SEYFARTH SHAW

2016
YEAR IN REVIEW

Trading Secrets

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

Trading Secrets

Dear Clients and Friends,

2016 was another year of great change and accolades for our dedicated Trade Secrets, Non-Compete, and Computer Fraud group. In particular, we were again ranked nationally as the leading U.S. Firm in Trade Secrets by *The Legal 500*, an independent guide to lawyers in the U.S. In the guide, clients said Seyfarth is "well worth it" and they "could not be happier" with the service provided by our team. Since 2007, the blog has continued to grow in both readership and postings. Content from Trading Secrets has appeared on news sources such as JD Supra, Mondaq, Lexology, Law360, IP Magazine, SHRM, 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 the 2016 Year in Review, which compiles our significant blog posts from 2016 and highlights our blog's authors. For a general overview of 2016, we again direct you to our Top 2016 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2016 Trade Secrets Webinar Series - Year in Review blog entry, which provide a summary of key cases and legislative developments in 2016, as well as practical advice on maintaining trade secret protections as well as other pertinent topics in this area.

As the specific blog entries 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 continue to provide an informative resources page, special guest authors, cutting-edge infographics, and access to our well-received Trade Secret Webinar Series, archived from 2011 to the present. In 2016, we offered audio podcasts, guest authors, a feature on international law, and provided an additional enhanced Resources page on the blog. We also continued our special feature tracking the proposed federal trade secret legislation. In 2017, we will also offer additional content on recent developments in privacy, social media, Defend Trade Secrets Act decisions, and cybersecurity in our blog coverage.

In addition to our blog, Seyfarth's dedicated Trade Secrets, Computer Fraud & Non-Competes Practice Group hosts a popular series of webinars, which address significant issues facing clients today in this important and ever-changing area of law. In 2016, we hosted eleven webinars, which are listed in this Review. For those who missed any of the programs in the 2016 webinar series, the webinars are available on the blog or CD upon request.

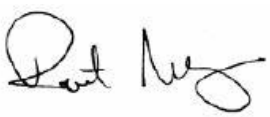
We are kicking-off the 2017 webinar series with a program entitled, "2016 National Year in Review: What You Need to Know About Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law." More information on our upcoming 2017 webinars is available in the program listing contained in this Review. Our highly successful blog and webinar series further demonstrate that Seyfarth Shaw's national Trade Secret, 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 and is recognized as a *The Legal 500* leading firm.

Thank you for your continued support.

Michael Wexler

Practice Group Chair

Robert Milligan



Practice Group Co-Chair and Blog Editor

Trading Secrets

Table of Contents

Trading Secrets

2016 Trade Secrets Webinar Series

- 2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law
  January 29, 2016

- Data Security & Trade Secret Protection for Lawyers
  February 25, 2016

- New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive
  March 29, 2016

- Protecting Confidential Information and Client Relationships in the Financial Services Industry
  April 29, 2016

- Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?
  May 10, 2016

- The Defend Trade Secrets Act: What Employers Should Know Now
  May 16, 2016

- Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements
  June 21, 2016

- International Non-Compete Law Update
  July 28, 2016

- The Intersection of Trade Secrets Violations and the Criminal Law
  October 4, 2016

- Trade Secret Audits: You Can't Protect What You Don't Know You Have
  November 16, 2016

- Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches
  December 13, 2016

2017 Trade Secrets Webinar Lineup

- 2016 National Year in Review: What You Need to Know About the Recent Cases/ Developments in Trade Secrets, Non-Compete, and Computer Fraud
- Protecting Your Trade Secrets in the Pharmaceutical Industry
- Update on the Defend Trade Secrets Act
- Financial Services and Trade Secret/Non-Compete Issues
- Trade Secret Protection/Audit
- Open Source Software as a Security Risk

Our Authors

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

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

Robert Milligan is the Editor of the blog and Co-Chair of the national Trade Secrets, Computer Fraud, and Non-Competes Practice Group. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation and other intellectual property theft, real estate litigation, insurance bad faith, invasion of privacy, products liability, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower cases, bankruptcy and other business torts. Mr. Milligan has represented clients in state and federal courts in complex commercial litigation and employment litigation. His experience includes trials, binding arbitrations and administrative hearings, mediations, as well as appellate proceedings.

Amy Abeloff is an associate in the Los Angeles-Century City office and is located within the litigation department. Ms. Abeloff works on various aspects of intellectual property law including trademark and copyright prosecution, enforcement, and litigation, as well as trade secrets litigation.

Trading Secrets

Kristine Argentine is an associate for the Litigation Department in the Chicago office of Seyfarth Shaw LLP. Ms. Argentine's practices focuses on complex commercial litigation, including cases involving restrictive covenants, misappropriation of trade secrets and intellectual property, unfair competition, contract disputes, consumer class action defense, and business torts.

