11, 2012, the Delaware Court of Chancery found that former employees are not indispensable parties for purposes of dismissal pursuant to Chancery Court Rule 19 in an action against their new employer for breach of covenants not to compete, misappropriation of trade secrets, and aiding and abetting a breach of fiduciary duty, based on allegations that the new employer improperly persuaded the employees to breach agreements with their former employer.

NuVasive, Inc. v. Lanx, Inc., C.A. No. 7266-VCB (Del. Ch. July 11, 2012) involved claims that Lanx, a medical device company, induced employees of NuVasive, a competitor, to work for Lanx. Specifically, NuVasive alleged that Lanx persuaded employees of NuVasive to breach various restrictive covenants that the employees had with NuVasive and to misappropriate NuVasive's trade secrets and other proprietary information. NuVasive further alleged that Lanx aided and abetted breaches of fiduciary duty by the former employees. Neither party asserted that the former employees are subject to personal jurisdiction in Delaware or could otherwise be joined. Lanx then moved to dismiss pursuant to Chancery Court Rule 12(b)(7), which allows a defendant to move for dismissal because of a failure to join an indispensable party under Rule 19.

Under Chancery Court Rule 19(a), the Court must determine whether an absent person is a necessary party to the litigation. If an absent party is deemed necessary and cannot be joined, the Court must then, pursuant to Rule 19(b), "determine whether in equity and good conscience the action should proceed among the parties before it, or should be dismissed, the absent person being thus regarded as indispensable." Rule 19(b) lists four factors for the court to consider in determining if a necessary party is indispensable to the action, including the extent to which a judgment rendered in the person's absence would be prejudicial to those already parties, and whether the plaintiff will have an adequate remedy if the action is dismissed for nonjoinder.

In *NuVasive*, the Court found that, while the former employees of NuVasive were necessary parties to the litigation concerning the restrictive covenant-based claims, they were not indispensable parties because the court could protect the rights of the absent parties by declining to enter injunctive relief, or by crafting a limited injunction that did not inappropriately prejudice the absent employees.

As to the remaining allegations, the Court found that the former NuVasive employees were not necessary parties for claims based on trade secret misappropriation and aiding and abetting a breach

of fiduciary duty. Specifically, the Court concluded that any ruling on the issues raised by this litigation would only affect the former employees' employment prospects with the new employer to the extent that their employment actually did rely on the misappropriation of trade secrets. Thus, the Court found that they were not necessary parties for the trade secret misappropriation claim. Nor were they necessary parties as to the aiding and abetting breach of fiduciary duty claims, because any potential reputational harm that could be suffered by the former employees in this litigation, in their absence, would not be sufficient to render them necessary parties.

Nevada Attorney General and FTC Scrutinize Nevada Healthcare Company's Alleged Anti-Competitive Behavior Concerning Use of Non-Compete Agreements

By Jessica Mendelson (August 15, 2012)

On August 6, the Nevada Attorney General announced the filing of a lawsuit and settlement against Renown Health ("Renown"), a Reno, Nevada based company, alleging violations of state and federal antitrust law.

At the same time, the Federal Trade Commission filed a complaint, also alleging anti-competitive behavior.

Renown had recently acquired two of largest cardiology practices in Reno, Nevada starting with Sierra Nevada Cardiology Associates ("SNCA") in 2010, followed by Reno Heart Physicians ("RHP") in March 2011. Prior to the acquisitions, SNCA and RHP allegedly held virtually all of the cardiologists in the Reno area.

The Nevada Attorney General's lawsuit alleged that Renown Health had violated federal antitrust laws by consolidating the two practice groups resulting in significantly reduced competition. Prior to the filing, Renown employed roughly 97% of the cardiologists in the metropolitan area. At the time of the filing, the number had dropped to roughly 88% of all cardiologists in the area, which according to the FTC, still "effectively eliminated competition." According to the Attorney General, this reduced competition had the potential to lead to higher prices for cardiology services in the area. In addition, this could deter doctors from going to competitors and reduce their bargaining power in negotiating employment contracts. Furthermore, the non-compete terms of the cardiologists' employment agreement allegedly block entry to the market because they allegedly limit doctors' employment choices.

Under the terms of the Attorney General's settlement, Renown will suspend the non-compete provisions in the employment agreements with the cardiologists formerly employed by SNCA and RHP. This suspension will allow cardiologists to terminate employment without breaching terms or being subject to other retaliation as long as certain conditions are met. Under the settlement, Renown must release a certain number of cardiologists, freeing them from the non-compete agreements and allowing them to practice elsewhere. Up to ten employees will be permitted to leave by submitting a notice of intent to terminate employment to an Attorney General monitor and then state that they intend to remain in the Reno metropolitan area for at least a year. Each doctor must provide sixty days notice prior to terminating his or her employment. If fewer than six employees leave during a year, the settlement provisions will continue until six employees leave.

The FTC proposed a similar settlement with Renown, agreeing to suspend its non-compete provisions with the cardiologists for at least 30 days while the FTC considers public comments on the proposed order. FTC officials have said previously that they are increasing their scrutiny of physician-acquisition deals by hospitals, due to recent increases in merger-and-acquisition activity, so similar actions are likely to occur in the future. According to representatives from the FTC, "When you have high levels of market share concentration, it really begs whether the market is competitive or not."

In light of the Department of Justice's recent activity in the high-tech sector concerning no-hire agreements and the FTC's activities here, companies should be cognizant of the effect of their market share/the use of non-compete agreements in particular markets and the possibility of government regulatory activity regardless of whether the jurisdiction, such as Nevada, permits non-compete agreements.

Texas Federal Courts Reach Differing Conclusions On Granting Injunctive Relief On Close To Expiring Or Expired Non-Competes: Some Courts Elect To Equitably Extend Covenants

By Paul E. Freehling (August 19, 2012)

Travelhost, Inc., produces magazines and other publications designed to help travelers. Over the course of the last several years, a number of employees, each of whom had signed a non-compete agreement, left the company and began working for its competitors.

Travelhost sued several of the ex-employees in the U.S. District Court for the Northern District of Texas for alleged violations of its non-compete agreements and achieved varying results. One defendant had stopped competing by the time judgment was entered and had departed the relevant territory. With only four months of the non-compete period left when Travelhost's motion for entry of a preliminary injunction was decided, Chief Judge Fitzwater ruled that if competition resumed injunctive relief would be inappropriate and a compensatory award would suffice.

In an action against a different ex-employee, Senior Judge Fish initially denied Travelhost's motion for a preliminary injunction – since the two-year non-compete period had run out before judgment was entered – but then, on reconsideration, "equitably extended" the agreement and granted the motion because of the defendant's "continuous and persistent" violations of the covenant. For the same reason, Judge Lynn also equitably extended the agreements signed by five employees.

In the case of the former employee who no longer competed with Travelhost and had moved away, the company argued that irreparable harm should be presumed in the instance "of a continued breach of a non-competition agreement by a highly trained employee." Chief Judge Fitzwater agreed that there is such a presumption but held that it is rebuttable and had been rebutted. The ex-employee started, but then sold, a competing business and left Travelhost's environs. Even if her violations were to resume, the judge said in a ruling late last year, monetary damages were calculable because such an abbreviated portion of the non-compete period had not expired. *Travelhost, Inc. v. Figg*, Civ. Action No. 3:11-cv-0455-D (N.D. Tex., Nov. 22, 2011).

This past February, Senior Judge Fish decided that Travelhost's motion for a preliminary injunction, against a different ex-employee whose two-year non-compete period expired a week before the judge

ruled, was moot. Travelhost moved for reconsideration and showed that the ex-employee had been continuously publishing a new magazine within the designated territory and was targeting Travelhost's markets, readers and distribution channels. Further, many of the advertisers were the same or similar. The injunction motion was filed more than four months before the non-competition covenant expired.

But for the ex-employee's devil-may-care attitude, the reconsideration motion might have been denied. However, when Travelhost sent the ex-employee a cease and desist letter promptly after verifying that he was competing, he never responded but continued competing. After suit was filed, he kept ducking service of process until, eventually, the only recourse was both to leave the complaint at, and to mail it to, his residence. He didn't respond until Travelhost moved for entry of an order of default. Then, he asked for and received two extensions of time to plead before finally answering. He failed to produce requested documents until he was served with a motion to compel and for sanctions, and he never replied to Travelhost's motion to reconsider denial of a preliminary injunction.

In June 2012, Judge Fish granted reconsideration and said he would enter a preliminary injunction. According to the court, the ex-employee "had been continuously and persistently involved in the publication of the competitor publication. . . . [He] directly competed against Travelhost . . . while he still was under contract . . . . As a result, it is only fair that this court use its equitable power to extend the term of the non-compete agreement for an additional two years." *Travelhost, Inc. v. Modglin*, Civ. Ac. No. 3:11-cv-0456-G (N.D. Tex., Feb. 29 and June 6, 2012). In still another case, *Travelhost, Inc. v. Brady*, Civ. Ac. No. 3:11-cv-454-M-BK (N.D. Tex., Feb. 17, 2012) Judge Lynn equitably extended the covenants of five ex-employees for two years.

Among the circumstances that have persuaded judges to exercise their discretion to equitably extend the duration of a non-competition covenant are the following:

1. The applicable terms of the agreement (for example, an express provision – although not in Travelhost's covenants – dealing with extension of the non-compete period if the employee violates the covenant during that period);

2. The employer's diligence in seeking judicial, and then injunctive, relief after learning the requisite facts;

3. The egregious nature of the ex-employee's violation and its continuation over an extended period (in other words, deprivation of the employer's "benefit of the bargain"); and

4. Delays not primarily attributable to the employer but, rather, caused by the ex-employee and/or the result of a prolonged litigation process.

Missouri Supreme Court Reaffirms That Missouri Is A Pro Non-Compete Jurisdiction, Enforcing Non-Competition and Modified Non-Solicitation Agreements Against Non-Resident Former Security Company Employees

By Robert Milligan and Grace Chuchla (August 21, 2012)

The Missouri Supreme Court recently issued a decision, *Whelan Security Co. v. Kennebrew, et al.,* 2012 Mo. LEXIS 167, reaffirming Missouri as a pro non-compete jurisdiction for employers.

The Court's decision makes clear that Missouri courts applying Missouri law will enforce non-competition and customer non-solicitation and employee non-solicitation agreements that are reasonable and necessary to protect legitimate interests against Missouri employees and non-resident employees.

In December 2008, two employees of Whelan Security Company (a Missouri company with 38 branches in 23 states), – Charles Kennebrew and Landon Morgan – resigned from their positions in Whelan's Dallas and Nashville offices, respectively. Curiously, Kennebrew was assigned to the Dallas office because of a non-compete agreement he had with his previous employer. Soon after their resignations, Kennebrew and Morgan allegedly joined forces to start their own small security company – Elite Protective Services. Trouble began to brew in November 2009, when Elite successfully solicited the business of Park Square Condominiums, one of Whelan's Houston-based clients, and also hired some of Whelan's employees.

Kennebrew and Morgan had signed non-solicitation and non-competition agreements during their employment with Whelan. Specifically, for a period of two years after his employment, Kennebrew's agreement restricted him, in pertinent part, from the following actions:

1. Solicit, take away or attempt to take away any customers or the business or patronage of any such customers or prospective customer(s) whose business was being sought during the last twelve months of employee's employment;

2. Solicit, interfere with, employ, or endeavor to employ any employees or agents of employer; and

3. Working for a competing business within a fifty mile radius of any location where employee provided or arranged for employer to provide services.

Morgan's agreement contained the same provisions; however, his agreement had a one year, rather than two year, prohibition.

With these agreements in hand and following the events at Park Square, Whelan filed suit, seeking both damages and a preliminary injunction. Whelan alleged that Kennebrew and Morgan violated their agreements. Whelan alleged that Kennebrew solicited Park Square's business and that Elite had signed a contract with Park Square. Whelan alleged that Morgan solicited Whelan's Park Square employees and that Elite retained several of Whelan's Park Square employees. The trial court denied Whelan's request for a preliminary injunction, and both sides then filed motions for summary judgment. The court denied Whelan's motion but granted the defendants' motion, finding that "the employment agreements at issue in this case, as written, are overbroad, not reasonable as to time and space and therefore are not valid."

Whelan appealed, and the Missouri Supreme Court returned a decision that is, on the whole, quite favorable to employers and their ability to enforce non-competition and customer and employee non-solicitation agreements against Missouri employees and non-resident employees. While the court found that some of the covenants were unreasonable as written, the Court modified the covenants and enforced them to give effect to the intent of the parties.

Specifically, with respect to Kennebrew's and Morgan's agreements, the Court found as follows:

1. The customer non-solicitation clauses (for both prospective and existing customers) were overbroad because they lacked geographic limitations. The Court recognized that the two employees could not have "had significant contact with a substantial number of Whelan's customers throughout the nation." The Court, however, only declared unenforceable the provision's prohibition on soliciting prospective customers. The Court reasoned that the prospective customer non-solicitation clauses prevented the employees from soliciting any business that Whelan sought as a customer in any of its 38 branches. The Court found that preventing the employees from soliciting any prospective customers throughout the nation would not protect Whelan from "the influence an employee acquires over his employer's customers through personal contact," which was a protectable interest under Missouri law, but instead would impermissibly protect Whelan from competition altogether. The Court indicated that under certain scenarios a prohibition on the solicitation of prospective customers could be permissible if for a legitimate purposes and tethered to prospective customers that the employee actually solicited, rather than tenuous and detached relationships.

The Court permitted the existing customer non-solicitation clause to remain but modified it to apply only to those customers with which Morgan or Kennebrew had contact in the last year of their employment. The Court reasoned that although Morgan and Kennebrew had significant client contact in their respective branch offices and possibly in the Houston area, there was no disputed facts showing that

they had significant contact with a substantial number of Whelan's contacts throughout the nation such as to warrant a national prohibition.

2. Morgan's one-year employee non-solicitation clause was reasonable and enforceable because it complied with Missouri Revised Section 431.202(4), which renders an employee non-solicit provision "per se reasonable if the duration is for a period of one year of less." The Court found that there was a genuine factual dispute regarding the purpose of Kennebrew's two-year prohibition that needed to be resolved by the trial court. On remand, Whelan will need to demonstrate that the clause is to protect "[c]onfidential or trade secret business information" or "[c]ustomer or supplier relationships, goodwill or loyalty, which shall be deemed to be among the protectable interests of the employer" under Revised Section 431.202(3).

3. Kennebrew's non-competition clause was enforceable, but a factual dispute remained over whether Kennebrew's actions violated the clause and specifically whether he provided services in Houston while working in Whelan's Dallas office. You will recall that he was working out of the Dallas office to avoid a violation of his non-compete with a previous employer.

In the end, this mix of enforcing, modifying, and returning questions to the trial court brings to light several salient points regarding employee non-competes in Missouri:

1. Missouri is a state that is very friendly for employers wishing to enforce non-competes. As Ken Vanko astutely pointed out, the Court's ruling "beg[s] the question of whether that [the] validated non-compete achieves the same purpose as the partially invalidated non-solicitation covenant." Further, the Court stated that in analyzing non-compete agreements, "the protection of the employer, not the punishment of the employee, is the essence of the law." Furthermore, Missouri courts are also willing to modify overly broad non-solicitation and non-competes in order to render them enforceable.

2. Non-solicitation of employee provisions shall be conclusively presumed to be reasonable if their post-employment duration is no more than one year. The Court stated that "even if an employee non-solicitation covenant seeks to protect interests not identified in Section 431.220(3), it is nonetheless per se reasonable if its duration is for a period of one year or less."

3. That said, one year is not an absolute limit for employee non-solicitations provisions in Missouri. Even agreements that exceed one year "can still be reasonable based on the facts of the case." When venturing into these grounds, employers would do well to clearly state the legitimate purpose of the provision under Section 431.220(3) in the agreement, as a lack of clearly defined purpose is what stymied the Court when analyzing Kennebrew's two-year employee non-solicitation clause and the Court remanded that issue to the trial court.

4. Missouri courts may scrutinize prohibitions on soliciting prospective customers. Special care should be given to tethering such provisions to prospective customers that the employee actually solicited, rather than tenuous and detached relationships, as well as stating the legitimate purposes for such provisions in the agreement. The Court indicated that under certain scenarios a prohibition on the solicitation of prospective customers could be permissible if tethered to prospective customers that the

employee actually solicited, rather than tenuous and detached relationships. Although the Court did reject the prospective customer non-solicitation clause in this case, in addition to recognizing that more narrowly tailored covenants may be enforceable, it also recognized that prospective customer information, if it rises to the level of a trade secret, is also independently protectable under Missouri's trade secrets act.

5. Missouri courts will enforce non-compete and customer and employee non-solicitation agreements against non-resident employees for alleged violations occurring outside of Missouri.

California Court Of Appeal Finds That Non-Competition Agreement Contained In Employment Agreement Is Unenforceable Against Former Seller/Employee Even Though It Was Executed In Connection With The Sale Of A Business

By Robert Milligan and Joshua Salinas (August 27, 2012)

Non-competition agreements executed in connection with the sale of a business are typically enforceable as a limited exception under Business and Professions Code section 16601 and applicable case authority to California's general prohibition against non-competition agreements. A recent California Court of Appeal decision, however, further narrows this limited exception.

In *Fillpoint v. Maas*, 2012 WL 3631266 (Aug. 24, 2012), the California Court of Appeal, Fourth District, found that two separate agreements–a stock purchase agreement and employment agreement–executed pursuant to the sale of a business, must be read together when analyzing the restrictive covenants contained in each agreement. The Court then held that the non-competition covenant in the employment agreement, whose terms differed from the non-competition covenant in the purchase agreement, did not fall under the "sale of business" exception, and thus was unenforceable. The Court reasoned that the covenant was not focused on protecting the acquired company's goodwill. Rather, it impermissibly "targeted an employee's fundamental right to pursue his or her profession" in violation of Business and Professions Code section 16600, California's statute prohibiting non-competition agreements.

Background Facts

Defendant Michael Maas was an employee of specialty video game publisher Crave Entertainment Group. When Handleman Company acquired Crave, Maas sold his company stock and signed a stock purchase agreement. The purchase agreement contained a three-year covenant not to compete, which restricted Maas from engaging in the business he sold, with the exception of working on behalf of Crave. Business was defined as "distribut[ion] and publish[ing] of interactive entertainment (videogames), software, hardware and accessories and provid[ing] videogame software, hardware and accessories category management services for certain game retailers."

In the purchase agreement, Crave also agreed to ensure that Maas would execute an employment agreement at closing. In fact, the purchase agreement contained an integration clause that made a blank form employment agreement part of the purchase agreement.

A month after the purchase agreement was signed, Maas entered into an employment agreement with Crave by which he agreed to work for Crave for three years. The employment agreement contained a covenant not to compete or solicit paragraph. The non-compete provision contained therein was different than the covenant not to compete in the purchase agreement. It prevented Maas from participating, engaging or having an interest in any competitive business in any county in which Crave does business. In addition to the covenant not to compete provision, the paragraph contained a covenant not to sell competitive products to customers and prospective customers of Crave, and a covenant not to employ or solicit employees or consultants of Crave –hereinafter this is referred to as the non-solicitation provision. Both the non-competition and the non-solicitation provisions lasted for one year after the expiration of the employment agreement or after the earlier termination of his employment. The employment agreement contained an integration clause specifying that the employment agreement and purchase agreement constituted the sole and entire agreements between the parties, that any prior agreements were of no force and effect, and that to the extent that there was any conflict between the two agreements, the purchase agreement shall prevail.