Scott Atkinson is a Counsel in the San Francisco office of Seyfarth Shaw LLP. Mr. Atkinson is a member of the firm's Labor & Employment Department and the Trade Secrets, Computer Fraud & Non-Competes practice group. Mr. Atkinson is an experienced litigator and counselor who focuses his practice on helping employers efficiently resolve problems and implement practices that help avoid those problems in the first place.

Eric Barton is a counsel in the Litigation Department of Seyfarth Shaw LLP. For more than a decade, Mr. Barton has represented, advocated for, and advised clients in all forms of dispute resolution, including serving as lead trial counsel in numerous jury trials and arbitration proceedings throughout the Southeast. Recognizing that trial is typically not the ultimate goal for a client, Mr. Barton devotes a significant portion of his practice to advising and counseling clients on issues related to pre-trial resolution and avoidance of business disputes.

Christopher Baxter is a staff attorney in the Boston office and is located within the litigation department. Mr. Baxter is a registered patent attorney whose practice includes advising clients on various aspects of intellectual property law. Mr. Baxter has experience in trademark and patent prosecution as well as patent litigation. Mr. Baxter has also drafted and prosecuted numerous patent applications regarding technologies ranging from business methods to the chemical and mechanical arts. He also has experience in technology licensing.

Justin Beyer is a partner 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. Mr. Beyer has represented plaintiffs and defendants in the agricultural, banking, construction, food processing equipment manufacturing, general manufacturing, healthcare, pharmaceutical, real estate development, and transportation industries.

Trading Secrets

Wayne Bond is a partner in the Litigation Department in Seyfarth Shaw's Atlanta office. Mr. Bond handles complex commercial litigation and class action cases in state and federal courts across the country, including breach of contract, commercial transactions, real estate, construction, corporate shareholder and partnership disputes, product liability, false advertising, lender liability, professional malpractice, corporate liability, personal injury, professional liability, clinical trials, employment disputes, government investigations, bankruptcy, white collar criminal defense, fraud, business torts, and administrative hearings.

Andrew S. Boutros is the National Co-Chair of Seyfarth Shaw LLP's White Collar, Internal Investigations, and False Claims Team. He is a distinguished trial attorney, accomplished litigator, Foreign Corrupt Practices Act (FCPA) pioneer, Lecturer in Law at the University of Chicago Law School, voting Member of the ABA Criminal Justice Section Council, Co-Founder and National Co-Chair of the ABA's Global Anti-Corruption Committee, board member to various professional and legal organizations, and former law clerk on the Sixth Circuit Court of Appeals. A decorated former federal financial fraud prosecutor, Mr. Boutros now represents clients in their most sensitive and important white collar matters; internal investigations, including those arising under the FCPA and other anti-corruption laws; and complex litigations. He also provides strategic counseling and advice to clients in a variety of industries and conducts comprehensive compliance audits, including in the areas of corporate social responsibility, country of origin matters, and supply chain integrity. Mr. Boutros is resident in the firm's Chicago and Washington, D.C. offices.

Matthew Christoff is an associate in the Commercial Litigation Practice Group of Seyfarth Shaw LLP. He focuses his practice on issues involving eDiscovery, including electronic document preservation, production, review, and spoliation. Mr. Christoff has a technical background that has included computer support, network administration, and programming.

Jesse Coleman is a partner in the Litigation Department of Seyfarth Shaw LLP. His practice encompasses various types of civil litigation facing the health care industry, energy industry, and related industries. This includes representing managed care organizations, insurance companies, hospital systems, and physicians in matters involving contract disputes, peer review and credentialing proceedings, Medicaid bid protests, antitrust claims, defamation claims, EMTALA claims, ERISA claims, professional liability claims, and regulatory matters before state and federal agencies. He has also represented and counseled both health care and energy-sector clients in numerous trade secret disputes.

Trading Secrets

Michael Cross is an associate in Seyfarth Shaw's Labor & Employment department based in the Sacramento office. His practice focuses primarily on litigation surrounding companies' intellectual property rights, including the protection of trade secrets and the enforcement of noncompetition agreements. He also defends individuals and companies who have been accused of violating covenants or stealing, using, or disclosing confidential information.

Andrew del Junco is an associate in the Commercial Litigation Department of Seyfarth Shaw LLP's Houston office. His practice focuses on high-stakes commercial litigation matters, including contract disputes, trade secrets and non-competes, business torts, and antitrust issues.

Ada Dolph is a partner in the Labor & Employment Department of Seyfarth Shaw LLP. She represents clients in a wide range of labor and employment matters, with an emphasis on employment discrimination, ERISA and whistleblower claims. She is a member of the Firm's ERISA & Employee Benefits Practice Group, as well as its Whistleblower and Health Care Fraud and Provider Billing Litigation Teams.

Robert A. Fisher is a partner in the Labor & Employment Department of Seyfarth Shaw LLP's Boston office. He represents employers in all aspects of labor and employment law, with significant experience handling traditional labor matters on behalf of employers in a wide variety of industries, including higher education, hospitality, technology, and construction. He regularly represents employers before the National Labor Relations Board in representation petitions and unfair labor practices proceedings. Mr. Fisher also advises clients on responding to union organizing and corporate campaigns, collective bargaining and on labor issues related to corporate transactions. He has tried dozens of labor arbitrations before the American Arbitration Association and other ADR organizations.

Justine Giuliani is an associate in the Melbourne office of Seyfarth Shaw Australia. She is a member of the firm's International Employment Law practice. Justine has experience across all aspects of employment and industrial relations law. She advises clients in relation to employment arrangements and industrial instruments, workplace policies, executive employment issues, termination of employment, enterprise bargaining, industrial action and workforce restructures.

Trading Secrets

Lauren Gregory is an associate in the Litigation Department of Seyfarth Shaw LLP. Ms. Gregory's practice centers around the resolution of complex commercial disputes, including general business and contract disputes, unfair competition, misappropriation of trade secrets and other confidential information, and trademark, trade dress, and copyright infringement.

Karla Grossenbacher is a partner in Seyfarth Shaw's Washington, D.C. office concentrating in labor and employment law. She is Chair of the Washington, D.C. Labor & Employment Practice Group. Ms. Grossenbacher serves on the firm's national Labor and Employment Steering Committee, as well as the Steering Committee of the Firm's Global Privacy and Security team. She also heads the Firm's National Workplace Privacy team.

Daniel Hart is a partner 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.

Ming Henderson is a partner in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP's London office. She is qualified in both France and the UK. Before joining the firm, Ms. Henderson worked as an in-house employment counsel for a global software and hardware company covering Europe Middle-East and Africa (EMEA). She was also previously head of the EMEA Employment Law Practice for a global financial institution in the UK.

Dominic Hodson is a partner in the San Francisco Office of Seyfarth Shaw LLP. Mr. Hodson specializes in the firm's International Employment Law practice and has devoted his career to the development of this niche practice. He works regularly and closely with some of the world's best known brands to assist them with all of their labor and employment needs outside of the US and guide them to compliant and commercially-practical resolutions to those needs. Mr. Hodson's practice covers each region of the globe and encompasses not only the day-to-day issues which global employers face in managing their workforce in specific countries, but also the complex and detailed issues arising from the implementation and management of multi-jurisdictional HR projects. He has a particular focus on the labor and employment aspects of international business transactions.

Trading Secrets

Cassie Howman-Giles is a senior associate in Seyfarth Shaw Australia's International Labour & Employment practice in Sydney. She has more than 7 years of experience advising clients in respect of employment and workplace relations law in both Australia and the UK.

Scott Humphrey is a partner in the Trade Secrets, Computer Fraud & Non-Competes Group. He serves on the Group's National Steering Committee and has successfully prosecuted and defended trade secrets and restrictive covenant cases throughout the United States. In doing so, Scott has successfully obtained and defeated temporary restraining orders, preliminary injunctions and permanent injunctions involving trade secret and restrictive covenant matters for clients in the technology, securities and financial services, transportation, electronics, software, insurance, healthcare, consumer products, and manufacturing industries.

Marc Jacobs is a senior counsel in the Chicago office in the Labor & Employment Department. Mr. Jacobs regularly helps employers insulate themselves against liability and claims by counseling them through employment-related problems and situations; analyzing employers' practices and procedures; negotiating and preparing employment, restrictive covenant, confidential information and severance agreements; writing employment policies and manuals; and conducting interactive supervisor training programs for clients. Marc represents client in numerous industries, including aviation, hospitality, parking services, manufacturing, pharmaceuticals, specialty chemicals, and professional services.

Salomon Laguerre is an associate in the Labor & Employment Department of Seyfarth Shaw LLP's Atlanta office. Mr. Laguerre represents many of the nation's leading companies in employment related matters in both state and federal courts. His practice includes counseling and representing clients on a wide range of employment issues including discrimination, wage and hour, wrongful termination, as well as disputes arising out of non-compete agreements. Mr. Laguerre represents clients in proceedings before the Equal Employment Opportunity Commission, and regularly handles employment-related transactional matters including drafting and analyzing employment agreements, separation agreements, and company policies.