Maas resigned exactly three years after executing the purchase agreement, purportedly satisfying the three-year non-competition covenant contained within the purchase agreement. Shortly thereafter, Maas became the President and CEO of competitor Solutions 2 Go.

Plaintiff Fillpoint LLC is a videogame distributor that acquired Crave's assets from Handleman, including the rights to Maas' employment agreement. Because of Maas' employment with competitor Solutions 2 Go, Fillpoint filed suit against Maas for breach of the employment agreement and against Solutions 2 Go for tortious interference with the employment agreement. The defendants asserted, among other defenses, that the covenant not to compete or solicit paragraph in the employment agreement was unenforceable under California Business and Professions Code section 16600.

Trial Court's Decision

After Fillpoint's opening statement at trial, the defendants moved for nonsuit (i.e. as a matter of law, the evidence presented by plaintiff was insufficient to permit a jury to find in its favor). The trial court granted the defendants' nonsuit motion and found the following: (1) Maas' non-competition covenants were assignable to Fillpoint, (2) the covenants were contained in separate agreements and should not be read together, and (3) the covenant not to compete or solicit in the employment agreement was unenforceable under section 16600. The court later decided to dismiss the tortious interference claim because it was based upon the covenant not to compete or solicit in the employment agreement, which the court found to be unenforceable.

Court of Appeal's Holding

The Court of Appeal reversed the trial court's decision and held that the purchase agreement and employment agreement must be read together, adopting Fillpoint's argument. (See Cal. Civ. Code § 1642: "Several contracts relating to the same matters, between the same parties, and made as parts of substantially one transaction, are to be taken together."). The Court, however, affirmed the trial court's

judgment and found that the covenant not to compete or solicit in the employment agreement was void and unenforceable under California law. The Court reasoned that the covenant not to compete or solicit did not fall under the "sale of business" exception (Business and Professions Code section 16601) because it was overly broad and not designed to protect the acquired company's goodwill.

1. The Non-Competition Covenants in the Purchase Agreement and Employment Agreement Must Be Read Together

The Court stated that neither party cited any case with the same facts presented by the instant case–a purchase agreement and employment agreement entered at roughly the same time and as part of a single transaction, but containing different non-competition covenants. The Court proceeded to discuss several California cases that addressed non-competition covenants located in different and/or multiple documents.

The Court referenced the Court of Appeal decision in *Hilb, Rogal & Hamilton Ins. Services v. Robb* (1995) 33 Cal.App.4th 1812, which held that the placement of a three-year post-termination non-compete in an employment contract, rather than a merger agreement, did not affect the covenant's enforceability under section 16601 when both agreements were executed pursuant to the same business acquisition.

The Court also referenced the Court of Appeal decision in *Alliant Ins. Services, Inc. v. Gaddy* (2008) 159 Cal.App.4th 1292, which held that a non-compete contained in a purchase agreement executed pursuant to the sale of a business was enforceable under section 16601 in the context of a motion for preliminary injunction. The Fillpoint Court noted that the language in the purchase agreement was identical to the covenant contained in the related employment agreement. The identical covenants applied to the entire state of California, for a period of five years after the stock purchase closing date or two years after the termination of Gaddy's employment with the new company, whichever was later.

The Fillpoint Court distinguished the two cases from the instant case because they essentially involved a single non-competition covenant, where the instant non-competition covenants were different–three years after the purchase of Maas stock (purchase agreement) vs. one year after the termination of Maas' employment (employment agreement), with differing language.

The Court ultimately agreed with Fillpoint's argument that the purchase agreement and employment agreements should be read together because both agreements were part of the same single business transaction, referenced each other, were between the same parties, and contained an integration clause, but the Court did not reach the result that Fillpoint expected would result from that conclusion.

2. The Non-Competition Covenant in the Employment Agreement is Unenforceable Under Business and Professions Code Section 16600

The Court recognized that section 16601 permits the enforcement of non-competition covenants, executed in connection with the sale of a business, to protect an acquired company's goodwill and

guard the value of the property right that was acquired. The Court noted that the burden is on the buyer to prove that this exception applies.

The Court rejected Fillpoint's argument that the fact the purchase agreement and employment agreement should be read together automatically meant the non-competition covenant in the employment agreement was enforceable under section 16601.

The Court found that the non-competition covenants in the two agreements were different by their very nature. The Court explained that "the purchase agreement's covenant was focused on protecting the acquired goodwill of Crave for a limited time" and "[t]he employment agreement's covenant targeted an employee's fundamental right to pursue his or her profession." In fact, the Court reiterated that the non-competition covenant in the purchase agreement was fully satisfied and expired when Maas resigned three years later. The Court found that Fillpoint conceded in its briefing that the two non-competition covenants were intended to "deal with the different damage Maas might do wearing the separate hats of major shareholder and key employee." Thus, the Court concluded that the non-competition covenant in the employment agreement was unenforceable under section 16600 and failed to fit within the limited exception under section 16601.

The Court also found the non-solicitation provision in the employment agreement too broad and inconsistent with the purposes and terms of section 16600 and 16601 because it gave overly broad protection to the seller and extended beyond the business sold by barring Mass from selling to or soliciting the buyer's potential customers. The Court cited with approval *Strategix, Ltd. v. Infocrossing West, Inc.* (2006) 142 Cal.App.4th 1068, which found that "nonsolicitation covenants barring the seller from soliciting all employees and customers of the buyer, even those who were not former employees or customers of the sold business, extend their anticompetitive reach beyond the business so sold" and that such "covenants would give the buyer broad protection against competition wherever it happens to have employees or customers, at the expense of the seller's fundamental right to compete for employees and customers in the marketplace."

The Court concluded that Maas satisfied his covenant not to compete for three years under the purchase agreement. The employment agreement's covenant not to compete for an additional year, including its broad non-solicitation provision, cannot be reconciled with California's strong public policy permitting employees the right to pursue a lawful occupation of their own choice.

What Fillpoint Means: The Takeaways

1. **Current agreements.** Fillpoint may have a significant impact on companies who currently have different non-competition covenants contained within separate agreements that were executed pursuant to the sale of a business with sellers/key employees. While Fillpoint does not foreclose the ability to enforce non-competition covenants under section 16601, California courts may not enforce these covenants under this statute if the language of the agreement does not reflect a clear purpose to protect business goodwill.

Companies should evaluate their non-competition agreements and recognize the risk that covenants within employment agreements may not be enforceable to the extent that they conflict with or have a broader scope than the terms of the covenants in the purchase or merger agreements and are not clearly and expressly calculated to protect the business goodwill of the selling company. Companies should also recognize that, while not at issue in this case, they may still attempt to argue that such covenants are enforceable because they are necessary to protect trade secrets under the so called "trade secrets exception" to Business and Professions Code section 16600. There remains a dispute as to whether such an exception exists and if so, what it means.

2. **Future agreements.** Going forward, at a minimum, companies should include all non-competition covenants within the terms of the purchase agreements with sellers/key employees. As seen in the Gaddy case, a non-competition agreement that contains a latent tail (i.e. additional post-termination covenant triggered at an undetermined future date) may possibly be enforceable if contained within the terms of the purchase agreement. Some legal commentators, however, believe that latent tails that become effective many years after the sale may now be unenforceable. Companies should consider maxing out the duration of a permissible non-competition covenants in the purchase agreement with sellers/key employees. To the extent that companies include the non-competition covenants in employment agreements or other agreements, the non-competition provision should be identical to the non-competition provision in the purchase agreement and should contain clear language indicating that the purpose of the provision is to protect the business goodwill in connection with the sale of business. Any non-solicitation covenants in connection with the underlying transaction should be limited to customers and employees of the seller under the *Strategix* decision. The purchaser/new employer should also be able to prohibit the solicitation of employees that the key employee has contact with after joining the company under *Loral v. Moyes* (1985) 174 Cal.App.3d 268, for up to one year post-termination.

3. **This is only one Court of Appeal decision and other decisions may support a different result.** This case's holding that the non-competition covenant in the employment agreement did not fall under section 16601 because it focused on the "right to pursue a profession" appears to conflict with the Idaho Supreme Court in *T.J.T., Inc. v. Mori* (Id. 2011) 266 P.3d 476 (applying California law) and other California decisions. The Idaho Supreme Court in *T.J.T.* 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. Even though the non-compete agreement referred to the employee/seller's employment with the new employer/buyer 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 the employee's employment only came about as part of the larger transaction–the sale of the business to a competitor–and was therefore enforceable. Interestingly, *T.J.T.* examined the same cases *(Hilb, Rogal & Hamilton Ins. Services v. Robb* (1995) 33 Cal.App.4th 1812 (containing a three year post-termination non-compete in employment agreement) and *Alliant Ins. Services, Inc. v. Gaddy* (2008) 159 Cal.App.4th 1292 (2008) (containing a five year non-compete and two year post-termination non-compete in asset purchase agreement and employment agreement) as Fillpoint but came to a different conclusion.

Also, the *Fillpoint* Court did not address two existing California Court of Appeal decisions that may also be instructive and lead to a different result. In *Newlife Sciences v. Weinstock* (2011) 197 Cal.App.4th 676, the California Court of Appeal, Second District, upheld a preliminary injunction based upon discovery issue sanctions entered against an employee who breached his non-competition agreement contained in an employment agreement with his new employer. The non-competition agreement was operative during his new employment and for five years after termination of that employment. The trial court determined that it was enforceable because it was part of the transfer of business and its goodwill by the selling employee.

Additionally, in *Monogram Industries, Inc. v. SAR Industries, Inc.* (1976) 64 Cal.App.3d 692, the California Court of Appeal, Second District, affirmed the entry of a preliminary injunction against an employee on a breach of a covenant not to compete. The five year covenant not to compete was contained in a consultant agreement executed in a connection with a purchase agreement. The court upheld the provision under a previous version of section 16601 reasoning that the purpose of section 16601 is to permit the purchaser 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. Some may consider this interest as the same side of the coin compared to the *Fillpoint* Court's concern for the "employee's fundamental right to pursue his or her profession." The court also reasoned that there was an inference that business had a "goodwill" and that it was transferred where the covenant was executed as an adjunct of a sale of a business.

4. **California is unique regarding the enforcement of non-competes.** This case reminds us that California is different from other states in its general prohibition and strong public policy against non-competes. In most states, the one-year non-competition covenant at issue in this case would likely be enforceable in whole or part. Companies may want to consider including out-of-state forum selection and choice of law provisions, coupled with consent to jurisdiction provisions, to attempt to increase the likelihood of successfully enforcing their non-competition agreements against business sellers/key employees provided the parties to the transaction have a sufficient connection to the outside forum state.

Kentucky Appellate Court Affirms Authority of Kentucky Courts to Modify Overly Broad Non-Competition Agreements in the Employment Context and Sets Forth "Guiding Principles" for Future Non-Compete Cases

By Robert Milligan and Grace Chuchla (September 6, 2012)

In a recent opinion, *Creech, Inc. v. Brown*, the Kentucky Court of Appeals both affirmed the ability of Kentucky courts to modify overly broad non-competition agreements in the employment context and laid out a six-part framework that trial courts may follow when analyzing the reasonableness and enforceability of non-competition agreements.

The court also reaffirmed that continued employment is sufficient consideration for non-competition agreements, notwithstanding the existence of some critical commentary concerning existing Kentucky precedent.

In sum, the case confirms that employers can and should use non-competition agreements with Kentucky employees and that continued employment is sufficient consideration for asking an existing employee to sign a new or updated non-competition agreement. Employers should recognize, however, that each case is fact specific and that the courts may apply a six-part framework in determining the extent to which a non-competition agreement will be enforced, if at all.

Relevant Facts/Procedure

This opinion arose out of a dispute between Charles T. Creech, Inc. and Standlee Hay Company, Inc. Both Creech and Standlee provide hay and straw to horse farms in Kentucky and other areas of the United States. Donald Brown was hired by Creech in 1990. In 2006, Brown signed a document entitled "Conflict of Interest," which, in relevant part, prohibited him from "work[ing] for any other company that directly or indirectly competes with the company for three years after leaving Creech, Inc. without the companies [sic] consent."

In 2008, Brown resigned from Creech and began to work for Standlee Hay. Creech did not oppose this move; in fact, Creech signed a partial waiver of Brown's non-competition clause that allowed him to work for Standlee as long as he did not partake in business pursuits that competed with those of Creech. Additionally, after Creech signed the waiver, Standlee notified them that Brown would be working in Kentucky and therefore necessarily be contacting Creech's customers. Creech did not respond to this notification.

Creech proceeded to file suit against Standlee and Brown. The trial court entered a temporary injunction against Brown and Standlee, but this decision was overturned on appeal. On remand, in part because of the statements made by the court of appeals when overturning the injunction, the trial court granted Brown and Standlee's motion for summary judgment. Creech then appealed the trial court's summary judgment ruling.

On appeal, Creech argued that the agreement was supported by valid consideration and that its terms were reasonable. Creech also argued that if the agreement was fatally lacking in a reasonable geographic limitation, the trial court was empowered to establish such a limitation. Standlee and Brown countered that the agreement's restriction on Brown's future employment was invalid because its terms were unreasonable and because it lacked consideration. They also asserted the trial court did not possess the authority to insert a reasonable geographical limitation into the agreement and that Creech waived any rights it did secure under the contract.

Guiding Principles

In its analysis of the trial court's ruling, the court began by stating that "very few bright-line rules govern the inquiry now before us." However, despite the lack of bright-line rules, it stated that there are two "guiding principles" that govern non-compete cases in Kentucky:

1. Trial courts are empowered to modify unreasonable provisions of covenants not to compete, and doing so will save an agreement which might otherwise be unenforceable; and

2. Judgment on the reasonableness of non-competition agreements should be based on whether they sufficiently protect the interests of the employer while neither interfering with the public interest nor placing undue hardship on the employee.

The court stressed the need for case-specific flexibility. According to the court, the factual circumstances of a covenant not to compete will necessarily vary from industry to industry, from employer to employer, and from region to region and attempting to erect a set of bright-line rules to govern courts' treatments of these agreements would be futile and counterproductive.

In addition to these two guidelines, the court acknowledged that the "general rule" in Kentucky that non-competes "are not enforceable where they are&unlimited as to space but limited as to time" has never been explicitly overruled in the context of employment cases. The court then stated, however, the blue pencil rule extends to all provisions of a non-competition agreement. *Kegel v. Tillotson*, 297 S.W.3d 908, 913 (Ky. App. 2009) ("[O]ur courts have adopted a 'blue pencil' rule, whereby we are empowered to reform or amend restrictions in a non-compete clause if the initial restrictions are overly broad or burdensome.").

The court found that in another Kentucky appellate decision, *Hodges v. Todd*, 698 S.W.2d 317, 319 (Ky. App. 1985), the court held "that the trial court had the authority to enforce [a noncompetition] covenant [which wholly omitted a geographical limitation] by establishing a reasonable geographical limitation based on the intention of the parties at the time the contract was executed." According to the

court, the case admittedly addressed only those non-competition agreements which were part of a contract for sale of a business. The court reasoned, however, given "the persistent tendency of Kentucky courts to apply rules governing noncompetition agreements in contracts for the sale of business to those included in employment contracts, and vice versa, we believe it likely that the old rule that employment contracts whose covenants not to compete fail to state a geographic limitation are invalid is probably no longer the law."

Six Factors To Analyze As Part of Guiding Principles

The court then fleshed six factors that it stated that may be considered when deciding the reasonableness and enforceability of a non-competition agreement:

1. The nature of the industry;

2. The relevant characteristics of the employer;

3. The history of the employment relationship;

4. The interests the employer can reasonably expect to protect by execution of the non-competition agreement;

5. The degree of hardship the agreement imposes upon the employee (The court stated that this is also the point in the analysis where the trial court may modify certain provisions of the noncompetition agreement if doing so would not work an injustice upon the parties, if a modification would make the agreement reasonable, and if the court determines in its discretion that it is wise to do so (citing *Kegel,* 297 S.W.3d at 913); and

6. The effect the agreement has on the public.

In a footnote, the court was careful to state that none of these factors are a new creation; rather, this opinion is simply "the first to express them together in this manner." The court also stated that not all of the categories or all questions within a category which are identified in the opinion must be addressed in every inquiry as the list of factual circumstances which may bear on each factor is neither mandatory nor exhaustive. Rather, the court reiterated that the trial court's approach must be flexible depending on the parties and their circumstances.

Working off this framework, the court reversed and remanded the trial court's entry of summary judgment, finding that "the evidence&was insufficiently developed to resolve all of the factors listed above." The court stated that the key issue on remand was to answer the question whether, "on consideration of the subject, nature of the business, situation of the parties, and circumstances of the particular case," the noncompetition clause now at issue "is such only as to afford fair protection to the interests of the [employer] and . . . not so large as to interfere with the public interests or impose undue hardship on the party restricted." The court concluded it must therefore reverse the summary judgment

order as prematurely issued and remand the matter to give the parties the opportunity to put forth sufficient proof for proper resolution of the case under this analysis.

Sufficiency of Consideration

The court also analyzed the sufficiency of consideration of the non-competition agreement. The court held that "[t]o the extent the entry of summary judgment may have been premised upon the court's conclusion that the noncompetition agreement lacked consideration, we also reverse." The court found that it was undisputed that Brown continued his employment with Creech for more than two years after he signed the Conflicts of Interest document and that he departed the company voluntarily. However, "the courts of Kentucky and those applying Kentucky law found that employer-employee agreements may be executed in exchange for merely retaining one's job." *Higdon Food Servs., Inc. v. Walker*, 641 S.W.2d 750 (Ky. 1982). The court noted that Higdon decision was strongly criticized but stated that "it remains precedent that this Court lacks authority to change." In applying the precedent to the undisputed material facts, the court concluded as a matter of law that the agreement was supported by sufficient consideration.

Also adding to the court's decision to reverse and remand was the aforementioned waiver that Creech had signed. At the time of filing its complaint, Creech raised the claim that the waiver was based off false information, and the court of appeals found that a question of fact still remained as to whether Creech intentionally waived its rights under the non-competition clause. Summary judgment was, therefore, premature.

In the end, *Creech, Inc. v. Brown* stands as a helpful and instructive case containing "guiding principles" for Kentucky employers looking to properly structure their non-competition agreements and to evaluate their enforceability.

Connecticut Federal Court Finds That Non-Competition Covenant Which Is Silent Regarding Assignability May Be Enforceable Depending Upon the Parties' Intent Under New York Law

By Paul E. Freehling (September 7, 2012)

A Connecticut federal court recently issued a significant decision concerning the rights of a buyer of a business to enforce non-competition agreements against employees who previously worked for the seller under New York law.

In 2003, Milso and each of its employees signed an employment agreement expressly governed by New York law. The agreement contained confidentiality, non-solicitation and non-competition covenants enforceable for 18 months after termination of employment, but assignability was not mentioned. In 2005, the employer, a casket company, sold its assets, expressly assigning all employment agreements. At the closing of the purchase and sale transaction, the seller terminated its employees, and then the purchaser re-hired them on substantially similar terms. The purchaser asked its employees to acknowledge that they remained subject to the covenants. Three years later, two of the purchaser's employees, who had worked for the seller but never executed the acknowledgement, resigned and began working for a competitor. The purchaser sued them in a Connecticut federal court for breach of contract, misappropriation of trade secrets, and similar causes of action. They responded by filing a declaratory judgment counterclaim asserting that, for purposes of the employment agreement covenants, they were terminated at the closing of the assets purchase and sale transaction which was more than 18 months before they began competing.

On cross motions for summary judgment, the court held that if the signatories to the employment agreements intended for the agreements to be assignable, the covenants were enforceable against employees who accepted comparable continuous employment by the purchaser. Here, the issue of the parties' intent with regard to assignability requires a trial. *Milso Indus. Co. v. Nazzaro*, Case No. 3:08CV1026 (AWT) (D. Conn., Aug. 30, 2012).

The purchaser also accused the departed employees of misappropriating trade secrets, namely, a customer list and a "confidential business plan." The court ruled that those items could qualify as trade secrets if they have "independent economic value" and reasonable efforts were undertaken to maintain

their confidentiality. A trial is necessary to determine whether the list and plan here qualified as trade secrets.

The Connecticut federal court's decision is particularly instructive with regard to the right of an assignee of an employment agreement, which contains no provision regarding assignability, to enforce covenants in the agreement. The court concluded that the dispositive question is: Did the parties to the agreement intend for it to be assignable. The assignee's burden is to prove that the signatories to the agreement – the assignor and the assignors' employee – understood at the time the agreement was signed that it was assignable.Companies involved in buy-sell transactions or mergers need to take special care to ensure that there are enforceable non-compete/restrictive covenant agreements in place with employees who remain with the buyer after the transaction is complete –that may include relying upon existing non-compete agreements between the seller and the employees or new agreements between the buyer and the employees depending upon the law in the applicable jurisdiction. John Marsh's Trade Secret Litigator blog has an excellent summary of two recent cases from Ohio and Florida concerning the assignment of non-competes agreements. Also, please consider watching our webinar on Key Considerations Concerning Trade Secrets and Non-Competes in Business Transactions for more information on this important topic.

California Federal Court Boots Employee's Challenge Of His Non-Compete Because Of Pennsylvania Forum Selection Provision

By Robert Milligan and Grace Chuchla (September 27, 2012)

In a recent order, a federal court in the Northern District of California weighed in on the validity a forum selection clause contained in an employment agreement in connection with a California employee's declaratory relief action to invalidate his non-compete provision with his former employer. The court found for the Pennsylvania-based employer and both denied the employee's motion to remand the case to California state court and granted the employer's motion to dismiss for improper venue. In doing so, the court rejected the employee's argument that the effect of enforcing the forum selection clause would permit a Pennsylvania court to enforce the non-compete provision against him and thus "deprive [Plaintiff] of the protection of his own jurisdication's laws and remedies."

Background

On March 5, 2012, plaintiff Philip C. Hartstein, a resident of San Mateo, CA, resigned from defendant company Rembrandt IP Solutions, a Delaware limited liability company headquartered in Pennsylvania. Rembrandt identifies and develops business opportunities for a related company, which is engaged in the management of funds focused on investing in intellectual property and related opportunities across a broad spectrum of industries, technologies, and business methods, including generating revenues from patents. That same day, Hartstein filed suit in San Mateo County Superior Court, requesting declaratory relief and an injunction to invalidate the non-compete covenant of his employment agreement. Within Hartstein's employment agreement, there was also a forum selection clause, which stated that Hartstein must "submit to the exclusive jurisdiction of the state courts located in Montgomery County, Pennsylvania and to the Federal Courts located in Philadelphia, Pennsylvania as to all actions and proceedings relating in any way to this Agreement and/or [Plaintiff's] relationship with [Defendant]."

After leaving Rembrandt, Hartstein began employment as the Vice President and Portfolio Manager of IPNav, a direct competitor of Rembrandt's. His new position at IPNav was similar to his old position, as both IPNav and Rembrandt compete for many of the same patent portfolios and investment opportunities.

Following Hartstein's complaint, on May 4, 2012 Rembrandt removed the action to federal court on diversity grounds, asserting that Hartstein earned well over $75,000 and that the value of their trade secrets known to Hartstein was also well over $75,000. Additionally, on May 11, 2012, Rembrandt filed a motion to dismiss for improper venue. Hartstein then responded with a motion to remand based on the fact that Rembrandt had failed to establish that the amount in controversy exceeded $75,000.

Plaintiff's Motion to Remand

Looking first to Hartstein's motion to remand, the court found, for numerous reasons, that Rembrandt had met its burden in proving that the amount in controversy exceeds $75,000. It began by rejecting Hartstein's argument that his worth to Rembrandt was too speculative to be properly considered when determining the amount in controversy. Based on Hartstein's "central and high level role," the court found it "more than likely" that Hartstein generated work worth more than $75,000 to Rembrandt. Additionally, putting future profits to the side, the court reasoned that Hartstein's salary while at Rembrandt is "a simple and straightforward way to value the object of this litigation," as this figure represents the value of the non-compete to the employee. Given that Hartstein's salary was well in excess of $75,000, such reasoning drove yet another nail in the coffin of his motion to remand. Finally, Hartstein argued that the value of the non-compete to Rembrandt was zero because he had not misappropriated and did not intend to misappropriate any of Rembrandt's trade secrets. Again, the court rejected this argument, finding that "the possibility that [Hartstein] will share Defendant's trade secrets and confidential information&is very real." Resting on this lengthy list of reasons, the court denied Hartstein's motion to remand.

Motion to Dismiss for Improper Venue

After rejecting the motion to remand, the court moved on to Rembrandt's motion to dismiss based on the forum selection clause of Hartstein's employment agreement. It began its discussion of this motion by recognizing that, while the Supreme Court held forum selection clauses to be presumptively valid in *M/S Bremen v. Zapata Off-Shore Co.,* 407 US 1, 92 S.Ct. 1907, 32 L.Ed.2d 513 (1972), the court also stated that such clauses are unenforceable if enforcement would "contravene a strong public policy of the forum in which suit is brought" *Id.* at 15. Hartstein's opposition proceeded exactly along these lines; he claimed that enforcing the forum selection clause would "deprive [him] of the protection of his own jurisdiction's laws and remedies" and result in a sure-fire win for Rembrandt in Pennsylvania to enforce the non-compete provision.

The court found Hartstein's argument unpersuasive on the grounds that it did not "challenge the reasonableness of the forum selection clause itself, only the reasonableness of its effect." Citing to *Manchester v. Arista Records, Inc.*, 1981 US Dist. Lexis 18642 (C.D.Cal Sept. 15, 1981), the court stated that finding in Hartstein's favor would force it to "make a determination of the potential outcome of the litigation" and lead to "speculation on the merits at the outset of the action." In short, it did not matter to the court whether the ultimate effect of enforcing the forum selection clause may result in the enforcement of the non-compete provision which "was purportedly contrary to California law"; for the

purpose of deciding the reasonableness of the forum selection clause, all that mattered was that, given the facts at hand, forum selection itself was not contrary to California law.

Takeaways

For some employers, particularly out-of-state employers, looking to work around California's hostility toward non-competes, this decision suggests that forum selection clauses may provide a solution. Building on some previous California federal court decisions, the court makes it amply clear that it will not look beyond the text of a forum selection clause when determining its reasonableness.

However, that is not to say that all forum selection clauses are enforceable in California. For instance, as the court points out here, those that attempt to dictate the forum for suits arising out of franchise agreements are contrary to section 20040.5 of the California Business and Professions Code and therefore unenforceable (See *Jones v. GNC Franchising, Inc.,* 211 F.3d 495). Additionally, some other California state and federal courts have been hostile to enforcing forum selection clauses when the impact would violate a strong California public policy such as California's prohibition on non-compete provisions in the employment context. Certainly, a California state court may not follow this court's reasoning particularly since the court relied upon federal law in analyzing the effect and scope of the forum selection clause. Thus, the court's denial of the motion to remand could have been outcome determinative as a California state court could have ruled differently concerning the enforcement of the forum selection clause.

Finally, this order lays out four factors to keep in mind when trying to determine the amount in controversy in a declaratory relief action seeking to invalidate a restrictive covenant: 1) the employee's role and responsibilities within the company; 2) the profits earned by the employer on business generated by the employee during the period immediately before his termination; 3) the value of the non-compete to the employee (that is, how much money would the non-compete preclude the employee from earning); and 4) the value of the company's trade secrets and confidential information known to the employee. Such a list is helpful to keep in mind when arguing for or against remand or removal.

We will continue to keep you apprised of the current developments in this evolving area.

Ignorance Isn't Always Bliss: What to Do When Your Job Candidate Isn't Sure if She Is Bound By A Non-Compete

By Molly Joyce (September 28, 2012)

If you're an employer in an industry where non-compete agreements are common, perhaps you've been faced with the following scenario: You offer a sales position to a candidate who tells you she doesn't think she has a non-compete with her employer, which is a competitor of yours. Once she's onboard at your company, she begins soliciting her former employer's clients. Within a matter of days, both you and your new hire get a cease and desist letter from your new hire's former employer. The letter encloses a non-compete agreement that your new hire, in fact, signed with the former employer several years ago. The agreement prohibits, for one year after her termination, the very activity you hired her to perform.

What are your options at this point? Assuming the restrictions are enforceable, you could keep your new hire in the same role and expect that she (and maybe you) will be sued; you could staff your new hire in a non-competing position you had not anticipated for the next year; or you could terminate her. No matter what decision you make, the new hire probably just became much less useful to your organization and much more costly. What could you have done differently? Here are some pointers for any employer to avoid this same type of pitfall in a competitive hire situation:

- **Ask, ask and ask again.** If non-competes are common in your industry, ask your job candidates more than once if they might have signed one. Oftentimes candidates forget that they signed non-competes. This is especially the case if a candidate has worked for her employer for several years and signed the agreement when she was hired initially. Also remind your candidate that non-competes are often tied to stock rewards or other bonuses, even if they aren't present in an employment agreement.

Other times, your candidate knows that she signed an agreement with a non-compete clause. Yet, she does not have a copy of the agreement and does not want to ask her HR department for a copy because it will be a red flag that she is considering a new job. In that case, ask the candidate if she can find an unsigned copy of the agreement that likely contains the same or similar restrictions. Review it and consider the potential impact any enforceable provisions might have on your hiring and staffing decisions.

Job candidates often mistakenly think that the only agreements they are bound to are agreements with their most recent employer. Remind them that they need to provide you with all agreements that might

still be in effect. For example, if they have only worked for their current employer for six months, chances are that they might have an agreement with the previous employer that is also in play.

- **Give Your Job Candidate Fair Warning.** If your candidate tells you she doesn't have an agreement with her employer, advise her that any offer you give her could be rescinded should a non-compete agreement surface in the future. If your candidate cannot get a signed copy of her agreement until she gives her employer notice, inform her that her offer will become "firm" only after you determine that there are no additional (or more significant) hurdles to hiring her.

- **Put it in Writing.** Once she's onboard, have your new employee sign an acknowledgement letter or an employment agreement informing her that your company has no interest in acquiring a ny proprietary information belonging to her former employer. Further advise that you expect her to abide by any lawful agreement she may have entered into with her former employer and it is her responsibility to make sure she complies with any ongoing obligations to the former employer. Finally, consider a provision that warns the new hire that you will not necessarily defend or indemnify her should any action be brought against her by her former employer for violation of a restrictive covenant agreement.

Employers looking to hire talented employees in a competitive landscape are often frustrated by the non-competes their job candidates are bound by. Yet, it's best to know what those limitations are ahead of time so you can make fully informed decisions that protect your company. If you proceed otherwise, you will likely find that ignorance isn't always bliss.

Can an Employer Enforce a Non-Compete Agreement That It Forgot to Sign? Perhaps Not In Texas

By Randy Bruchmiller (October 3, 2012)

Employers periodically fail to sign employment agreements. This situation generally occurs when the employer obtains an employee's signature on a form employment agreement and simply puts the document in the employee's personnel file. In this scenario, the signature of an authorized representative of the company is never added to the document. The missing signature usually comes to light when the employee violates the agreement years later, resulting in the employer wanting to take legal action to enforce the agreement. A recent Texas Court of Appeals opinion suggests that an unsigned employment agreement may be unenforceable if the agreement contains a term of more than one year.

In *Holloway v. Dekkers*, the Dallas Court of Appeals held that an employment agreement lacking the employer's signature was unenforceable. Dekkers and Twin Lakes Golf Course hired Holloway to serve as the head golf professional at Twin Lakes. The parties initially had an oral agreement that Holloway's employment contract would be for three (3) years. After further negotiations, the parties agreed that Holloway's employment would last for a one-year term with the understanding that, prior to the end of one (1) year, they would negotiate the terms of a three (3) year agreement.

Holloway moved from Illinois to Texas and started his employment on August 5, 2008. Within a week, Dekkers' daughter-in-law presented Holloway with a one-page employment agreement dated July 23, 2008. In addition to other terms, the document provided for a "yearly contract that will be up for renewal after annual performance evaluation." It also contained the recitation, "This contract is hereby agreed upon by both [Dekkers and Holloway] and verified by" their signatures. Holloway signed the document and was given a copy. Dekkers, as owner of Twin Lakes, never signed the document. Holloway was terminated on September 30, 2008, approximately eight weeks later.

Holloway filed suit for breach of contract and fraudulent inducement. The trial court granted summary judgment in favor of Dekkers and Twin Lakes. The Court of Appeals affirmed and held the agreement was unenforceable due to the statute of frauds. The statute of frauds encompasses agreements that are "not to be performed within one year from the date of making the agreement." If there is more than a year between the time of the making the contract and the time when performance is to be completed, then a writing is required to render the agreement enforceable. The Court of Appeals found that the oral agreement between Holloway and Dekkers/Town Lakes was to work for a term from August 5,

2008 to August 5, 2009, one day more than a year, meaning it had to be backed up in writing for Holloway to enforce it.

The employment agreement at issue in this case involved an employee trying to enforce the agreement instead of the employer. However, employees wanting to get out of their noncompetition or other obligations in their employment agreements that an employer forgot to sign may rely upon this case to argue that the agreement is unenforceable. The statute of frauds argument may be successful if the employment agreement contains a term of more than one year.

Holloway also argued that his initial work for Twin Lakes amounted to partial performance, sufficient to enforce the contract. The Court of Appeals rejected this argument because Holloway was already paid for the work that was partially performed.

Holloway's fraudulent inducement claim also failed. The Court of Appeals stated that the cause of action fails because the agreement failed. In other words, Holloway could not be induced into a nonexistent agreement.

Employers should always be careful to make sure their employment agreements are signed by both employees and themselves. The best practice is to make sure employment agreements are signed by all parties before new employees begin their employment in order to minimize issues relating to the enforceability of the agreements.

California Appellate Court Holds That Non-Compete Restriction in Stipulated Injunction Is Enforceable Because There Was No Showing That It Was Not Necessary to Protect Trade Secrets

By Joshua Salinas and Robert Milligan (October 11, 2012)

A California Court of Appeal recently reversed a trial court ruling that found a stipulated injunction preventing the solicitation of customers was invalid and unenforceable under California Business & Professions Code section 16000.

In *Wanke, Industrial, Commercial, Residential, Inc. v. Sup. Ct.,* 2012 WL 4711888 (Cal.App. 4 Dist., October 4, 2012), the Court of Appeal held that since the trial court could not conclude, based on the language of the stipulated injunction, that it does not protect the plaintiff's trade secrets, the court erred in concluding that it was an unlawful business restraint.

Facts

Plaintiff Wanke is a southern California company that installs waterproofing systems. Defendants Scott Keck and Jacob Bozarth are former employees of Wanke that left Wanke to start their own competing waterproofing company, WP Solutions.

Wanke brought action in late 2008 against Keck and Bozarth alleging that they misappropriated and misused Wanke's trade secrets and confidential information, and used that information to actively target and recruit Wanke's customers.

The parties ultimately resolved the action in 2009 by entering into a settlement and mutual general release agreement. Pursuant to the settlement agreement, Keck, Bozarth and WP Solutions agreed to a stipulated injunction, in which they would refrain from contacting or soliciting any customers listed on an agreed customer list for five years subject to certain exceptions. The stipulated injunction also provided for liquidated damages in the amount of $50,000 for initial violations of the order, with the amounts increasing in increments of $10,000 for each subsequent violation of the order, plus Wanke's attorneys' fees, costs, and expenses.

Proceedings to Enforce the Stipulated Injunction

A dispute arose the following year when the defendants allegedly contacted and/or supplied labor and materials to a customer on the prohibited customer list, Con Am Management. Wanke subsequently filed an application for an order to show cause requesting the trial court to hold the defendants in

contempt for having violated the stipulated injunction. Wanke also filed a motion to enforce the settlement agreement related to Con Am Management and requested the court order defendants to pay liquidated damages as provided in the stipulated injunction.

The trial court held a combined trial/hearing on Wanke's order to show cause for contempt and motion to enforce the settlement agreement. The trial ultimately court found that Wanke failed to establish the "existence of a lawful order," which is required before a party may be held in contempt of that order.

Specifically, the trial court determined that the stipulated injunction was invalid to the extent it prohibited defendants from soliciting any entity merely because the entity appeared on the customer list attached to the stipulated injunction. Citing Business and Professions Code section 16600, the trial court viewed the stipulated injunction as a non-compete agreement, which could only prohibit customer solicitation if the employee was utilizing trade secret information to solicit those customers.

The trial court found that the identity and location of Con Am Management was easily identifiable and thus, not a trade secret. To avoid striking down the injunction in its entirety, and thereby unwind the entire settlement and resolution between the parties, the trial court narrowed the application of the injunction only to the extent it was used to prohibit defendants from undertaking or proposing to undertake jobs from customers on the customer list while defendants were employed by Wanke. The trial court explained that only on these jobs can defendants be said to be using information they learned while employed at Wanke to identify customers with particular needs or characteristics that would be protectable under California law.

With respect to the motion to enforce the settlement agreement, the trial court ruled that no liquidated damages may be imposed because the alleged violations were not in fact violations of the stipulated injunction as interpreted above by the court. Notwithstanding, the trial court awarded Wanke attorneys' fees on the motion to enforce the settlement agreement because it obtained a declaratory judgment regarding the scope and enforceability of the stipulated injunction.

A few months later, Wanke filed second motion to enforce the stipulated injunction with respect to a different customer identified in the customer list, AV Builders. This time, the trial court found the defendants violated the stipulated injunction because the AV Builders work involved jobs undertaken or proposed to be undertaken when defendants were employed by Wanke. The trial court awarded Wanke its attorneys' fees, along with $50,000 in liquidated damages as provided in the settlement agreement.

Court of Appeal

Both parties appealed. Defendants appealed the trial court's findings that they violated the stipulated injunction as to AV Builders and the award of attorneys' fees to Wanke regarding the motion to enforce the settlement as to Con Am Management. Wanke appealed the trial court's order denying its motion to enforce the settlement as to defendants' work for Con Am Management. Additionally, Wanke filed a petition for writ of mandate challenging the trial court's order which refused to hold Keck and WP Solutions in contempt for violating the stipulated injunction. Wanke requested the Court of Appeal to

enforce the entirety of the settlement agreement and stipulated injunction. Wanke also asked the appellate court to annul the trial court's order discharging the OSC for contempt and direct the trial court to hold Keck and WP Solutions in contempt.