Ashley Laken is an associate in the Chicago office and a member of the firm's Labor & Employment department. Ms. Laken's practice focuses on labor relations law as well as defending employers against age, race, national origin, sex, and disability discrimination claims. Ms. Laken represents clients in many industries, including hospitality, publishing, broadcast, media, manufacturing, retail, and transportation.

Trading Secrets

Wan Li is a partner in the Shanghai office of Seyfarth Shaw LLP. He has over 20 years of experience in China-related matters advising a diverse range of clients in employment, mergers and acquisitions (corporate and cross-border), private equity and corporate matters including restructuring. Wan Li has a broad practice focused on foreign direct investments into China and representing Chinese companies in relation to multinational transactions including acquisition of equity and assets of telecommunication, internet, high-tech, energy and resources, medicine and dairy products companies.

Richard Lutkus is a partner in the San Francisco office of Seyfarth Shaw LLP. His practice is dedicated to complex information governance issues including information security, eDiscovery consulting and litigation response, digital forensics, data breach prevention and response, cyber-stalking mitigation, and information technology related policies and practices.

Kevin Mahoney is an associate in the Litigation Department of Seyfarth Shaw LLP's Chicago office. His practice focuses on complex commercial litigation, including cases involving restrictive covenants, misappropriation of trade secrets and intellectual property, unfair competition, contract disputes, and business torts. He has represented clients at each phase of litigation, including alternative dispute resolution, emergency injunctions, jury and bench trials, and appeals in multiple jurisdictions in the United States.

Andrew Masak is an attorney in the Atlanta office of Seyfarth Shaw LLP and is a member of the firm's Labor & Employment department. Mr. Masak represents employers in all aspects of labor and employment issues, including the National Labor Relations Act, arbitration, collective bargaining, discrimination, workplace harassment and retaliation claims under Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, and other state and local statutes, as well as various other common law torts and employment contractual disputes.

Georgina McAdam is an associate in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP, based in the firm's London office. Her focus is on all areas of employment law, both contentious and non-contentious. Prior to joining Seyfarth Shaw, Ms. McAdam worked in one of London's top-tier employment departments.

Trading Secrets

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's commercial litigation practice focuses on complex matters involving breach of contract; insurance bad faith; franchise, dealer and distribution disputes; unfair competition; business torts; false advertising; discriminatory pricing; and anti-trust. He prosecutes and defends trade secret misappropriation claims, including obtaining associated expedited discovery and relief. Mr. McNairy's employment litigation practice focuses on restrictions on competition and freedom of employment (non-compete and non-solicitation agreements), ERISA, discrimination, harassment, wrongful termination, and wage and hour class actions brought under state and federal law.

Alex Meier works in Seyfarth's Labor and Employment Group. His practice includes the full array of federal remedial rights, non-compete and trade secret litigation, and traditional labor law.

Dawn Mertineit is an associate in the Litigation Department of Seyfarth Shaw LLP. Ms. Mertineit specializes in non-compete and trade secrets litigation, representing both plaintiffs and defendants in state and federal courts, from pre-litigation counseling through to judgment or settlement, as well as advising her clients on their non-compete agreements and other restrictive covenants. Ms. Mertineit also has experience litigating a variety of employment actions, Computer Fraud and Abuse Act claims, partnership disputes, banking and finance matters, breach of contract suits, product and premises liability actions, real estate disputes, construction claims, and various tort actions.

Marcus Mintz is a partner in the Chicago office of Seyfarth Shaw LLP. Mr. Mintz's practice focuses on complex commercial litigation, including cases involving post-merger disputes, misappropriation of trade secrets and intellectual property, equity rights, and business tort claims. Mr. Mintz has represented a wide range of clients, including medical device manufacturers, clinical research organizations, automotive manufacturers, defense contractors, construction companies, insurance companies, and a variety of private business owners. Mr. Mintz has represented and counseled clients through all phases and forms of litigation, including pre-litigation resolution, alternative dispute resolution, administrative law proceedings, emergency injunctions, jury trials, and appeals.

Kristen Peters is a senior associate in the Labor & Employment Department in the Los Angeles office of Seyfarth Shaw, LLP. Ms. Peters represents employers in all aspects of labor and employment litigation, including sexual harassment, discrimination, wrongful termination, retaliation, wage and hour, and class action matters. Ms. Peters is also a member of the firm's Health Care Fraud and Provider Billing Litigation Specialty Team.

Trading Secrets

Christopher Robertson is Co-Chair of the National Whistleblower Team and a member of the Complex Litigation, Capital Markets and Investment Management practice areas in the Boston Office of Seyfarth Shaw LLP. His areas of focus include complex commercial and financial litigation, securities litigation, consumer fraud litigation, regulatory compliance, corporate governance, and internal investigations.