A. Contempt Ruling

With respect to the contempt issue, the Court of Appeal concluded that the double jeopardy clause of the Fifth Amendment to the federal constitution precluded the court from reviewing the trial court's acquittal of Keck and WP Solutions on the contempt charges. Wanke argued that double jeopardy did not apply because the government did not prosecute the action. The Court found that there was no language in the binding U.S. Supreme Court decision of United States v. Dixon that limited application of the clause to the contempt proceeding here, which it characterized as a nonsummary criminal contempt proceeding, rather than civil contempt proceeding.

B. Validity of Stipulated Injunction Ruling

Notwithstanding its conclusion on the contempt issue, the Court then analyzed whether the trial court erred in determining the stipulated injunction was invalid and unenforceable. The Court reasoned that a party may successfully defend against the enforcement of an injunction that the trial court issued in excess of jurisdiction. The court, however, found that party may not defend against enforcement of a court order by contending merely that the order is legally erroneous. The Court reasoned that under existing authority an injunctive order enforcing an invalid contract, the invalidity of which is not apparent on its face, is not an injunction issued in excess of jurisdiction.

The Court then reasoned that the courts have repeatedly held a former employee may be barred from soliciting existing customers to redirect their business away from the former employer and to the employee's new business if the employee is utilizing trade secret information to solicit those customers. The Court also discussed *Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, in which the court concluded that there was substantial evidence to support the trial court's finding that the employer's customer list constituted a protectable trade secret. And as a result, the *Morlife* court concluded that the trial court had not erred in enjoining former employees from soliciting any business from any entity that did business with Morlife before the former employees stopped working there, provided they obtained knowledge about the customer during the course of their employment at Morlife. The Court also reasoned that under the California Supreme Court's decision in *Edwards v. Arthur Andersen LLP* (2008) 44 Cal. 4th 937, section 16600 generally prohibits the enforcement of nonsolictiation agreements in all cases in which the trade secret exception does not apply. The Court also noted that there was a dispute among California appellate courts as to whether such an exception actually exists.

The Court held that Keck and WP failed to make a showing against the enforcement of the injunction on the ground that the injunction was beyond the trial court's jurisdiction to issue. The Court reasoned that at the time the trial court issued the injunction it had personal and subject matter jurisdiction over the parties. It was also undisputed that Wanke had filed a lawsuit alleging trade secret misappropriation and had requested an order enjoining Keck and WP Solutions from soliciting its customers and the trial

court entered the stipulated injunction as part of final resolution of the case. According to the Court, each of these fact supported the validity of the stipulated injunction.

The Court also noted that Keck and WP Solutions did not claim that the Stipulated Injunction was obtained in an unauthorized manner or in violation of statutory procedures. Further, there was nothing on the face of the stipulated injunction that indicated that it was unconstitutional or that it violated a statute. On the contrary, the Court noted that Keck and WP Solutions had conceded that employee non-competition agreements could be enforceable to protect the former employer's confidential trade secret information and that the misuse of trade secret information may be properly enjoined by agreement. The Court highlighted the fact that defendants failed to oppose the existence of the so called "trade secret exception" to California's prohibition on the enforcement of non-compete agreements.

The Court held that, because the stipulated injunction was valid to the extent that it protects Wanke's trade secrets, and one cannot conclude from the face of the stipulated injunction that it does not protect Wanke's trade secrets, the stipulated injunction was facially valid. The court remarked that even assuming that Keck and WP Solutions could demonstrate that the trial court erred in issuing the stipulated injunction because the customer list attached to the stipulated injunction was not a protected trade secret, such a showing would be insufficient to avoid enforcement of the injunction. That is because the Court reasoned that demonstrating that the trial court erred in issuing the injunction would not be sufficient to demonstrate that it acted in "excess of its jurisdiction" in doing so.

Finally, the Court recognized that common sense and fundamental fairness support its ruling. The Court explained that parties cannot stipulate to injunctions that identify certain customers whom they will not solicit in order to resolve claims that they misappropriated trade secrets, then proceed to violate the injunction and claim that the customer list is not a trade secret. Even assuming that Keck and WP Solutions were permitted to collaterally attack the validity of the stipulated injunction, and that they could prove that the customer list attached to the stipulated injunction was not a trade secret, the Court found that they made no such factual showing in this case.

In short, since the trial court could not conclude, based on the language of the stipulated injunction, that it does not protect Wanke's trade secrets, the court erred in concluding that the stipulated injunction was an unlawful business restraint.

The defendants' two claims in their appeal both failed in light of the Court's conclusion that the trial court erred in determining that the stipulated injunction could not be enforced as drafted.

Takeaways

This case reminds us that California's general prohibition on noncompetition agreements applies to all agreements that restrain anyone's engagement in a lawful profession, trade, or business (unless there is an applicable exception); not merely agreements in the employer-employee context. Indeed, even settlement agreements and stipulated injunctions as part of the resolution of a lawsuit are within the ambit of Business and Professions Code section 16600.

While this case does not foreclose the ability to obtain injunctive relief when the settlement agreement and stipulated injunction contain restrictive covenants, it illustrates the difficulties in obtaining relief if the other side enters the agreement in bad faith. Thus, it is important to include language in any settlement agreement, which also contains restrictive covenants, and stipulated injunction references and stipulated findings as to the existence of trade secrets and how and why the agreement and/or injunction is necessary to protect trade secrets.

This case demonstrates that one possibility to increase the effectiveness of a settlement agreement, containing restrictive covenants, is to include a liquidated damages clause for any violations. Another possibility would be to require that money be placed in an escrow account for the life of the restricted period. While these remedies will not guarantee a party will not violate the terms of the agreement or ensure further injunctive relief, they may provide some relief for any damages suffered from a breach.

The case also demonstrates that the California appellate courts are presently split on whether there is a trade secret exception to Business and Professions Code section 16600, which may ultimately necessitate the California Supreme Court's guidance.

This case is significant as it provides insight for parties that are assessing the enforceability of restrictive covenants contained within settlement agreements, stipulated injunctions, and other agreements. Specifically, parties may attack such agreements on the grounds of the lack of trade secrets and/or language that the restrictive covenants are necessary to protect trade secrets. At least in the case, however, the Court placed some stock in the parties' agreed resolution to dissuade future collateral attack of the parties' agreed language. What is clear, however, based on this decision is that non-solicitation of customers provisions that are unnecessary to protect trade secrets or not otherwise subject to an applicable exception are void and unenforceable.

Are Non-Competition And Non-Solicitation Provisions In An Employment Agreement Enforceable Despite The Absence Of Compensable Damages?

By Paul E. Freehling (October 15, 2012)

In a recent ruling, a West Virginia federal judge held that litigation involving a former employee's claimed violation of covenants not to compete and not to solicit the ex-employer's workers must proceed to trial even though the ex-employer produced no evidence of monetary loss. Relying on 76-year old and 118-year old West Virginia cases neither of which concern similar covenants, the court reasoned that if the ex-employer proves a breach of contract, the company will be entitled at least to nominal damages and might be awarded attorneys' fees and costs. The possibility that the plaintiff might recover damages was held to be a sufficient basis for denying the defendant's motion for summary judgment. *Panhandle Cleaning & Restoration, Inc. v. Vannest*, Civil Ac. No. 5:11CV178 (Stamp) (N.D. W. Va., Oct. 5, 2012).

Panhandle constructs, restores and remodels residential and commercial buildings. It alleged that Golec, a former employee, breached an employment agreement promising not to compete within a 50-mile radius of his former place of business for two years after termination, and not to solicit Panhandle's employees or customers during those two years. The agreement also recited that "The Employee expressly acknowledges that [the covenants not to compete and not to solicit are] reasonable and will not prevent [sic] or impose an undue hardship or otherwise prevent the Employee from earning a livelihood during the time it is in effect." Golec denied that he had signed the agreement, and he insisted that, in any event, it was unenforceable.

According to the court, in addition to the issue of whether Golec's signature was authentic, factual disputes included Panhandle's claim that it had interests requiring protection, and Golec's contention that enforcement would impose an undue hardship on him. Golec denied that he had solicited Panhandle's employees, but the company identified witnesses who would testify to the contrary, and that was sufficient to defeat his summary judgment motion on Panhandle's suit for breach of the non-solicitation covenant. Regarding the non-competition provision, the court cited cases holding that two-year and 50-mile restrictions are reasonable under West Virginia law. However, not determinable without a trial were "what exactly Panhandle's business is and thus, what type of work constitutes being in direct competition with Panhandle."

When the case goes to trial, the fact finder may sympathize with Golec at least with respect to the covenant not to compete. That sympathy may impact the decision as to whether the agreement is enforceable against him. Notwithstanding the employment agreement provision to the contrary, it is hard to believe that he posed a threat of substantial economic harm to Panhandle solely as a competitor. By the same token, enforcement of the non-compete would impose a hardship on him by depriving him for two years of virtually all opportunity to earn a living anywhere near Panhandle's place of business – a 50-mile radius, after all, translates into a circle with a diameter of 100 miles – doing what he does best. The sympathy factor might be diluted, however, if Golec is found to have solicited Panhandle's employees, and particularly if he refuses to promise that he will not attempt to solicit them for the remainder of the two-year period.

"Gist Of The Action" Doctrine May Require Dismissal Of Tort Claims Based On Breach Of Restrictive Covenants In Employment Agreement

By Paul E. Freehling (October 18, 2012)

Pursuant to the "Gist of the Action" doctrine, tort claims may be dismissed if they are "intertwined with," and not just "collateral to," contract claims in the same complaint.

In a Pennsylvania federal court case, an ex-employee was accused by his former employer of breaches of confidentiality, non-solicitation and non-compete agreements, and related causes of action. The portion of the plaintiffs' tortious interference with contract claim that was "intertwined" with the cause of action for breach of the non-solicitation agreement was dismissed pursuant to Federal Rule 12(b)(6) and the "Gist of the Action" doctrine, but the motion to dismiss those allegations that were "collateral" to the breach of contract claim was denied.The court also found that plaintiffs' Computer Fraud and Abuse Act (CFAA) allegations, to the extent that the ex-employee, for his personal benefit, induced a current employee to access the plaintiffs' computers, survived the motion to dismiss. *Synthes, Inc. v. Emerge Medical, Inc.,* Civ. Ac. No. 11-1566 (E.D. Pa., Sept. 19, 2012).

Synthes makes and sells implant devices used for orthopedic surgery. Powell, a Synthes salesman, signed – and was accused of violating – the company's confidentiality, non-solicitation and non-compete agreements. After a half-dozen years with Synthes, he resigned to join two other former Synthes employees at Emerge, a competitor company. Synthes' 13-count complaint included, among other causes of action against him (and in some instances against one or more other defendants), claims for breach of contract, tortious interference, misappropriation of trade secrets, and violation of the CFAA. A total of six briefs were filed supporting or opposing Powell's motion to dismiss. The decisions announced in the court's 74-page slip opinion mostly were adverse to Powell.

The "Gist of the Action" doctrine serves to prevent an award of punitive or exemplary damages for what is basically a breach of contract. The doctrine also helps in some cases to avoid the potential confusion resulting from different statutes of limitation applicable to tort and contract claims alleged to have arisen out of the same incident.

Synthes' non-solicitation agreement with Powell was intended to prohibit him from encouraging the company's workers to accept employment elsewhere. His alleged violation of that agreement was "intertwined" with the claim that he thereby tortiously interfered with the company's contracts with those

workers. So, the court dismissed that tort claim. Synthes also charged him with tortiously interfering with the company's vendor relationships, but since the non-solicitation agreement said nothing on this subject his motion to dismiss that claim was denied. His non-competition agreement was somewhat convoluted, and the court could not determine at the pleading stage whether the "Gist of the Action" doctrine required dismissal of Synthes' tortious interference claim relating to Powell's efforts to sell Emerge's products to Synthes' customers.

Powell's motion to dismiss the CFAA cause of action asserted that (a) the allegations did not satisfy the statutory mandate that a claim against him must aver that he improperly accessed a protected computer and, even if the allegations did satisfy that mandate, (b) no compensable loss could be shown to have resulted from any such improper access. The court held that the CFAA mandate regarding improper access was adequately pleaded by allegations that, after leaving Synthes' employ, he induced the company's workers to provide him with confidential and proprietary computerized information. Regarding the requirement that "damage or loss by reason of a violation" must be shown, the court determined that Synthes' pleading that it had incurred "the costs of responding to [Powell's] wrongful actions, conducting damage assessments, and restoring data and programs" met the statutory test.

The *Synthes* opinion provides the reader with an exhaustive analysis of Pennsylvania law, mainly derived from unofficially reported rulings, relating to the "Gist of the Action" doctrine (in some cases from courts in that state and elsewhere, the principle that tort damages cannot be recovered for a breach of contract is referred to as the "Economic Loss" doctrine). In addition, the *Synthes* ruling contains an extensive discussion of what conduct does, and what conduct does not, violate the CFAA. Parties to disputes potentially involving those issues will want to study this opinion.

Trading Secrets

Paramedics Defeat Noncompete and Customer Nonsolicit Preliminary Injunction on Grounds of Potential Harm to Public and Paramedics

By Paul E. Freehling (October 24, 2012)

A private medical transport service was recently unsuccessful in persuading the U.S. District Court for the Northern Mariana Islands to enter a preliminary injunction prohibiting two ex-employees from competing with and soliciting customers of their former employer. The judge cited Section 188 of the Restatement of Contracts (Second) as authority for denying injunctive relief where the potential harm to the public and the defendants outweighed the likely benefits to the plaintiff. Further, according to the court, the names on the plaintiff's customer list are not trade secrets. The relevant community is small, and so the names of people likely to need medical transport services are readily determinable. *August Healthcare Group, LLC v. Manglona,* Case No. 1:12-CVI-00008 (D. Northern Mariana Islands, Oct. 12, 2012).

The plaintiff does business as St. Michael's Medical Response. Until recently, it provided the only non-public ambulance and medical transportation service in Saipan. All of St. Michael's workers, including defendants Takai and Pelisamen, signed a "Confidentiality and Non-Disclosure Statement" which contained a confidentiality provision but not a non-competition clause. In addition, Pelisamen signed a "Non-Competition Agreement" (whether Takai signed one was in dispute). Shortly after they signed the Statement and Pelisamen signed the Agreement, Takai and Pelisamen were terminated. Both went to work for Priority Care, a start-up competitor. According to St. Michael's, before they left its employ the two individuals memorized the names of its customers who they then solicited for Priority Care.

The court observed that because of their specialized skills and the fact that there are no other private ambulance services in Saipan, an injunction would result in "an extreme financial burden" to Takai and Pelisamen. "Furthermore, the public will be harmed if enjoining Takai and Pelisamen from working for Priority Care reduces Priority Care's ability to serve its customers to the point of removing St. Michael's only competitor from competition." Finally, St. Michaels conceded that only three customers had been lost to Priority Care, and so St. Michael's could calculate its damages.

Pelisamen also challenged the enforceability of the non-compete agreement on the ground that he received nothing of value in exchange for his signature. The court decided to save "the issue of consideration for another day."

Although this case is pending in a federal court in which few of us practice, the recent opinion contains valuable lessons for all litigants and their lawyers. First, a judge is unlikely to grant an anti-competitive injunction unless the equities weigh heavily in favor of the party seeking injunctive relief. Second, courts scrutinize claims that there is no adequate remedy at law. Third, a party's credibility with the court may be weakened by filing a motion which is minimally supportable. Consequently, parties filing motions that over-reach risk not only denial of the motion but also jeopardy to their chances for ultimate success in the litigation.

Speculative Fears Insufficient for Non-Compete Temporary Restraining Order Against Former Employee

By Paul E. Freehling (October 31, 2012)

While treats are in abundance on Halloween, a Minnesota employer recently received a trick when a federal court denied its temporary restraining order application. A Minnesota federal court held that an ex-employer's apprehension that a former employee violated or would violate a non-compete and confidentiality agreement was entirely speculative and, thus, did not warrant a TRO. *Sempris, LLC v. Watson,* Civil Ac. No. 12-2454 ADM/JJG (D. Minn., Oct. 22, 2012). The court found that there was insufficient evidence of damages or harm to warrant injunctive relief.

In 2009, Watson was hired to work out of his Texas home for Provell which was a Minnesota company that developed, sold and managed membership reward clubs. His title was Vice President for Business Development, and his employment agreement included non-compete and confidentiality provisions. The non-compete agreement prohibited him from directly or indirectly soliciting any current or potential Provell client for one year after termination of his employment.

In January 2011, another Minnesota company, Sempris, purchased Provell's assets. Sempris develops membership and customer loyalty rewards programs for businesses. Watson did not sign a new employment agreement, but Sempris claimed that it assumed Provell's rights under the prior agreement. Sempris made no significant changes in the terms of Watson's employment until October 2011 when the maximum amount he could earn as a commission was capped at 40 % of his base salary (previously there had been no cap). He resigned in September 2012 and accepted a position with a new employer, Reunion, based in Ft. Lauderdale, Florida. Sempris sued him, alleging that Reunion was a competitor and that Watson was violating his non-compete and confidentiality commitments. He denied any such violation and asserted that the covenant against competing with Sempris was unenforceable.

In support of a motion for a TRO, Sempris submitted no evidence that any of its current or potential clients was lost to Reunion. No proof was offered of an identity between Reunion's products or sales methods and those of Sempris. The two companies never competed directly for the same client. In fact, neither company was aware of the other until Watson transitioned.

The court said that even if Watson did work for a competitor, Watson was not shown to have been in contact with any current or potential Sempris client, and his mere possession of trade secrets did not

warrant injunctive relief. Further, Minnesota law disfavors enforcement of a non-competition agreement. Under the circumstances, the harm that would be caused to Watson by enjoining him from gainful employment for one year outweighed the risk to Sempris of denying the TRO. The court did not resolve the dispute concerning validity of the non-compete covenant.

The target of Sempris' litigation was a single former employee whose conduct apparently had not injured his ex-employer. Of course, Sempris' motive in filing the case may have been primarily to discourage other employees from following or emulating Watson. Significantly, perhaps, Reunion was not named as an additional defendant. Or, Sempris may have merely wanted to warn Watson that his activities were being monitored, and to an extent the company succeeded. The court's opinion concluded by cautioning him that "he remains bound by the terms of his employment contract" and "may ultimately be found to be in breach of his Non-Compete Agreement; and, if so, Watson will be responsible for damages to Sempris."

Illinois Supreme Court Affirms Liability Against Former Employer For Unlawful Investigation Methods Used By Private Investigators In Non-Competition Investigation Into Activities By Ex-Sales Agent

By Marcus Mintz (November 21, 2012)

Recognizing the trend across Illinois appellate courts in recent years, the Illinois Supreme Court joined the "vast majority of other jurisdictions" in recognizing the tort of intrusion upon seclusion – a claim against one who intentionally intrudes upon another's privacy if such intrusion would be highly offensive to a reasonable person. In *Lawlor v. North American Corporation of Illinois*, 2012 IL 112530, (Oct. 18, 2012), the departure of a successful sales agent, Lawlor, from the company to a direct competitor, spurred the employer to launch an investigation into whether Lawlor breached her duty of loyalty and non-compete obligations to the company. Lawlor's departure eventually led to both parties asserting claims against each other relating to commission payments, Lawlor's compliance with her obligations to the company, and the company' s liability for its investigator's unlawful acts.