Eddy Salcedo is an experienced first-chair trial lawyer and is currently in the New York office of Seyfarth Shaw LLP. He has successfully represented a wide range of clients in trade secret, enforcement of non-competition agreements, partnership disputes, and trademark infringement litigations. He has also served as trial counsel for parties in construction and real estate development disputes, contract disputes, and general commercial and civil litigation.

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. Mr. Salinas' experience includes the prosecution and defense of trade secret misappropriation and unfair competition claims.

John Skelton is a partner in the Litigation Department of Seyfarth Shaw LLP. He is an experienced trial lawyer having tried cases and appeared before a variety of state and federal courts and administrative agencies. In addition to a diverse commercial litigation and trial practice, Mr. Skelton has successfully defended numerous manufacturers and franchise clients in a variety of matters, including terminations, challenges to the establishment and relocation of dealerships and other outlets, the enforcement of operating standards, and "mass" and class actions.

Andrew Stark is an associate in the Litigation Department of Seyfarth Shaw LLP. His practice covers a broad range of complex commercial litigation, primarily representing corporations and their directors and officers in all stages of litigation, including appeals. Mr. Stark is a member of the Commercial Litigation, Consumer Financial Services Litigation, Distribution and Franchise Litigation and Counseling, and Securities and Financial Litigation groups within the Litigation Department.

Trading Secrets

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

Robert Szyba is an associate in the Labor & Employment department in the New York office of Seyfarth Shaw LLP. Mr. Szyba's practice focuses on litigating employment law matters before state and federal courts, both trial and appellate levels, as well as federal and state administrative agencies, including the Equal Employment Opportunity Commission, Department of Labor, New Jersey Division on Civil Rights, New Jersey Office of Administrative Law, and New York State Division of Human Rights. He has litigated claims involving restrictive covenants, such as non-compete agreements, non-solicitation agreements, confidentiality agreements, and misappropriation of trade secrets. In addition to his litigation practice, Mr. Szyba regularly advises clients about pre-litigation strategy and litigation avoidance, employment contracts, employment policies and procedures, privacy considerations, and minimizing exposure to liability.

Peter Talibart is a partner in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP and leads the firm's London office. He is qualified in both Canada and the UK. Mr. Talibart is employment counsel to major multinationals and financial institutions on strategic cross-border employment issues. His expertise is in all aspects of UK and cross-border employment law, in particular corporate restructuring, mergers and acquisitions, corporate governance (employment), financial services compliance and ethical issues.

Erik von Zeipel is a partner in Seyfarth Shaw's Los Angeles office. A member of the firm's Litigation department, Erik maintains a broad litigation and counseling practice representing businesses in a variety of areas. Erik has significant experience in complex litigation, including class actions, trade secrets, breach of contract, unfair competition, construction, and real estate lawsuits.

Erik Weibust is a partner in the Litigation Department of Seyfarth Shaw LLP, and is a member of the Securities & Financial Litigation and Trade Secrets, Computer Fraud & Non-Competes practice groups, and an active member of the firm's national Whistleblower Team. Mr. Weibust regularly represents clients in disputes involving trade secrets and restrictive covenants, shareholder disputes, consumer class actions, and claims of unfair competition, fraud, and commercial disparagement, among other matters.

Trading Secrets

Dallin Wilson is an associate in Seyfarth Shaw's Boston office and is a member of the Commercial Litigation, Construction, Consumer Financial Services Litigation, and Securities and Financial Litigation practice groups. Mr. Wilson represents clients in all manner of litigation matters in state and federal court. His clients include banking institutions, supermarkets, contractors, and privately held corporations. Mr. Wilson also has experience representing healthcare entities in government investigations related to violations of HIPAA, Anti-Kickback Statutes, and other state and federal regulations.

Rebecca Woods is a partner in the Atlanta office of Seyfarth Shaw LLP and co-chair of the firm's Commercial Litigation practice group. She is a seasoned litigator with trial experience. She also counsels clients on litigation avoidance strategies. As a commercial litigator at heart, her subject matter experience is broad, and includes trade secrets, insurance coverage, business torts, construction litigation and real estate matters

James Yu is senior counsel 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. He has regularly handled and tried a diverse range of matters, including complex contract disputes, trade secret misappropriation and business tort cases, products liability and toxic tort defense, and several actions defending servicers of commercial mortgage loans involving multi-level debt structures.

Candice Zee is a partner in the Los Angeles office of Seyfarth Shaw LLP. As a member of the Labor & Employment Department and Single Plaintiff Litigation and Wage and Hour Practice Groups, she has substantial experience in defending employers against class action and single-plaintiff claims for alleged wage and hour violations, discrimination, harassment, retaliation, and violation of public policy, as well as workplace torts, including defamation, emotional distress, and interference with contractual relations. Ms. Zee has taken and defended numerous depositions and conducted several factual investigations. She frequently appears and argues on behalf of clients at state and federal courts. She also has extensive trial experience and has litigated multiple trials.

Trading Secrets

2016 Summary Posts

- Top Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2016
  By Robert B. Milligan and Daniel Joshua Salinas (January 27th, 2017)

- 2016 Trade Secrets Webinar Series Year In Review Released
  By Robert B. Milligan (January 5th, 2017)

Trade Secrets Legislation

- Senate Judiciary Committee to Hold Meeting About Passage of the DTSA
  By Amy Abeloff and Robert B. Milligan (January 21st, 2016)

- Senate Judiciary Committee Votes in Favor of Passage of an Amended Defend Trade Secrets Act
  By Amy Abeloff and Robert B. Milligan (January 28th, 2016)

- Senate Judiciary Committee Issues Report in Support of Defend Trade Secrets Act
  By Amy Abeloff and Robert B. Milligan (March 22nd, 2016)

- U.S. Senate Passes Bill Creating A Civil Cause of Action in Federal Court for Trade Secret Misappropriation
  By Robert B. Milligan (April 5th, 2016)

- What Does the Passage of the Defend Trade Secrets Act Mean for Your Business?
  By Amy Abeloff and Robert B. Milligan (April 27th, 2016)

- President Obama to Sign Defend Trade Secrets Act into Law
  By Robert B. Milligan (May 11th, 2016)

- President Obama Signs the Defend Trade Secrets Act: Tips for Navigating the New Law
  By Robert B. Milligan, Daniel P. Hart, and Amy Abeloff (May 11th, 2016)

- Webinar Recap! The Defend Trade Secrets Act: What Employers Should Know Now
  By Robert B. Milligan, Daniel P. Hart, and Amy Abeloff (June 16th, 2016)

- Federal Court Rejects Defend Trade Secrets Act Whistleblower Immunity Defense on a Motion to Dismiss and Orders Employee to Return Stolen Trade Secrets
  By Erik Weibust, Andrew Stark, and Robert A. Fisher (December 19th, 2016)

Trading Secrets

Trade Secrets

- Charities Take Note: Ninth Circuit Reaffirms CA Attorney General's Entitlement to Sensitive Donor List
  By Seyfarth Shaw LLP (January 15th, 2016)

- Oil-And-Gas Services Companies Argue Over Trial Court's Authority to Exclude Corporate Representatives Under New Texas Trade Secret Law
  By Jesse M. Coleman (January 19th, 2016)

- Webinar Recap! Data Security & Trade Secret Protection for Lawyers
  By Richard Lutkus and James Yu (March 8th, 2016)

- Webinar Recap! New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive
  By Robert B. Milligan, Justin K. Beyer, and Daniel P. Hart (April 11th, 2016)

- Webinar Recap: Protecting Confidential Information and Client Relationships in the Financial Services Industry
  By J. Scott Humphrey, Marcus Mintz, and Kristine Argentine (May 5th, 2016)

- Drones & Trade Secrets – How Low Can They Go?
  By Wayne Bond (May 9th, 2016)

- Texas Supreme Court: Company Representative May Be Excluded from Trade Secret Hearing
  By Jesse M. Coleman (May 31st, 2016)

- When Stealing in Baseball Can Land You in Jail: Computer Fraud Sentencing Announced in MLB Case
  By Erik Weibust (July 20th, 2016)

- Federal Precedents Under the DTSA Have Arrived
  By Kevin Mahoney (August 1st, 2016)

- We Traced The Trade Secret Leak … It's Coming From Inside The Business
  By James D. McNairy and Michael Cross (August 3rd, 2016)

- What To Do About Employee Thieves—Catch Them If You Can!
  By Kristen Peters (August 10th, 2016)

- Texas Appellate Court Affirms Injunctive Relief and $2.8 Million Award in Attorney's Fees Against Former Employee in Trade Secret Misappropriation Case
  By Jesse M. Coleman (September 1st, 2016)

- You get to write the script for this story…
  By Michael Tamvakologos and Justine Giuliani (October 26th, 2016)

- Webinar Recap! The Intersection of Trade Secrets Violations and the Criminal Law
  By Andrew S. Boutros, Katherine Perrelli, and Michael Wexler (October 28th, 2016)

Trading Secrets

- CFTC Proposes New Rule Allowing it to Obtain Trading Firm's Trade Secrets Without Due Process
  By Erik Weibust and Andrew Stark (November 10th, 2016)