Similar to many employers seeking to protect their customer relationships and confidential information, after Lawlor left the company, it directed its outside counsel to hire a private investigation firm, Probe, to determine whether Lawlor violated her obligations to the company. The company provided Probe with Lawlor's personal information, including her date of birth, her address, her home and cell phone numbers, and her social security number. Probe then hired another investigative firm, Discover, to obtain Lawlor's phone records by using her personal information and pretending to be Lawlor. After Discover obtained Lawlor's phone records, they were sent to the company and distributed among certain employees to determine whether Lawlor had been contacting the company's clients. While the company expected to receive the phone records, it did not direct Probe or Discover into how they were to perform their investigation or what investigative methods they were to use.

At trial, Lawlor contended that the investigators' access to her phone records constituted an intrusion upon her seclusion and the company should be liable under the theory that the investigators were acting as the company's agents. The company disputed any liability, arguing that it did not hire the investigators – its attorney did, and it did not tell the investigators how to do their job. The jury returned a verdict in Lawlor's favor on her claim for intrusion upon seclusion, finding that the company was

vicariously liable for its investigators' conduct and awarding both compensatory and punitive damages against the company.

On appeal to the Illinois Supreme Court, the Court expressly found that because the company knew the phone records were not publicly available, the jury could reasonably infer that the company was setting a process in motion whereby the investigators were going to pose as Lawlor to obtain the phone records. In addition, although the investigators were hired by the company's attorney, the attorney had no other role in the investigation. In contrast, the company approved the payments to the investigators and tasked a company vice president to be the company's contact person for the investigation. Accordingly, the Court held that sufficient evidence existed to sustain the jury's finding that Probe and Discover were acting as the company's agents and that the company is liable for their unlawful acts. However, because the investigation was conducted for a legitimate business purpose, the Court limited the award of punitive damages to Lawlor's compensatory damages, just $65,000, from the jury's award of $1.75 million and the appellate court's remitter to $650,000.

Following Lawlor, employers in Illinois are put on notice that they may be charged with the conduct of their investigators – even if such investigators are not directly hired or controlled by the employer. While professional investigation provides a useful tool to combat against employee malfeasance, efforts must be taken to ensure that investigations are conducted within the bounds of the law to preclude potential liability. Please also see Ken Vanko's informative post about this important new case.

Employers Thankful For New Second Circuit Non-Compete Decision

By Jessica Mendelson and Grace Chuchla (November 22, 2012)

Employers in the Second Circuit are thankful for a recent non-compete summary order in which the Court found that an employee's challenge of his non-compete agreement by way of a preliminary injunction motion failed because he failed to show irreparable injury.

Specifically, the Court found that an employee's potential loss of income does not qualify as an irreparable injury in determining whether to invalidate a non-compete agreement and issue injunctive relief. In sum, in *Hyde v. KLS Professional Advisors Group*, the Second Circuit vacated a preliminary injunction issued by a New York federal district court, and in doing so, provided noteworthy insight on what constitutes irreparable injury with respect to the challenges by employees of non-compete agreements in the Second Circuit.

The facts in this case are fairly straightforward. Bruce Hyde ("Hyde") resigned from KLS Professional Advisors Group ("KLS"), and he then filed suit and obtained a preliminary injunction preventing the enforcement of the restrictive covenants that Hyde had signed at the beginning of his employment with KLS. The covenants prohibited Hyde from contacting any of the firm's past, present, or future clients for three years following his departure from KLS.

In reviewing the district court's grant of a preliminary injunction, the Second Circuit reversed the preliminary injunction granted by the district court, finding that Hyde had clearly failed to show irreparable harm. According to the Second Circuit, irreparable harm was the "single most important prerequisite for the issuance of a preliminary injunction." *Fiaveley Transportation Malmo AB v. Wabtec Corp*, 559 F.3d 110, 118 (2nd Cir. 2009).

According to the Court, prior to this case, the Second Circuit had yet to directly address the question of irreparable harm in the context of a challenge by an employee of his non-compete agreement. The reasoned, however, that in both the Supreme Court's opinion in *Sampson v. Murray*, 415 US 61 (1974), and the Second Circuit's opinion in *Savage v. Gorski*, 850 F.2d 64 (2d Cir. 1988), the courts denied requests for injunctions by government employees who had sought injunctions to keep or extend the jobs. Based on these cases, the Court reasoned, in what must have been a turkey of a decision for

Hyde, that loss of employment and any difficulties arising therein do not constitute irreparable injury. Therefore, Hyde's alleged showing that his restrictive covenant inhibited his ability to find a new job was insufficient to satisfy the irreparable harm requirement. The Court reasoned that "difficulty in obtaining a job is undoubtedly an injury, but it is not an irreparable one" as any harm suffered could be adequately compensated with monetary damages at trial.

Hyde also argued that his restrictive covenanst caused him irreparable harm through a loss of client relationships. The Court, however, quickly rejected that argument given that "Hyde had signed multiple agreements in which he acknowledged that KLS's client base was proprietary and belonged to the firm." Furthermore, even if the Court were to assume that Hyde had a legally protected interest in his client list, he had failed to demonstrate that losses related to his client list could not be remedied with monetary damages.

The Second Circuit's ruling may be helpful to employers seeking to enforce non-compete agreements against their former employees and also provide them with helpful reasoning should former employees challenge their non-compete agreements.

Massachusetts Court Rules That Facebook Posting of New Job Does Not Violate Non-Competition Covenant

By Paul E. Freehling (November 30, 2012)

A hair salon's motion for entry of a preliminary injunction against a stylist was denied even though she had signed non-competition, non-solicitation and confidentiality agreements with the salon, and immediately after leaving her prior employment she was employed by a nearby competitor, a fact noted on her Facebook page. *Invidia LLC v Difonzo*, Case No. MICV20123798H (Middlesex [Mass.] County Super. Court, Oct. 22, 2012).

The stylist, DiFonzo, worked at the Invidia salon for two years. At the outset of her employment, she signed a non-competition covenant that had two-year and ten-mile restrictions. Invidia claimed that she brought no clients of her own, and it stated that it gave her "education and training" which were "unprecedented in the salon industry." When she resigned from Invidia, she immediately commenced employment by its competitor less than two miles away. Information concerning her new position was posted on her Facebook page. Although Invidia said her departure precipitated an "unprecedented . . . wave of no-shows, cancellations or non responses," the salon could not demonstrate that she was responsible.

After Invidia's attorney threatened to sue both DiFonzo and the competitor, she was laid off. In a conversation with the competitor's owner, Invidia's majority owner, Patzleiner, allegedly stated that Invidia simply "intended to send a message" to its employees and "did not care" whether DiFonzo solicited Invidia's customers.

The Superior Court of Middlesex (Massachusetts) County declined to determine immediately whether the two-year and ten-mile restrictions were too broad to be enforceable. Rather, the court concluded that since Invidia demonstrated its ability to calculate with reasonable certainty the monetary loss it would sustain for each client DiFonzo takes, money damages should suffice to compensate Invidia if it prevails at trial. There was no evidence that DiFonzo breached her confidentiality covenant or solicited any Invidia customers. A few contacted her but, according to the court, "So long as they reached out to [her] and not vice versa, there is no violation of the non-solicitation provision." Thus, even though Invidia was likely to succeed in proving that DiFonzo breached the non-competition covenant and that she may have the opportunity to compete in the future, the court denied Invidia's motion for a preliminary injunction.

This decision stands for the proposition that a non-solicitation covenant is not violated by a Facebook post that merely informs readers of the ex-employee's subsequent employment. Also, the ruling illustrates difficulties an employer faces in demonstrating immediately after an employee quits that the ex-employee's conduct will inflict an irreparable injury. Invidia asserted, understandably, that it had good reasons not to interview its clients and bring DiFonzo's departure to their attention. Yet, without evidence that she solicited them or used confidential information, Invidia could not show that the harm it faced absent an injunction outweighed the harm to her if she was rendered unemployable for an extended period.

New York Federal Court Rejects Heightened Specificity Pleading Standard for Breach of Confidentiality and Non-Disclosure Claim

By Joshua Salinas and Jessica Mendelson (December 4, 2012)

The secret is out, Tic Tacs and bubblegum have the most valuable and desirable real estate in the entire grocery store.

On September 27, 2012, a district court for the Eastern District of New York granted in part and denied in part a motion to dismiss in a commercial dispute arising out of the home of these consumables–grocery checkout displays. *Dorset Industries, Inc. v. Unified Groceries, Inc*, 2012 WL 4470423 (E.D.N.Y. Sept. 27, 2012).

The dispute arose when the defendant, inter alia, allegedly misappropriated the plaintiff's trade secrets and confidential information to allegedly create a competing business program that marketed checkout areas, which also allegedly "cut out" the plaintiff from their alleged exclusive business arrangement.

Plaintiff Dorset Industries develops and implements "checkout programs," which allegedly allow grocers to maximize their sales opportunities by utilizing the front end of checkout areas. These areas are believed to be the most desirable real estate in the store as the volume of foot traffic is unmatched. To capitalize on this valuable marketing opportunity, Dorset allegedly uses its "knowhow, experience, and intellectual property" to design and manufacture display units for the grocers, and accordingly leases space in those displays to manufacturers of grocery products (e.g. candy, magazines, and health and beauty products).

Defendant Unified Groceries is allegedly one of the largest retailer-owned grocery cooperatives, and allegedly the largest wholesale grocery distributor in the Western United States. Unified allegedly signed agreements with Dorset to implement Dorset's checkout programs. Under the alleged agreements, Unified would be responsible for finding retail grocers within its member stores to sign up for Dorset's checkout program; Dorset would be exclusively responsible for providing the displays and leasing the spaces out to manufacturers. Both parties would share in the resulting income stream.

Unified also signed confidentiality and non-disclosure agreements that restricted the use and disclosure of any business information provided by Dorset concerning the business methods and procedures of its checkout programs.

A dispute arose when Unified allegedly attempted to circumvent the parties' business arrangement by creating its own checkout program and dealing directly with the manufacturers to lease the checkout display space. Consequently, Unified was allegedly able to "cut out" the intermediary (i.e. Dorset) and contract with the manufacturers directly–thereby obtaining 100% of the income stream. Unified also allegedly notified Dorset that it was terminating their program agreements, although the timing and sufficiency of that notification was disputed.

Dorset sued Unified in New York state court, alleging breach of contract, breach of the confidentiality agreement, usurpation of corporate opportunity, and unfair competition. Dorset also sought a declaratory judgment that the agreement's termination was invalid. Unified subsequently removed the case to the Eastern District of New York and filed a motion to dismiss the entire lawsuit pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.

The significance of this case concerns the Court's analysis of the third cause of action–breach of confidentiality and non-disclosure provisions. Unified contended that (1) Dorset failed to identify any confidential information allegedly used by Unified in creating its competing checkout program, (2) any such information was not confidential, and (3) Dorset failed to adequately allege that Unified misappropriated any confidential information. The Court disagreed.

The Court recognized that under New York law, ***a combination of characteristics and components in the public domain could be a protectable trade secret when uniquely combined into a unified process or product***. The Court found that Dorset had set forth facts plausibly alleging that the information allegedly utilized by Unified constituted confidential information and/or trade secrets when Dorset identified this information as "checkout counter programs and its business model, plan-o-grams and designs, methods and procedures … including creating and designing the specific Program for Unified."

Additionally, the Court found that Dorset adequately alleged that it took reasonable efforts to guard the secrecy of its trade secret, confidential, and proprietary information because Dorset alleged that it (i) restricted access to certain information within the company, (ii) utilized passwords to protect its computer system, (iii) limited remote access to those with authority, and (iv) limited access to certain documents containing confidential information within the company. The Court also underlined Dorset's use of confidentiality and non-disclosure agreements, which defined such confidential and proprietary information and which also contained several express restrictive covenants, including specific covenants of non-disclosure of trade secrets and confidential and proprietary information.

The Court **emphatically** rejected Unified's argument that Dorset's complaint required a greater level of specificity at the pleading stage.

This case is also noteworthy considering the fact that Dorset allegedly admitted that ***it does not even know whether Unified had actually used or disclosed any confidential information***, ***or whether it was merely speculating that it might do so at some unspecific future date***. Unified contended that, at most, Dorset had alleged that Unified misappropriated a single form used for entering into

agreements with vendors, and that the form did not constitute trade secret or confidential information because it was a one page five line form that contained nothing more than basic contact information.

The Court explained that it could plausibly infer that the confidentiality provisions were violated by Unified when it allegedly created its competing checkout program. Specifically, the court reasoned that (1) the form supported **the inference** that Unified created a checkout program that utilized the same methods and procedures as the Dorset program, (2) Unified had previously admitted to Dorset its intent to take over Dorset's program after observing it for several years, and (3) the subsequent decline of customers that signed up for Dorset's program compared to previous years implied that Unified began enrolling customers into its competing program. Thus, the Court found a **reasonable inference** from Dorset's allegations that Unified had created a checkout display program that would replicated the allegedly confidential "methods or procedures" used in operating Dorset's program.

Accordingly, the court denied Unified's motion to dismiss as to Dorset's claim for breach of confidentiality and non-disclosure provisions. The court also granted Unified's motion to dismiss on the unfair competition and usurpation of opportunities claims, and granted in part and denied in part the claims for declaratory judgment and breach of implied covenant of good faith and fair dealing.

This case reminds us of the importance of non-disclosure and confidentiality agreements when conducting business with third parties. The existence of these agreements is often the deciding factor when analyzing whether the trade secret holder took reasonable efforts to maintain and protect the secrecy of the information. This case also reiterates that allegations for misappropriation of trade secrets and confidential information (at least in this Court) are not subject to a heightened level of specificity at the pleading stage. Indeed, as with other claims, the Court accepted as true the factual allegations set forth in the complaint and drew all reasonable inferences in the plaintiff's favor. As illustrated in this case, a plaintiff that lacks direct evidence of misappropriation of trade secrets or confidential information should plead all corresponding facts that support a plausible inference that misappropriation occurred.

US Supreme Court Strikes Down Oklahoma Supreme Court Decision And Holds That Arbitrator, Rather Than Court, Must Determine the Enforceability of Non-Compete Agreements Containing Arbitration Provisions

By Robert Milligan and Grace Chuchla (December 5, 2012)

There are not many issues that the United States Supreme Court can unanimously resolve in five short pages.

The preeminence of the Federal Arbitration Act ("FAA") is apparently one such issue, as the Supreme Court recently illustrated in its November 26 per curium opinion in *Nitro-Lift Technologies LLC v. Howard*, 568 U.S. __ (November 26, 2012).

In the decision, the Supreme Court reaffirmed the FAA's national policy in favor of arbitration and emphatically shot down an attempt by the Oklahoma Supreme Court to exert judicial review over the enforceability of a non-compete agreement that contained a mandatory arbitration provision.

This dispute arose when Eddie Lee Howard and Shane D. Schneider left Nitro-Lift Technologies ("Nitro-Lift") and began working for one of Nitro-Lift's direct competitors in Arkansas. Upon learning of Howard and Schneider's new employment, Nitro-Lift served them with a demand for arbitration in an effort to enforce the non-competition agreements that both had signed at the outset of their employment. These agreements contained a clause that required arbitration in Houston, Texas of all disputes arising under the agreement and for the application of Louisiana law. However, despite this arbitration clause, Howard and Schneider responded to Nitro-Lift's demand for arbitration by filing suit in the District Court of Johnson County, Oklahoma and asking the court to enjoin the enforcement of their non-competition agreements as contrary to Oklahoma state law.

The district court dismissed Howard and Schneider's complaint because the arbitration clause demanded that an arbitrator, rather than the court, settle such disputes. However, plaintiffs appealed to the Oklahoma Supreme Court, which not only accepted the appeal but also ordered the parties to demonstrate why Okla. Stat., Tit. 15, §219A should not be the deciding factor in this dispute over the enforceability of a non-competition agreement. The Oklahoma Supreme Court held that: 1) in

conformance with its prior jurisprudence, the existence of an arbitration agreement in an employment contract does not prohibit judicial review of the underlying agreement; 2) as drafted, the non-competition covenants are void and unenforceable as against Oklahoma's public policy expressed by the Legislature's enactment of Okla. Stat., Tit. 15, §219A; and 3) judicial modification of the covenant not to compete is inappropriate where, as here, the contractual provisions would have to be substantially excised, leaving only a shell of the original agreement, and would require the addition of at least one material term. For an in-depth look at what the Oklahoma Supreme Court said in its November 2011 opinion, see our previous post.

In a nutshell, the US Supreme Court was not pleased with the Oklahoma Supreme Court's attempt to circumvent and weaken the FAA and the disregard that it showed toward Supreme Court precedent. Despite the Oklahoma court's claim that it had conducted an "exhaustive review of US Supreme Court decisions construing the Federal Arbitration Act," the Supreme Court flatly rejected the argument that its previous decisions did "not…inhibit [Oklahoma's] review of the underlying contract's validity" (slip op. at 3).

Under its controlling authority, the US Supreme Court ruled that an arbitrator must decide whether the non-compete agreement was valid. The Court stated that "it is a mainstay of the [FAA's] substantive law that attacks on the validity of the contract, as distinct from attacks on the validity of the arbitration clause itself, are to be resolved by the arbitrator in the first instance, not by a federal court."

Additionally, the Court took issue with the Oklahoma Supreme Court's claim that its "decision rests on adequate and independent state grounds" (slip op. at 3). Rather, as the Supreme Court saw it, Oklahoma's reasoning "necessarily depended upon a rejection of the federal claim" and controlling federal laws and precedents (slip op. at 3). Thanks to the all-important Supremacy Clause of the US Constitution, such a rejection cannot stand. Thus, per the Supreme Court's previous decisions in cases such as *Buckeye Check Cashing, Inc. v. Cardegna*, 546 U.S. 440 (2006), *Preston v. Ferrer*, 522 U.S. 346 (2008), and *Prima Paint Corp. v. Flood & Conklin Mfg, Co.,* 388 U.S. 395 (1967), the question of whether or not Howard and Schneider's non-competition agreements are enforceable under §219A is not a proper question for a state court to answer. In short, although the validity of an arbitration agreement is subject to a court's review, "the validity of the remainder of the contract (if the arbitration provision is valid) is for the arbitrator to decide" (slip op. at 4).

Coming on the heels of *AT&T Mobility v. Concepcion*, 563 US __ (2011), this opinion is yet another clear affirmation of the US Supreme Court's desire to bolster the power of the FAA. Especially notable in this case is the fact that the non-competition agreement in question was, as we discussed in our previous post, unenforceable under Oklahoma state law. Nevertheless, the Supreme Court still chose to remove the question of the agreement's enforceability from the hands of the state court and turn it over to an arbitrator – a clear demonstration of the high court's desire to maintain the process of arbitration even in the face of a legal question with an all but perhaps foregone conclusion at least under Oklahoma law. Query though whether an arbitrator in Texas, where the arbitration is to be conducted pursuant to the agreement, may have a different view of the enforceability of the non-competition provisions and may question the application of Oklahoma law where the agreement

specifies the application of Louisiana law. Finally, employers and employees alike should note that there is nothing in this opinion that alters the status of non-competition agreements under Okla. Stat., Tit. 15, §219A. Such agreements still remain generally unenforceable, although such a question will now often be for an arbitrator to decide if an employer's utilizes arbitration agreements.

As far as takeways from this decision, employers should carefully consider whether disputes with employees concerning non-compete/trade secrets issues should be resolved through the courts or arbitration and draft their agreements accordingly. Some legal commentators such as John Marsh believe that the arbitration of non-compete/trade secret disputes in the employment context should rarely be handled by arbitration and that employers should include carve outs for such disputes if they generally employ arbitration agreements with their employees. Please also see Ken Vanko's informative summary of the case. In our experience some of the reasons why the courts may be preferably for such disputes include the ability to obtain injunctive relief more expeditiously as well as the appearance of authority and finality of a court order, rather than an arbitrator's order. A word of caution on the use of such exclusions, however, as at least in California, some courts have pointed to such exclusions in arbitration agreements as purported evidence of unconscionability to invalidate such agreements. Notwithstanding those decisions, a California federal court recently ruled that the use of such an exclusion was not unconscionable.

Accordingly, the utilization of arbitration agreements, coupled with forum selection, choice of law, and consent to jurisdiction provisions, specifying an employer's pro non-compete forum, with employees from jurisdictions that limit or prohibit non-compete agreements may provide some employers with additional options that they did not otherwise consider, notwithstanding the drawbacks discussed above. Such a strategy is not without risk, however, as employees can always attempt to challenge such provisions in their home forum on several grounds, including unconscionability, adhesion, or lack of reasonableness under forum selection standards, but the scope of such challenge may be limited by this decision, the United States Supreme Court's other recent pro arbitration decisions, as well as future Supreme Court decisions.

Legislation

At Long Last, New Jersey Passes Trade Secrets Act

By David Monachino (January 9, 2012)

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.

Virginia Bill Proposes to Ban Most Non-Competes

By Rebecca Woods (January 30, 2012)

Although Virginia is already generally hostile to non-competition agreements, enforcing only those that are very limited in function, geographic scope, and duration, a bill has been proposed in the 2012 session of the Virginia General Assembly that would severely restrict the enforceability of non-compete agreements. House Bill 1187 proposes to add to the Code of Virginia a provision that, with limited exceptions, would deem unlawful "any contract that serves to restrict an employee or former employee from engaging in a lawful profession, trade, or business of any kind." The limited exceptions would only allow businesses, partners in a partnership, or members of a limited liability company to agree to refrain from carrying on similar business in the area in which it or they had been conducting such business. The bill excepts from its coverage nondisclosure agreements intended to prohibit the sharing of certain information such as trade secrets and proprietary or confidential information.

The effect of the bill, if passed, would be to invalidate all employee non-compete agreements. Proponents of the bill claim it would transform Virginia into an entrepreneur haven like Silicon Valley. Opponents have not yet made public pronouncements, but it is generally expected that business interests will lobby against the bill.

New Jersey Adopts Variation of Uniform Trade Secrets Act

By Robert Milligan (February 3, 2012)

With Governor Chris Christie's signature on January 9, 2012, New Jersey became the 47th state to adopt a form of the Uniform Trade Secrets Act (UTSA). Previously governed by common law, trade secrets of persons or entities in New Jersey will now have statutory protection under the New Jersey Trade Secrets Act (S-2456/A921). The new statute went into effect immediately after its signing, and applies to all new claims which arise on or after January 9, 2012.

To read the full text of the law, please visit this website.

Effects of the Act on Trade Secret Protection in New Jersey

The New Jersey Trade Secrets Act (NJTSA) sets forth clear statuatory language for trade secret protection for the first time in the state, including defining what a trade secret is as well as what acts constitute misappropriation of a trade secret. Prior to the Act, trade secret analysis relied on the Restatement of Torts, pursuant to New Jersey cases such as Sun Dial Corp. v. Rideout (1954), making protection somewhat inconsistent as varying interpretations of the common law were applied.

Protections afforded to persons and entities with valid trade secret claims under the NJTSA include injunctive relief for "actual or threatened misappropriation, & a reasonable royalty" for misappropriation, and monetary damages (compensating for both actual losses as well as "unjust enrichment caused by the misappropriation"). In addition, for cases of "willful and malicious misappropriation," attorney fees may be recovered and punitive damages may be awarded for up to two times the damages otherwise awarded. There is also no statutory requirement to identify trade secrets prior to commencing discovery unlike some jurisdictions.

Variations between the UTSA and NJTSA

Despite being based on the UTSA, the New Jersey legislature did make certain adjustments in drafting its state's trade secret statute. One such adjustment was the exclusion of a clause present in the UTSA which directs courts to take trade secret rulings in other states into account when handing down decisions. Another key difference between the UTSA and NJTSA is the NJTSA's explicit mention that the provisions of the act are "in addition to and cumulative of any other right, remedy or prohibition provided under the common law or statutory law of this State." In practice, this allows confidential and proprietary information that does not satisfy the trade secret requirements set forth by the act, but was previously protected under the state's common law, to remain protected. This in contrast to some states who have adopted adapted versions of the UTSA, many of which take the stance of preemption of common law claims. Finally, the NJTSA contains more robust protections for the preservation of trade secrets in the court system than in the standard UTSA. Courts are directed to use "reasonable means" to ensure the protection of trade secrets during litigation, including sealing court records when necessary, limiting disclosure of trade secrets to attorneys' eyes only, and granting protective orders

during discovery. This is particularly significant because some jurisdictions are reluctant to seal court records even in trade secrets cases.

Advice for Employers

The NJTSA offers companies statutory protections for trade secrets, though it is their responsibility to ensure this protection by making "efforts that are reasonable under the circumstances to maintain its secrecy." To accomplish this, companies should have explicit policies preventing disclosure of their trade secrets while also being vigilant in educating employees of their responsibilities. Any suspicion of trade secret misappropriation by an employee or competitor should be investigated immediately in order to prevent the loss of rights in trade secret protection. Under the NJTSA, the statute of limitations for bringing a misappropriation claim has been reduced from six years, to three years from discovery of the misappropriation. An attorney with knowledge and experience in litigating trade secret claims is best suited to guide companies through this process.

Questions for the Future

With New Jersey joining the other 46 states who have passed some form of trade secret protection legislation, just three states, Texas, New York and Massachusetts, have yet to adopt a variation of the UTSA. It will be interesting to se how the New Jersey courts construe the new law, including "threatened misappropriation" and preemption of common law claims. How long these hold-outs will remain reliant on common law protections is an important discussion moving forward. Part of the UTSA's goal when drafted in 1979 was to address the disparity in trade secret protection across state lines, and to that end there has been some interest in Congress in instituting federal civil trade secret protections, but the scope and preemptive effect of such legislation is entirely uncertain.

Idaho and New Hampshire Propose Significant Trade Secret and Non-Compete Legislation

By Jessica Mendelson (March 22, 2012)

Recently, state legislatures in both Idaho and New Hampshire have proposed significant legislation relating to trade secret and non-compete agreements. Each of these bills has the potential to significantly impact employers and their hiring processes.

Idaho

In the Idaho state senate, a bill was recently introduced to amend the Idaho Trade Secrets Act. The proposed bill clarifies that trade secret misappropriation requires acquisition, disclosure, use or physical retention of the information. As a result, memorization of a trade secret does not qualify as misappropriation. Whether trade secrets can be misappropriated via memory is very much an undecided issue, and there is much disagreement nationally. In Massachusetts, for example, some courts have found that a person, can, in fact, be held liable for misappropriation by memory, while others have found the exact opposite. As a result, this issue is likely to remain a contested topic throughout the United States.

In addition to requiring physical possession for misappropriation, the bill would also allow the prevailing party to recover reasonable attorney's fees. Finally, the bill makes anyone acting in concert with a misappropriator jointly and severally liable for misappropriation if they turn a blind eye to the misappropriation.

New Hampshire

In New Hampshire, the House recently considered a bill requiring employers to disclose any non-compete and non-piracy agreements before hiring an individual. If this bill were to pass, any contract which does not comply with it would be void and unenforceable. On March 7, the House recommended that the bill be passed, but the vote has yet to occur. Such a policy would ensure that employees are fully aware of their future rights before accepting a new position.

We will continue to keep you apprised of relevant future updates in state trade secret and non-compete laws.

Access To Social Media Accounts In The Hiring Process And Employer Ownership Of Trade Secrets Or Confidential Information Contained In Social Media Accounts: Legislation On Horizon?

By Jessica Mendelson (April 4, 2012)

On Monday March 26, 2012, Senators Richard Blumenthal (Connecticut) and Chuck Schumer (New York) called for federal agencies to determine whether requiring prospective hires to hand over social networking usernames and passwords violates federal law. Blumenthal and Schumer called on the United States Equal Employment Opportunity Commission ("EEOC") to investigate whether such practices violate federal anti-discrimination laws and the United States Department of Justice to investigate whether such practices violate the Stored Communication Act ("SCA") or Computer Fraud and Abuse Act ("CFAA").

Allowing access to a prospective employee's social media password could allow the employer to access information the company is prohibited from asking about in the hiring process. Under the Americans with Disabilities Act and Genetic Information Nondiscrimination Act, prospective employers are prohibited from asking about genetic information, age, or disability. However, if employers can access a prospective employee's social media page, they may have access to such information. An employer who then chooses not to hire a member of a protected class or takes other adverse action, may run the risk of allegations that the company violated federal law or state law by refusing to hire a person because of his or her membership in a protected class.

In addition to potentially violating anti-discrimination laws, allowing prospective employers to access a person's social networking username and password may implicate the SCA or CFAA, according to Blumental and Schumer. "Requiring applicants to provide login credentials to secure social media websites and then using those credentials to access private information stored on those sites may be unduly coercive and therefore constitute unauthorized access under both SCA and the CFAA," they said in a letter to Attorney General Eric Holder Jr. These two acts, respectively, prevent unlawful access to electronic information without authorization, and unlawful access to a computer without authorization. In *Konop v. Hawaiian Airlines Inc.,* 236 F.3d 1035 (2001), a case cited in their letter, the Ninth Circuit held that the unauthorized access and review of contents of a password protected website can be a violation of the SCA.

Although many commentators agree that it is fairly unusual for employers to ask job applicants for social network usernames and passwords, the issue is one that inspires heated debate. It also appears

that the practice may be more prevalent amongst law enforcement agencies and schools. While commentators disagree as to whether the use of such a pre-hiring practice is legal, commentators generally agree that the practice is not likely wise because the information an employer discovers could lead to a claim regarding disparate treatment or discrimination.

Recently, in Michigan, a teacher was fired for failing to handover her password and username after a parent complained of objectionable content on her Facebook page. The story received national media attention, and there has been significant debate over what expectation of privacy an employee should be entitled to. Facebook itself has come out against such practices, issuing a written statement objecting to employers asking applicants or employees for this information. The company has also threatened to sue employers who utilize such practices.

As of now, the current debate on this issue is primarily focused on pre-hire required turnover of passwords for social media accounts. However, in the future, the argument is likely to focus on whether companies can assert an ownership interest in such social media accounts in whole or part, including the passwords, contacts, and other information contained in the accounts and whether there is truly any differentiation between personal and work accounts.

The question of whether a company can claim ownership in a social media account and the extent to which a company can is just beginning to be addressed by the courts. This past year, in *Eagle v. Morgan*, a federal court in Philadelphia ruled an employer could claim ownership of a former executive's LinkedIn Account, where the employer had significant involvement in the creation, maintenance and operation of the account. Similarly, the Northern District of California recently addressed the case of *PhoneDog v. Kravitz,* which addressed the question of corporate ownership of a Twitter Account. There, PhoneDog, an interactive mobile news and reviews web resource, sued Noah Kravitz, a former employee, who the company claims unlawfully continued using the company Twitter account after he quit. The court found there was sufficient evidence to state a claim for trade secret misappropriation, based on the argument that the Twitter account, the password, and the followers were trade secrets.

Most recently, a Colorado federal court in *Christou v. Beatport, LLC*, No. 10-cv-02912-RBJ-KMT, 2012 WL 872574 (D. Colo. Mar. 14, 2012), allowed a plaintiff's trade secret misappropriation claim premised on the theft of MySpace "friends" to proceed. The court found Plaintiff's efforts and expense in "friending" thousands of potential dance club patrons, and thus having their contact information and permission to contact them, could constitute a protectable trade secret under Colorado law.

Both the legality of pre-hire required turnover of social media passwords and company ownership of social media accounts is likely to be a growing issue in the future, and we will continue to follow it closely.

Hey Lumbergh, You Don't Own My Facebook Account: Maryland Passes Legislation To Protect Employee's Social Media Accounts

By Jessica Mendelson (April 18, 2012)

Recently the legality of requiring prospective hires to hand over social networking usernames and passwords received national attention when New York Sen. Charles Schumer and Connecticut Sen. Richard Blumenthal asked the U.S. Department of Justice to investigate whether the practice violates federal laws. Although federal legislation has yet to be passed, state legislatures have begun to address the issue.

This month, Maryland will become the first state to pass a law on the practice. Two identical bills, S.B. 433 and H.B. 964, were passed by the State legislature on Monday, and are now headed to Governor Martin O'Malley, who is likely to sign the legislation into law. Under this legislation, which will take effect on October 1, 2012, employers and their agents or representatives are prohibited from requiring workers and job applicants to "disclose any user name, password, or other means for accessing a personal account or service" electronically. In addition, employers are prohibited from refusing to hire an applicant for not providing access to such information. Similarly, employers are not permitted to terminate or discipline an employee for refusing to provide such information.

In addition to protecting the privacy of current and prospective employees, the Maryland law also provides employers with some protections as well. Under the terms of the law, employees are prohibited from downloading "unauthorized employer proprietary information or financial data" to personal accounts or to websites, and employers are permitted to investigate upon hearing of such activity. Such investigations are intended to ensure "compliance with applicable securities or financial law or regulatory requirements." Additionally, employers are permitted to require employees to provide passwords and login information for non-personal accounts that are part of the employer's own systems, such as company e-mail accounts. Please find our management alert on this new law.

Similar legislation has been filed or is under consideration in other states, including California, Illinois, and New Jersey. In New Jersey, Assemblyman John Burzichelli recently proposed legislation, stating that the practice of handing over usernames and passwords is "no different than asking someone to turn over a key to their house. Demanding this information is akin to coercion when it might mean the difference between landing a job and not being able to put food on the table for your family."

In Illinois, State Representative LaShawn Ford proposed House Bill 3782, which would prevent employers from requesting any employee or prospective employee to provide a password or account

name for a social networking site. The Illinois state Senate will vote on the bill in the next couple of weeks. Assuming the bill passes in the Senate, it will move to a full House vote. According to Ford, the bill will help prospective employees, “afraid to speak up because they don’t want to prevent themselves from receiving employment, and it protects employers from facing future lawsuits,” which in turn saves taxpayers money.

The increasing state and federal regulation of this practice suggests a growing trend in protecting the privacy of individual employees. However, some employers are getting around this legislation through the use of third party applications, such as BeKnown or BranchOut, which can be used to provide limited access personal profiles if a job seeker allows it. Often, a prospective employee will be asked to check a box in the job application allowing the use of such third party software. Lori Andrews, an internet privacy law professor at Chicago-Kent College of Law, worries about the pressure placed on applicants, even those who voluntarily provide access to social networking websites. According to Andrews, “Volunteering is coercion if you need a job.”

Some states, such as California, have taken viewpoints like Andrews’ into account in proposing legislation. California Senator Leland Yee (D-San Francisco/San Mateo) recently introduced legislation designed to prevent employers from requesting employees or job applicants provide their social media usernames and passwords, and prohibit employees from voluntarily sharing such information. According to Yee, “It is completely unacceptable for an employer to invade someone’s personal social media accounts. Not only is it entirely unnecessary, it is an invasion of privacy and unrelated to one’s work performance or abilities.” The Senate Committee on Education recently approved the legislation authored by Senator Yee.

The debate over the amount of privacy interest prospective employees and existing employees are entitled to with respect to social networking is far from over, and we will continue to provide updates in this important area.

Massachusetts Legislature Considers New Social Media Bill

By Ryan Malloy and Erik Weibust (May 1, 2012)

The Massachusetts legislature recently joined the growing wave of states nationwide that are considering bills, which, if enacted, would forbid employers from requesting social media user names and passwords from employees or prospective employees. The issue of privacy with regards to social media accounts has garnered significant attention across the country during recent months, as some employers have blocked employee access to social media websites such as Facebook or Twitter, while others have terminated employees for refusing to provide their account access information.

The Massachusetts Social Media Privacy Bill (entitled "An Act relative to social networking and employment") provides, rather simply, that "[n]o employee or prospective employee shall be required to provide access to an employer for a social networking site." Furthermore, the bill prohibits any employer from asking employees or prospective employees to provide "any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website or electronic mail." The bill makes clear that it does not prohibit employers from obtaining information about employees or prospective employees that is in the public domain, such as by searching their publicly-available online profiles on Facebook, LinkedIn, or the like, nor does it "limit an employer's right to promulgate and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding internet use, social networking site use, and electronic mail use."

As previously reported, on April 9, 2012, Maryland became the first state to pass a social media privacy bill. In addition to prohibiting employers from asking or forcing employees and prospective employees to provide social media login credentials, the Maryland bill prohibits employers from taking adverse action against an employee who refuses to hand over the requested social media information. Although legislatures in other states, including California, Illinois, and Michigan, are also considering similar bills, Congress is not yet on board. In late March, a rule amendment that would have allowed the Federal Communications Commission to prevent employers from forcing potential employees to disclose social media passwords was halted.

Georgia's New Restrictive Covenant Act Turns One Year Old

By Daniel Hart and Bob Stevens (May 14, 2012)

Friday, May 11, 2012 marked the one-year anniversary of Georgia's new Restrictive Covenant Act ("New Act"). As we have written on this blog before (here and here), passage of the New Act marked a dramatic change in Georgia's public policy regarding restrictive covenants in employment agreements. Prior to passage of the New Act, Georgia was one of the most difficult jurisdictions for employers to enforce restrictive covenants against former employees. With the passage of the New Act, Georgia is now a comparatively favorable forum for employers seeking to enforce restrictive covenants against former employees.

Among other changes, the New Act creates statutory presumptions under which courts must presume that restrictive covenants two years or less in duration are reasonable in time and that restrictive covenants 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 Act also permits Georgia courts to "blue pencil" (i.e., partially enforce) restrictive covenants that otherwise would be overbroad and, therefore, completely unenforceable under prior Georgia law. Because the New Act applies only to restrictive covenants entered into on or after May 11, 2011, few court decisions have construed the New Act in the one-year since its passage. But in one decision, the United States District Court for the Northern District of Georgia exercised its power under the New Act to modify a restrictive covenant that would have been unenforceable under previous Georgia law.

In that decision, *Pointenorth Ins. Group v. Zander*, No. 1:11-cv-3262-RWS, 2011 U.S. Dist. LEXIS 113413 (N.D. Ga. 2011), an employer sought to preliminarily enjoin its former employee from violating customer nonsolicitation covenants in an employment agreement that she signed on May 11, 2011 – the same day that the New Act went into effect. The covenant prohibited the employee from soliciting,

accepting, or attempting to solicit or accept, "any of the Employer's clients which would be in competition with the products or services offered by the Employer, including actively sought prospective clients, with whom Employee had any contact or who were clients of Employer within the three months immediately preceding such termination of this Agreement." The district court granted the employer's motion for preliminary injunction. Although the covenant was overbroad because it extended to all of the employer's customers, and not merely those with whom the employee had interacted, the court blue-penciled the provision to prohibit the employee only from soliciting customers whom she had contacted and assisted with insurance. By prohibiting the employee only from "soliciting" these customers, the court also effectively struck the term "accepting" from the provision.

The *Pointenorth* decision remains significant in that it is the first – and, to date, only – published opinion in which a court has used its power under the New Act to modify an overbroad restrictive covenant. Although only time will tell whether other courts follow the lead of the *Pointenorth* court, this decision – and the language of the New Act itself – suggest that employers will have considerably greater ease in enforcing restrictive covenants in Georgia than they did prior to enactment of the New Act.