- Webinar Recap! Trade Secret Audits: You Can't Protect What You Don't Know You Have
  By Robert B. Milligan, Eric Barton, and Scott E. Atkinson (November 17th, 2016)

- Webinar Recap! Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches
  By James D. McNairy and Justin K. Beyer (December 27th, 2016)

- Challenge to ITC's Extraterritorial Authority over Trade Secret Dispute Launched by Chinese Corporation
  By Marcus Mintz (December 28th, 2016)

Computer Fraud and Abuse Act

- Ninth Circuit Poised to Address the "Without Authorization" Debate under the Computer Fraud and Abuse Act Again
  By Amy Abeloff (January 13th, 2016)

- Computer Fraud and Abuse Act Not Violated Unless Plaintiff Shows Defendant Had Intent To Defraud
  By Paul E. Freehling (February 9th, 2016)

- Recent Decision Highlights Important Pleading Requirements for Computer Fraud and Abuse Act Claims
  By Eric Barton (February 18th, 2016)

- Federal Court Rejects Employer's Trade Secret and Computer Fraud and Abuse Act Claims
  By Paul E. Freehling (February 29th, 2016)

- Computer Fraud and Abuse Act Ruling: Did the Ninth Circuit Just Criminalize Password Sharing?
  By Scott E. Atkinson (July 13th, 2016)

- Facebook, Inc. v. Power Ventures, Inc.: Shotgun-Toting Borrowers of Jewelry From Bank Safe Deposit Boxes and the CFAA. Wait. What?
  By James D. McNairy (July 19th, 2016)

- What Underlying Facts are Required to Assert a Valid CFAA Claim Based on "Exceeds Authorized Access" in Georgia?
  By Eric Barton (November 7th, 2016)

Trading Secrets

Non-Competes & Restrictive Covenants

- Five Easy Tips for Improving Your Company's Non-Compete and Confidentiality Agreements and Related Practices Now
  By Robert B. Milligan (February 10th, 2016)

- Webinar Recap! 2015 National Trade Secret, Non-Compete and Computer Fraud Law Year in Review
  By Robert B. Milligan, Jesse M. Coleman, and Daniel Joshua Salinas (February 17th, 2016)

- Ex-Employee Hit With Six-Figure Judgment For Violating His Non-Competition Agreement By Helping His Son Compete
  By Paul E. Freehling (March 10th, 2016)

- Extensive Training Of Ex-Employee By Former Employer Not Enough For Injunction Against Competition
  By Paul E. Freehling (March 21st, 2016)

- Leave No E-mail Unturned in Trade Secret and Non-Compete Cases
  By Eric Barton (March 30th, 2016)

- New Utah Law Limits Restrictive Covenants to a One-Year Period
  By Arielle Eisenberg (March 31st, 2016)

- North Carolina Courts Are Forbidden To "Blue Pencil" An Unenforceable Non-Compete
  By Paul E. Freehling (April 4th, 2016)

- You Can't Put Lipstick On This Pig: Beauty Company's Non-Compete Deemed Unenforceable
  By Erik Weibust and Andrew Stark (April 7th, 2016)

- Court Won't Enjoin Physician Who Breached Non-Compete Covenant And Consented To Injunction
  By Paul E. Freehling (April 8th, 2016)

- California Court Gives Two Thumbs Down and Voids Non-Compete in Actor's Agreement
  By Robert B. Milligan, Daniel Joshua Salinas, and Amy Abeloff (April 20th, 2016)

- U.S. Treasury Department Suggests That Non-Compete Reform is Necessary
  By Erik Weibust and Andrew Stark (April 28th, 2016)

- Despite Evidence That Ex-Employee Violated Customer Non-Solicitation Covenant, Injunction Denied Because No "Irreparable" Harm
  By Paul E. Freehling (May 6th, 2016)

- White House Issues A Call To Arms With Respect To Non-Competes
  By Erik Weibust and Andrew Stark (May 6th, 2016)

- No Microscope Needed to See Why This Non-Compete Is Unenforceable
  By James D. McNairy and Michael Cross (May 10th, 2016)

Trading Secrets

- Georgia's Restrictive Covenants Act Turns Five Years Old: Assessing the Impact of Georgia's Law Five Years On
  By Daniel P. Hart, Bob Stevens, and Alex Meier (May 12th, 2016)

- Webinar Recap! Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?
  By Gary Glaser and James D. McNairy (May 13th, 2016)

- Bring Out the Body Bags: Seller's Covenant, In Asset Sales Agreement, Not To Compete Within 150 Miles For 10 Years Unenforceable
  By Paul E. Freehling (May 20th, 2016)

- Court Upholds Non-Compete Giving Former Employer Discretion To Determine Whether Ex-Employee Is Working For A Competitor
  By Paul E. Freehling (June 15th, 2016)