Despite this positive trend for employers, it is also clear that Georgia courts will continue to apply previous Georgia law to agreements that pre-date the New Act, as illustrated by another decision of the United States District Court for the Northern District of Georgia that we previously discussed here. In that case, *Boone v. Volt Information Sciences, Inc. v. Corestaff Support Servs., Inc.*, No. 1:11-CV-1175-RWS 2011, U.S. Dist. LEXIS 119297 (N.D. Ga. 2011), a former employee and his new employer filed a declaratory judgment action against a former employer, seeking a declaration that a noncompete agreement between the employee and former employer was unenforceable under Georgia law. The noncompete agreement had a Delaware choice-of-law provision, and the district court initially concluded that Delaware law would apply to the agreement because Delaware law is in accord with Georgia's new public policy position on restrictive covenants in employment agreements. On a motion for reconsideration, the district court vacated its prior order, holding that, under the Georgia Court of Appeals' decision in *Bunker Hill Int'l, Ltd. v. Nationsbuilder Ins. Servs., Inc.*, 710 S.E.2d 662 (Ga. Ct. App. 2011), courts must apply Georgia public policy in effect at the time the agreement was entered into. Because the agreement was signed in 2008, it was subject to Georgia's old public policy, which was not in accord with Delaware law. Finding that the noncompete agreement was unenforceable as a matter of law under old Georgia law, the court granted summary judgment to the plaintiffs on their claim for declaratory relief.

Despite the limited number of published decisions that have interpreted the New Act in the first year of its existence, three trends appear clear: (1) Georgia courts are considerably more likely to enforce restrictive covenants under the New Act than they were under prior Georgia law, (2) Georgia courts will "blue pencil" overbroad restrictive covenants, and (3) Georgia courts will continue to apply prior Georgia law to agreements that predate the New Act. If you have employees in Georgia and have not yet updated your standard restrictive covenant agreements to take advantage of the New Act, now is an excellent time to take advantage of this change in the law. If you are interested in reviewing your existing restrictive covenant agreements for compliance with the New Act, or if you would like assistance drafting such agreements for your workforce, contact a Seyfarth Shaw Trade Secrets Group attorney.

New Federal Trade Secrets Legislation Proposed

By Jessica Mendelson and Robert Milligan (July 19, 2012)

On July 17, 2012, Democratic senators Herb Kohl (Wisconsin), Sheldon Whitehouse (Rhode Island), and Chris Coons (Delaware) introduced legislation which they believe will aid American companies in effectively combating the theft of trade secrets. The proposed legislation, known as the Protecting American Trade Secrets and Innovation Act of 2012 ("PATSIA"), will allow American companies dealing with economic espionage and trade secret theft to seek redress in federal courts, rather than having to file suit in individual state courts. A similar bill was introduced in October of 2011 as reported here.

The bill is intended to create one federal statute under which businesses could bring lawsuits in the federal courts, rather than requiring businesses to rely on a "patchwork" of state laws to seek redress. Under the current law, companies generally file lawsuits in individual state courts, requiring litigants to navigate the different laws of the fifty states. The proposed legislation would allow these companies to take advantage of the federal court system and its services, including nationwide service of process for subpoenas, discovery, and witness depositions. As a result, this law would make it far easier to prosecute trade secret theft cases.

The bill requires plaintiffs bringing a complaint in a civil action to "(A) describe with specificity the reason able 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."

This language may provide a limitation on the number of actions brought in federal court but may be helpful to US companies who have rogue employees or suppliers who steal their trade secrets in the United States and go to foreign countries to produce competing products.

In civil actions, courts have the authority to issue seizure orders, injunctions, and damages, including attorneys' fees and exemplary damages.

According to the drafters, the legislation is intended to protect American businesses from the theft of trade secrets. According to Senator Kohl, such a bill "ensures that companies have the most effective and efficient ways to combat trade secret theft and recoup their losses, helping them to maintain their global competitive edge." Senator Coons, another sponsor of the bill echoes that sentiment: "When a company's trade secrets are stolen, the company loses its competitive edge, and the jobs of its employees are threatened. We must do all we can to ensure that American innovators are able to protect themselves from economic espionage." This new legislation would "establish a strong and uniform civil remedy" for trade secret misappropriation, and send a "clear signal that we will not sit idly by while American companies' ideas are stolen."

Prior to introducing PATSIA, Senator Kohl previously sponsored the Economic Espionage Penalty Enhancement Act of 2011, which proposed increased penalties for persons committing economic espionage. This legislation would have increased the maximum prison sentence for those found guilty of economic espionage from 15 to 20 years. The legislation was recently amended by the Senate Judiciary Committee, and is awaiting consideration from the entire Senate.

The House has also recently taken up the issue of economic espionage. This past month, Lamar Smith, the Chairman of the House Judiciary Committee, introduced a bipartisan Espionage Penalty Act, which increases the penalties for foreign espionage to deter foreign companies from stealing American trade secrets. The bill increases prison sentences for those found guilty of economic espionage, and allows for significant fines of convicted individuals and organizations.

Federal legislation on both trade secrets and economic espionage is far from settled, and we will continue to keep you apprised of future developments.

Illinois Becomes Second State In Nation To Bar Employers From Obtaining Access To Employee Social Networking Pages

By Ronald Kramer (August 16, 2012)

On August 1, 2012, Illinois became the second state in the nation to adopt a law prohibiting employers from seeking employee or prospective employee passwords to access their non-public portions of their social networking sites.

The Illinois law, an amendment to the Right to Privacy in the Workplace Act that will become effective January 1, 2013, makes it unlawful for an employer to request or require an employee or prospective employee to provide password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking site or to demand access in any manner to an employee's or prospective employee's account or profile on a social networking website.

The law defines "social networking site" to mean an Internet-based service that allows individuals to: (a) construct a public or semi-public profile within a bounded system, created by the service; (b) create a list of other users with whom they share a connection within the system; and (c) view and navigate their list of connections and those made by others within the system. By definition, a "social networking site" does not include electronic mail.

Nothing in the new law is intended to prohibit an employer from: (a) accessing employee and prospective employee information in the public domain; (b) maintaining lawful policies governing the use of its electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use; or (c) monitoring its electronic equipment and electronic mail to the extent otherwise permitted by state and federal law.

Employers who violate the Right to Privacy in the Workplace Act are liable for actual damages plus costs, and, for willful and knowing violations, an additional $200 fine plus attorney's fees. Violations of the Act also constitute a petty offense. Last but certainly not least, employers also are prohibited from discriminating against persons who exercise their rights under the Act.

Illinois joins Maryland as the only two states with laws addressing this issue. But they will not be alone for long. The issue is currently under various stages of consideration in several other states, including Washington, California, New York, New Jersey, Minnesota and Michigan. In addition, earlier last year some members of Congress asked the Department of Justice and the EEOC to investigate whether

employer demands that job applicants turn over their social media passwords violates current federal law, discrimination statutes, or the Stored Communications Act and/or the Computer Fraud and Abuse Act.

Bills have been introduced in both the House (Social Networking Online Protection Act) and the Senate (Password Protection Act of 2012) which would prohibit employers from requiring current or prospective employees to provide their username or password to access online content.

Illinois employers, as well as Maryland employers, should take steps to comply with these new laws. In particular, employers should ensure that interviewers or other persons in the hiring process do not request passwords from applicants. Given the risks of asking for passwords, and the likelihood that many states will follow the lead of Maryland and Illinois, all employers should think twice before asking or requiring employees or applicants for social network passwords.

Proposed Social Media Legislation On California Governor's Desk

By Jessica Mendelson and Grace Chuchla (September 26, 2012)

On September 12, 2012, California Assembly Bill 1844 was enrolled and presented to Governor Brown. This bill is the counterpart to the Social Media Privacy Act (SB 1349), which was approved by the California State Senate in August 2012. AB 1844 is the work of Assemblywoman Nora Campos (D-San Jose), and seeks to prohibit employers from requiring employees to divulge their social media passwords during either the course of their employment or the hiring process. If Governor Brown signs AB 1844 into law, this would make California only the third state in the nation, after Maryland and Illinois, to limit an employer's ability to request an employee's social media passwords. We previously wrote about the new social media laws in Maryland and Illinois.

Assemblywoman Campos first proposed AB 1844 in February 2012. After many rounds of revision in both the Assembly and the Senate, the Assembly voted unanimously to accept the Senate's revisions to the bill and pass it to Governor Brown. Notably, this bill has a nearly perfect unanimous record; aside from one reading in the Senate where the vote was 29-5 in favor, it has passed with zero "nay" votes at every other reading. Governor Brown has until September 30 to either sign or veto the bill.

The core of AB 1844 "prohibit[s] an employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media." In other words, an employer may neither request nor require an employee or an applicant to divulge his or her social media passwords. However, employers are still permitted to require employees to divulge social media passwords when the information is used solely to investigate allegations of employee misconduct. Similarly, employer-issued electronic devices do not fall under the umbrella of AB 1844; the bill specifically states that it shall not be construed to preclude an employer from requiring an employee to disclose passwords or usernames for such devices.

The reaction to this bill has been strong and varied among the business and legal community. Some people believe the legislation will benefit the business community. Bradley Shear, a leading social media attorney in Washington D.C. was quoted in a Wall Street Journal legal blog, as saying that this bill is "a huge win for the business community because it may provide California businesses with a legal liability shield from plaintiffs who may allege that businesses have a legal duty to monitor their employees' personal password protected digital content." According to the article, Mr. Shear believes

this legislation could potentially save businesses millions of dollars by reducing costs related to monitoring social media accounts and cyber liability insurance premiums. Recently, both the California Chamber of Commerce and organized labor have made statements in support of the bill.

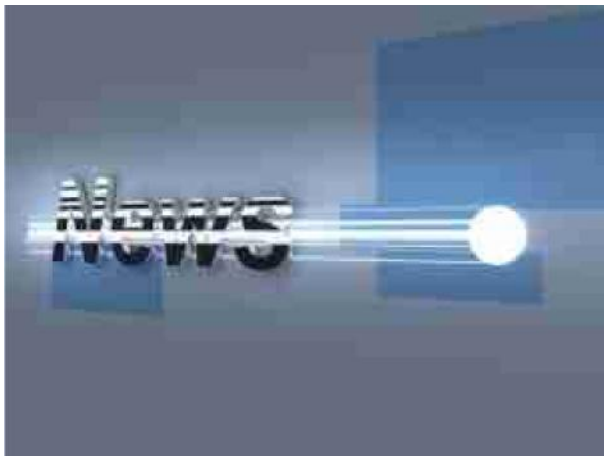
Others, however, take a different perspective. Margaret DiBianca, a Delaware attorney specializing in employment law, wrote on a Lexis Nexis blog that the new law will not benefit employers, and in fact, may hurt them. According to Ms. DiBianca, the law "limits an employer's ability to regulate its workplace, investigate wrongdoing, and, in some instances, to protect employees." She also wrote that "there has never been a successful lawsuit based on an employer's failure to monitor [its] employees' personal password protected digital content." California State Senator Ted Gaines was quoted in the Huffington Post as saying that the bill may make it more difficult for companies to identify workplace harassment. Although Gaines is concerned with "protecting people's privacy" he fears the bill will not allow employers to "address early harassment issues."

A number of business organizations and companies have come out against the bill in recent days. The Securities Industry and Financial Markets Association ("SIFMA") recently asked Governor Jerry Brown to veto this legislation. According to a recent BNA social media blog post, SIFMA recently wrote to Governor Brown, saying that while the bill may have been well-intended, it "conflicts with the duty of security firms to supervise, record, and maintain business-related communications." The Financial Industry Regulatory Authority ("FINRA") also opposes the bill. In a letter to Governor Brown, FINRA suggested California should exempt financial institutions, noting that other states, including Maryland, had discussed this type of exemption in similar bills.

We will continue to keep you apprised of future developments related to this legislation and other social media legislation across the nation.

California Governor Jerry Brown Signs New Social Media Legislation

By Robert B. Milligan (September 27, 2012)



California Governor Jerry Brown announced on Twitter, Facebook, Google+, LinkedIn and MySpace today that he has signed two bills (Senate Bill 1349 and Assembly Bill 1844) prohibiting public and private postsecondary schools and California employers from requiring applicants and employees to provide their social media account passwords.

"California pioneered the social media revolution. These laws protect Californians from unwarranted invasions of their social media accounts," Brown tweeted.

Senate Bill 1349 prohibits public and private postsecondary schools from requesting social media passwords from students.

Assembly Bill 1844 prohibits employers from requiring or requesting an employee or applicant for a job from disclosing a user name or password for the purpose of accessing personal social media.

The Securities Industry and Financial Markets Association and FINRA previously spoke out against Assembly Bill 1844.

We will provide a management alert outlining the requirements of the new law.

Failed Federal Cybersecurity Act May Emerge In Executive Order

By Misty Blair (October 1, 2012)

In August, we waved farewell to the Cybersecurity Act of 2012 (S.3414). Or, so we thought. The bill, which followed a tortured path of at least four major iterations since the introduction of its predecessor in 2010, finally hit the brick wall of Senate gridlock when a cloture vote failed to end debate. While this failure effectively killed the bill, proponents are moving forward with alternative methods to implement some of its measures, including entreaties from legislators for voluntary compliance with cybersecurity schemes, and an executive order currently being drafted by the Administration.

On a broad level, the Act was intended to create a mechanism for protecting "critical infrastructure," loosely defined as entities for which damage or unauthorized accessed could result in "the interruption of life-sustaining services," "catastrophic economic damage," or "severe degradation of national security." The Act would have created a new agency to direct an inventory of the most at-risk sectors, as well as identification of the categories and owners of critical infrastructure within each such sector.

Perhaps the most controversial portion of the Act would have authorized private entities to monitor their systems and share information with the government regarding perceived cyber threats. The Act also would have provided private entities with certain liability protections, including (1) immunity from suit arising in connection with the companies' monitoring and information-sharing activities, and (2) protection from punitive damage claims arising out of cyber attacks occurring while an entity conformed to government-approved standards.

The Act attracted opposition from the left and the right. Some raised privacy concerns based on the information sharing provisions, while others worried that government-imposed standards would unnecessarily burden businesses. Last-minute amendments designed to alleviate or remove some of these concerns did not save the bill, despite garnering the approval of some watchdog groups.

The Administration apparently is no longer waiting on Congress. Homeland Security Secretary Janet Napolitano recently confirmed that a draft executive order is nearing completion. The draft is reported to contain many provisions similar to those in the Act, including the creation of a program through which companies operating key infrastructure could elect to meet government-developed standards. However, unlike the Act, an executive order would not be able to offer these companies protections from legal actions.

Congressional members are not sitting idle, either. Last week, Senator Jay Rockefeller, Chairman of the Senate Committee on Science, Technology and Transportation, took the unusual step of writing directly to the CEO's of the nation's 500 largest corporations. He told them that he "would like to hear more... about their views on cybersecurity, without the filter of Beltway lobbyists," and he asked that they each answer a survey regarding their company's cybersecurity practices and concerns (if any) with the Act's proposed voluntary information-sharing programs.

Meanwhile, the need for some form of escalation in cybersecurity efforts is clearer than ever, as just last week sources confirmed that several major banks have been hit by some of the largest cyber attacks in history. For now, we must wait and see which avenue – legislation, executive order, senatorial supplications, or a combination – will bring this much-needed action.

What Employers Need to Know About California's New Social Media Law

By Robert Milligan, Jessica Mendelson, and Joshua Salinas (October 2, 2012)

On September 27, 2012, California Governor Jerry Brown signed two bills, AB 1844 and SB 1349, into law, making California the third state in the country – Maryland and Illinois are the others – to regulate employers' ability to demand access to employees' or prospective hires' personal social media accounts. Appropriately enough, Governor Brown made the announcement via five major social media networks: Twitter, Facebook, Google+, LinkedIn and MySpace. Brown tweeted, "California pioneered the social media revolution. These laws protect Californians from unwarranted invasions of their social media accounts."

California Assembly Bill 1844

California Assembly Bill 1844 ("AB 1844") "prohibit[s] an employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media." In other words, an employer may neither request nor require an employee or an applicant to divulge his or her personal social media account information.

This law, however, allows for employers to request the employee divulge social media "reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding." Furthermore, this law prohibits employers from threatening or taking retaliatory measures against employees that fail to comply with employer requests or demands that violate the statute.

This law "does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law." Finally, unlike many other labor and employment laws, "the Labor Commissioner. . . is not required to investigate or determine any violation of this act."

Senate Bill 1349

Senate Bill 1349 ("SB 1394") prohibits public and private postsecondary educational institutions, and their employees and representatives, from requiring students or prospective students to disclose their personal user names or passwords, or to divulge personal social media information.

SB 1394 requires private nonprofit or for-profit postsecondary educational institutions to post its social media privacy policy on the institution's Internet website.

Both AB 1844 and SB 1394 define the term "social media" broadly to include "electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."

Perspectives on the Bills

Proponents of these social media laws believe the laws will benefit the business community by providing California businesses with a shield from legal liability against plaintiffs who allege that these businesses have a legal duty to monitor their employee's social media accounts. Additionally, they argue that this legislation could potentially save businesses millions of dollars by reducing costs related to monitoring social media accounts and cyber liability insurance premiums. Recently, both the California Chamber of Commerce and organized labor have expressed their support for the law.

Opponents of the bill argue that it will hurt employers by limiting their ability to regulate the workplace and investigate misconduct. Others believe the bill may make it more difficult for companies to identify workplace harassment. Members of the financial industry, including FINRA, argued that while the bill may have been well intended, it conflicts with the duty of security firms to record, supervise, and maintain business-related communications.

Some legal commentators have also expressed their concern that the definition of "social media" is far too broad because it governs effectively all digital content and activity. In fact, Illinois excludes "e-mail" from the definition of social media in its version of the statute.

What These Laws Mean For Employers

Businesses in California should take steps to comply with these new laws which will go in effect on January 1, 2013. Employers should make sure that interviewers or other persons involved in the hiring process do not request personal user names or passwords from applicants. Additionally, employers will need to be careful with company social media accounts. While the laws only apply to personal accounts, the lack of definition of the phrase "personal" is problematic, particularly since it is not always clear who owns company social media accounts. We have previously blogged on cases concerning the ownership of "social media assets" on Twitter, Facebook, and MySpace. Some experts recommend that companies utilize ownership agreements governing the social media accounts and content created by employees on behalf of the company and that they always have the account name and password for the company social media account (certainly prior to the employee's termination). It may be helpful for employers to create clear policies on this issue to prevent future disputes.

Finally, employers should understand that the law does not constitute a complete ban on employers' access to their employees' social media sites. Employers are still permitted to require employees to divulge social media passwords when the information is used solely to investigate allegations of

employee misconduct or employee violation of applicable laws and regulations. Similarly, employer-issued electronic devices do not fall under the umbrella of AB 1844; the bill specifically states that it shall not be construed to preclude an employer from requiring an employee to disclose passwords or usernames for such devices. Notwithstanding, an employer cannot ask for access to the "personal social media" that may be contained on the employer-issued electronic device.

There may also be additional issues for employers that employ BYOD (bring your own device) policies, where the employee uses their own personal device to access company email, applications, or other data. While the employer may not technically own the device, it still has an interest in its data and information that reside on the device. The broad definition of social media and lack of definition of "personal" in the new law may lead to some unintended consequences for employers.

Update on Proposed Massachusetts Non-Compete and Trade Secret "Reform" Legislation

By Ryan Malloy and Erik Weibust (November 5, 2012)

The status of law reform in Massachusetts with respect to employee non-compete agreements remains in flux. Pending Massachusetts House Bill 2293, "An Act Relative to Noncompetition Agreements," aims to codify Massachusetts common law with respect to non-compete agreements while affording greater procedural protections to those subject to contractual restrictions on employment mobility. Since its inception, House Bill 2293 has undergone significant review, comment, and revision. We have previously blogged on the proposed legislation.

The basic requirements of House Bill 2293 remain the same as common law. Under the proposed legislation, non-compete agreements must be necessary to protect one or more of the following legitimate business interests of the employer: i) trade secrets to which the employee had access while employed; ii) confidential information that would otherwise not qualify as a trade secret; or iii) goodwill and/or customer relationships. The restrictions imposed by the non-compete agreement must be reasonable in duration, geographic reach, and scope of proscribed activities. Furthermore, the agreement must be consonant with public policy.

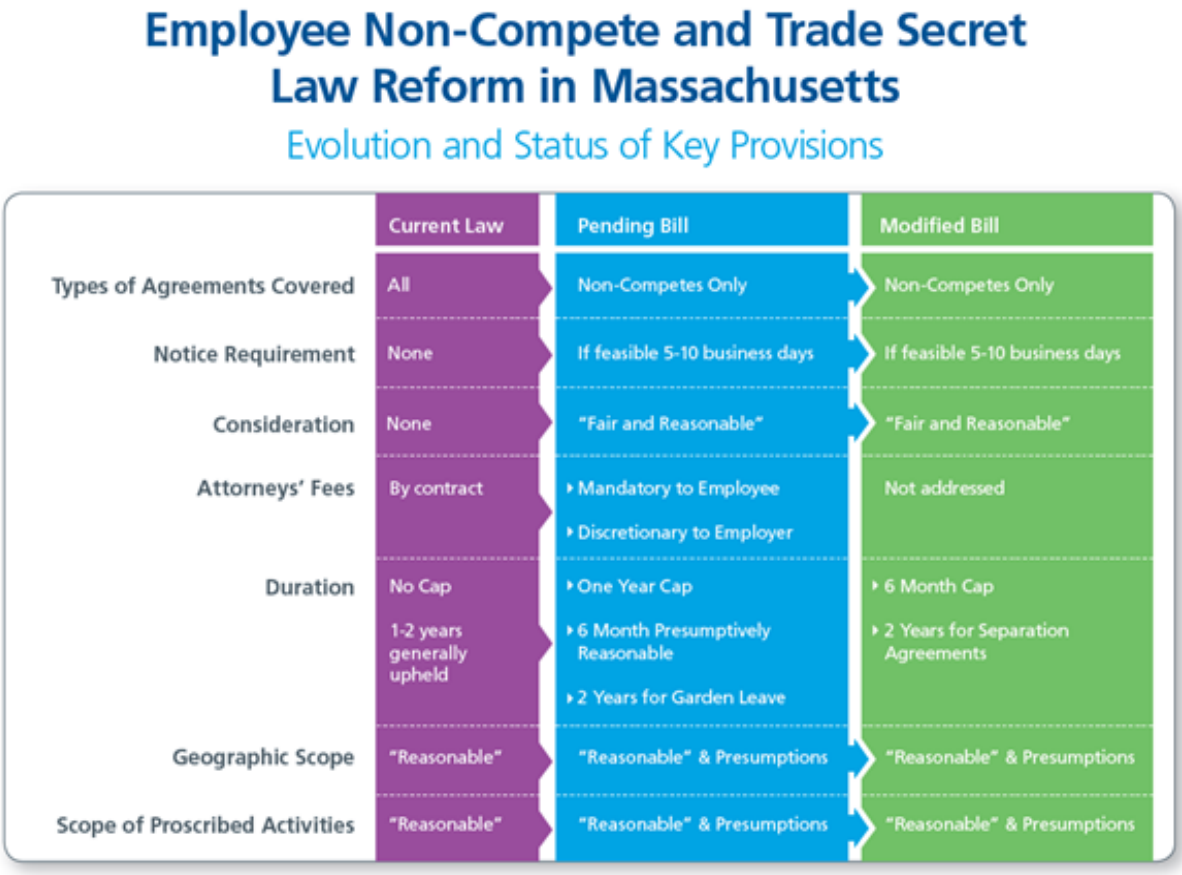
Notably, the bill applies only to non-compete agreements; it does not concern non-solicitation, anti-raid, confidentiality, or assignment of invention agreements. The most recent draft of the bill would statutorily cap the duration of non-compete agreements to 6 months (compared to a one-year cap under the current pending bill), with a cap of 2 years for separation agreements. The modified draft also omits the current pending bill's provision that would require an employer to pay the subject employee's attorney's fees if the employer acts in bad faith or is unsuccessful in enforcing the non-compete agreement because either the court does not enforce it or the court substantially reforms a material restriction in it.

Constituents have voiced both support and concern for the bill. While many object to the 6-month duration cap as insufficient to protect employer interests, others oppose the bill in its entirety, viewing any restrictive covenant legislation as a potential impetus for costly litigation and citing to economic hardship in California as a symptom of failed attempts to regulate non-compete agreements. Additional concerns include an unclear definition of "fair and reasonable consideration" and the court's ability to deny enforcement of otherwise valid contractual obligations under the bill. Still, those in support insist that the bill is necessary to achieve consistent judicial results that would protect valuable employer proprietary and confidential information.

Trading Secrets

According to Massachusetts State Representative Lori Ehrlich, co-sponsor of House Bill 2293, it is not likely that the controversial bill will be taken up again before the end of 2012. In fact, House Bill 2293 may be combined with proposed legislation that would largely adopt the Uniform Trade Secrets Act (UTSA) in Massachusetts, thereby rendering the final version of the bill unrecognizable.

Please see the instagraphic below summarizing the evolution of the proposed law reform and status of key provisions.



For more information regarding the proposed legislation, please listen to our recorded webinar concerning the latest in trade secret and non-compete legislative developments.

On Election Day, Cybersecurity Is A Part Of Candidates' Platforms

By Misty Blair (November 6, 2012)

Today, people are laser-focused on who will win the U.S. presidential election, President Barack Obama or Governor Mitt Romney. And, though cybersecurity has been a hot topic in the last year, for the time being it has been displaced from the 24-hour news cycle with political punditry, which has reached a fever pitch heard (thankfully) only once every four years.

Rest assured, however, that the "hacktivists" are not pausing from their nefarious activities to await the exit polling and election returns with the rest of us. Indeed, just yesterday, the hacker collective Anonymous marked Guy Fawkes Day ("Remember, Remember, the Fifth of November") with cyber attacks against governments and financial institutions, and demonstrations in London, Washington, D.C., and other cities worldwide.

In the spirit of this day, we may ask ourselves how the results of the election will affect the landscape of cybersecurity for the next four years. The answer is that there may not be that many differences. While President Obama would likely continue his path of addressing cybersecurity through legislation and regulations, a President Romney would likely not shy away from similar actions.

To be sure, Mr. Obama has been busy in his first term. On the cybersecurity front, he and his administration issued a Cybersecurity Policy Review with a 10-point action plan in 2009, formally established a cooperative approach by the Department of Defense and Department of Homeland Security to address cyber threats in 2010, and most recently backed the Cybersecurity Act of 2012 in the Senate. Following the failure of the CSA to gain cloture, the administration has openly discussed its plans to issue an executive order establishing a set of voluntary security standards for critical infrastructure to meet.

So, if Mr. Obama wins re-election today, should we expect the issuance of the executive order tomorrow? Not so fast. As of October 25th, Homeland Security Secretary Janet Napolitano cautioned that Mr. Obama had not yet had the opportunity to review the draft of the executive order, as he has been occupied with campaign activities. Based on his presidency thus far, however, cybersecurity appears to be a priority that will undoubtedly feature in his second term. This leads us to the next question.

If Mr. Romney wins the election today, should we expect the issuance of the executive order before the end of Mr. Obama's term? That is a strong possibility, but there is also a possibility that Mr. Romney would simply undo any such order upon taking office. The question then becomes what actions Mr. Romney would take as President.

There are indications that he would make room in his administration's agenda for the subject. He has issued a white paper stating that, within the first 100 days of his presidency, he will order "a full interagency initiative to formulate a unified national strategy to deter and defend against the growing threats of militarized cyber-attacks, cyber-terrorism, cyber-espionage, and private-sector intellectual property theft." He may champion legislation such as the Cyber Intelligence Sharing and Protection Action (CISPA), which passed through the House of Representatives earlier this year with a majority of Republican votes and a small number of Democratic votes.

While both candidates have said relatively little about cybersecurity on the campaign trail, each has at least signaled their plan to make cybersecurity a key component of his administration's agenda. And, just as with today's election, we hope tomorrow will bring more clarity with respect to this all-important defense of our nation's infrastructure.

Cybersecurity Act of 2012 Dies Again in the Senate

By Misty Blair (November 16, 2012)

You may recall that hopes were high this summer that the Cybersecurity Act of 2012 would become law, as various advocacy groups attempted to reach compromises on the most controversial portions of the bill, resulting in it being revised to address those groups' concerns. Then, on August 2nd, the Senate voted 52-46 (largely along party lines) against moving forward.

Perhaps expecting a more moderate Senate after the conclusion of the election season, Senate Majority Leader Harry Reid worked with Senators Joe Lieberman and Susan Collins to schedule another vote on the same bill for yesterday afternoon. But, Mr. Reid may have been a little too optimistic, as the Senators voted 51-47 for the same result. Now, his tenor has changed a bit: "A bill that was and is most important to national security was just killed, and that's cybersecurity," he said after the vote. "So everyone should understand cybersecurity is dead for this Congress."

For his part, Senate Minority Leader Mitch McConnell blamed Mr. Reid for the failure, pinning opposition to the bill on the lack of an open amendment process. However, Mr. McConnell left open the possibility of further debate in this session. "My expectation is that sometime in December after we have completed [consideration of other bills], we will then attempt to get an agreement on amendments to the cybersecurity bill," he said.

Meanwhile, as expected, newly re-elected President Obama is not waiting on the legislature to take action. Even in the heat of campaigning in mid-October, the President managed to sign a policy directive outlining the classified role the government and military will play in the event of cyberwarfare waged on the nation's government and private computer networks. And, though the President had little to no chance to review his administration's draft executive order prior to the election, cybersecurity is one of his administration's top priorities going into his second term, and issuance of the order could come any day.

The election is over, but partisan politics is alive and well in Washington, D.C. We should expect to see cybersecurity issues raised on a daily basis, through the end of this year and well into the next.

United States Senate Unanimously Approves the Theft of Trade Secrets Clarification Act

By Jessica Mendelson (December 3, 2012)

Last week, the United States Senate unanimously approved the Theft of Trade Secrets Clarification Act ("the TTSCA"). The TTSCA, which was co-authored by Senator Patrick Leahy of Vermont and Senator Herbert Kohl of Wisconsin, was introduced as S.3462 in order to strengthen the Economic Espionage Act of 1996 ("the EEA"). To achieve this goal, the TTSCA broadens federal law to ensure it addresses the theft of trade secrets related to a product or service used in interstate commerce.

Senators Leahy and Kohl decided to introduce the bill following the Second Circuit's decision in the case of United States v. Aleynikov. In that case, the defendant allegedly stole software code from his former employer and took the code to his next employer in another state. At trial, Aleynikov was convicted of stealing trade secrets, however, on appeal, the Second Circuit interpreted the EEA narrowly, and found that the trade secrets relating to the source code Aleynikov had taken were not related to a product "produced for. . . interstate or foreign commerce," and thus, were not entitled to protection.

The TTSCA seeks to strengthen the scope of the EEA to prevent results like the one in Aleynikov. Under the EEA, only trade secrets "related to or included in a product that is produced for or placed in interstate commerce" are protected. The Second Circuit interpreted this provision narrowly in Aleynikov, and found it only protected actual products intended to be placed in interstate commerce. Passing the TTSCA would expand the EEA to cover trade secrets "related to a product or service used in or intended for use in interstate or foreign commerce." This would mean that the EEA would protect a broader range of trade secrets, including trade secrets with a relationship to a product or service intended for interstate use. Furthermore, the TTSCA would attempt to correct the Aleynikov loophole, and would mean that using a stolen product in interstate commerce is illegal. Please also see John Marsh's informative blog on the new legislation, as well as Russell Beck's blog entry.

According to Senator Leahy, the legislation is "a straightforward fix, but an important one, as we work to ensure that American companies can protect the products they work so hard to develop, so they may continue to grow and thrive." To become law, the TTSCA must also pass in the House of Representatives. The bill was referred to the House Committee on the Judiciary on November 28, 2012. We will continue to keep you apprised of future developments as the legislative process continues.

Big Brother Can't Ask For Access To Your "Personal" Social Media Accounts Either….More Social Media Legislation Proposed In California

By Robert Milligan and Jessica Mendelson (December 11, 2012)

Recently, we blogged about the passage of California Assembly Bill 1844 ("AB 1844"), which regulates employers' ability to demand access to employees' or prospective hires' personal social media accounts. Assembly Bill 1844 was codified as section 980 of the California Labor Code. Recently, California State Assemblywoman Nora Campos has proposed an additional bill, AB 25, which amends California Labor Code section 980 to specify that it applies to private and public employers.

Although the language of AB 1844 does not specify that it only applies to private employees, Campos' office likely proposed the bill to make clear that it applies to both public and private sector employees in light of recent California court decisions. Although public employees are not specifically excluded by the statute, the term employer is not defined in California Labor Code section 980. Furthermore, recent California appellate decisions call into question whether certain Labor Code sections apply to public employers. For example, in *California Correctional Peace Officers' Association v. State of California*, 189 Cal.App.4th 849 (2010), the correctional officers union brought a class action against the state claiming penalties for alleged missed meal periods under Labor Code section 226.7. The meal period requirement in the statute did not explicitly exclude public sector employees, and the plaintiffs argued this indicated an intent to cover both public and private employees. However, the Court of Appeal held otherwise, finding that the union's arguments about alleged legislative intent were trumped by a more general presumption that the Labor Code does not apply to government employees. The Court found, "A traditional rule of statutory construction is that, absent express words to the contrary, governmental agencies are not included within the general words of a statute." The court drew upon the case of *Johnson v. Arvin–Edison Water Storage Dist.,* 174 Cal.App.4th 729 (2009) in its analysis, stating that "unless Labor Code provisions are specifically made applicable to public employers, they only apply to employers in the private sector."

As we have previously mentioned in our prior blog post about AB 1844, while California Labor Code section 980 is well-intentioned, the statutory language has some serious shortcomings. The definition of social media is overly broad, including "electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations." This could be construed to cover effectively all digital content and activity.

Furthermore, the law provides no definition of the term “personal.” While the law only applies to personal accounts, the lack of definition of the phrase “personal” is problematic, particularly since it is not always clear who owns company social media accounts. We have previously blogged on cases concerning the ownership of “social media assets” on Twitter, Facebook, and MySpace, each of which illustrate the importance of clear policies regarding the ownership of company social media accounts. Here, without clearly defining the term, the law goes too far and will likely lead to unintended consequences and perhaps misuse. Both public and private employers will need to make sure that they employ social media ownership agreements with their employees to ensure that company social media accounts stay with the company and that the employer has the username and password for the account when the employee departs.

U.S. House of Representatives Passes Theft of Trade Secrets Clarification Act

By Robert Milligan and Jessica Mendelson (December 18, 2012)

The United States House of Representatives approved the Theft of Trade Secrets Clarification Act today under a suspension of the House Rules, a process intended to expeditiously resolve non-contentious measures. The Act broadens federal law to ensure it addresses the theft of trade secrets related to a product or service used or intended to be used in interstate or foreign commerce.

Under House Rule XXVII, the Speaker of the House for the United States House of Representatives is permitted to suspend the House Rules and expeditiously resolve non-controversial measures in the last six days of a congressional session. In order to suspend the rules, two thirds of present and voting members of the House must approve the suspension, and amendments are not permitted unless they were submitted at the time the motion to suspend the rules is offered. Once a motion to suspend has been brought, the bill is debated for up to forty minutes, with twenty minutes of debate given to a representative who supports the bill, and twenty minutes given to a member who opposes the bill. A vote is then ordered, and the suspension can be issued.

This year, the suspension list included S.3642, the Theft of Trade Secrets Clarification Act of 2012, which recently passed in the Senate. The Act is intended to strengthen the scope of the Economic Espionage Act to prevent results like the Second Circuit's decision in *United States v. Aleynikov*, which we previously discussed. Under the Economic Espionage Act, only trade secrets "related to or included in a product that is produced for or placed in interstate commerce" are protected. The Second Circuit interpreted this provision narrowly in Aleynikov, and found it only protected actual products placed in interstate or foreign commerce. The court would not apply the law because the trade secret failed to satisfy the interstate or foreign commerce requirement. The passage of the Theft of Trade Secrets Clarification Act expands the Economic Espionage Act to cover trade secrets "related to a product or service used in *or intended for use in interstate or foreign commerce*." (emphasis added). This means that the Economic Espionage Act will now protect a broader range of trade secrets, including trade secrets with a relationship to a product or service intended for interstate or foreign commerce. Furthermore, the Theft of Trade Secrets Clarification Act attempts to correct the Aleynikov loophole. The bill moved under suspension of House Rules on Tuesday, December 18, and passed 388-4. It will now go directly to the White House for President Obama's signature. We will continue to keep you posted on the bill's progress.

President Obama Signs Trade Secrets Clarification Act and House of Representatives Considers Enhancing Economic Espionage Act Penalties

By Robert Milligan (December 31, 2012)

On December 28, 2012, President Obama signed into law the Trade Secrets Clarification Act to ensure that the Economic Espionage Act will cover trade secret violations for products or services used or "intended for use" in interstate commerce or foreign commerce.

The Senate passed the legislation in November and the House of Representatives approved the legislation earlier this month.

The legislation directly responds to the Second Circuit's decision in *U.S. v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), which overturned a jury verdict finding the defendant violated 18 U.S.C. 1832(a) of the Economic Espionage Act by stealing computer code from his employer. The court held that the statute did not apply because the computer code failed to satisfy the interstate or foreign commerce requirement.

The amended Section 1832(a) now applies to a trade secret "that is related to a product or service used in *or intended for use in interstate or foreign commerce*, to the economic benefit of anyone other than the owner thereof." (emphasis added).

The House of Representatives is scheduled to vote today on a bill enhancing the penalties for violations of the Economic Espionage Act. Under the bill, the upper limit of penalties for individual offenses at Section 1831(a) would be increased from $500,000 to $5,000,000; the upper limit for corporate offenses at Section 1831(b) would be increased from $10,000,000 to the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

The Senate previously approved the bill. We will keep you updated on the bill's status.

Index

Author

Trading Secrets

Trading Secrets

State

Trading Secrets

Trading Secrets

Cases

Trading Secrets

Trading Secrets

Trading Secrets

Trading Secrets

Court

Trading Secrets

Trading Secrets

Trading Secrets

Acknowledgments:

Special thanks to Bridget Rabb, Grace Chuchla, and Josh Salinas for their work in putting together this year in review.

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.