- Webinar Recap! Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements
  By John Skelton, Dawn Mertineit, and James Yu (July 1st, 2016)

- All or Nothing: Nevada Supreme Court Refuses to Adopt "Blue Pencil" Doctrine for Non-Compete Agreements
  By Salomon Laguerre (August 4th, 2016)

- D.C. Circuit Upholds NLRB Finding that Employment Agreement's Confidentiality and Non-Disparagement Provisions Violated the NLRA
  By Ashley Laken (August 9th, 2016)

- Federal Court Rejects Foreign Employee's Attempt to Avoid Forum Selection Clause on Grounds He Signed Under Duress Upon Arriving in U.S.
  By Andrew Stark and Erik Weibust (October 24th, 2016)

- HR Professionals Take Note: DOJ and FTC Issue Guidance Regarding Antitrust Laws in the Employment Context
  By Ashley Laken and Timothy F. Haley (October 26th, 2016)

- The White House's Call to Action: A Step in the Right Direction or a Bridge Too Far?
  By Katherine Perrelli, Erik Weibust, and Dallin Wilson (October 28th, 2016)

- Texas Court of Appeals Finds Noncompete Agreement Inapplicable to Former President's Post-Termination Activities Due to the Inexact Language of the Noncompete Period
  By Andrew P. del Junco and Jesse M. Coleman (December 1st, 2016)

- Texas Appellate Court Holds Condition Subsequent in Noncompete Agreement Excused Former Employee's Competitive Activities
  By Jesse M. Coleman and Andrew P. del Junco (December 27th, 2016)

Trading Secrets

Legislation

- Massachusetts Legislature Takes Up Noncompete Reform . . . Again
  By Erik Weibust (March 3rd, 2016)

- Umpteenth Time's the Charm? Massachusetts Has Another Go At Non-Compete Reform
  By Katherine Perrelli, Erik Weibust, and Dawn Mertineit (May 20th, 2016)

- Update: Massachusetts House of Representatives Edits and Unanimously Approves Non-Compete Bill in an Attempt to Make Progress Before End of Legislative Session
  By Dawn Mertineit, Katherine Perrelli, and Erik Weibust (June 30th, 2016)

- One Step Forward, Two Steps Back: Massachusetts Senate Reverses Course On Non-Compete Reform
  By Dawn Mertineit, Katherine Perrelli, and Erik Weibust (July 12th, 2016)

- Massachusetts Governor Supports Noncompete Reform, But Not Abolition
  By Dawn Mertineit, Katherine Perrelli, and Erik Weibust (July 26th, 2016)

- In Like A Lion, Out Like A Lamb: Following Much Fanfare, Massachusetts Noncompete Reform Again Fails
  By Erik Weibust, Dawn Mertineit, and Katherine Perrelli (August 1st, 2016)

- Two New England States Pass Legislation Restricting Physician Non-Competes
  By Erik Weibust and Andrew Stark (August 22nd, 2016)

- New California Law May Preclude Use of Forum-Selection Clauses to Enforce Non-Compete Agreements in Employment Contracts
  By James D. McNairy and Michael Cross (October 10th, 2016)

- A Holiday Miracle? Massachusetts Legislature Discussing Late-Session Non-Compete Deal
  By Erik Weibust (November 22nd, 2016)

International

- EU Publishes Text of Compromise Trade Secrets Directive for Approval by European Parliament
  By Daniel P. Hart (January 26th, 2016)

- Hidden Details: Thoughts on Trade Secrets From the UK
  By Guest Author for TradeSecretsLaw.com: Jeremy Morton (April 12th, 2016)

- European Parliament Debates Proposed Trade Secrets Directive
  By Daniel P. Hart (April 13th, 2016)

- Breaking News: European Parliament Approves Trade Secrets Directive
  By Daniel P. Hart (April 14th, 2016)

- Webinar Recap! International Non-Compete Law Update
  By Dominic Hodson (July 31, 2016)

Social Media and Privacy

- Q&A Concerning IP Protection and Social Media Issues in the Workplace
  By Robert B. Milligan (January 14th, 2016)

- The Legality of Tracking Employees By GPS
  By Karla Grossenbacher (February 16th, 2016)

- Monitoring Employee Communications: A Brave New World
  By Karla Grossenbacher (April 29th, 2016)

2016 Summary Posts

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

By Robert B. Milligan and Daniel Joshua Salinas (January 27th, 2017)

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

1. Defend Trade Secrets Act

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

The DTSA now allows trade secret owners to sue in federal court for trade secret misappropriation, and seek remedies previously unavailable. Employers should be aware that the DTSA contains a whistleblower immunity provision, which protects individuals from criminal or civil liability for disclosing a trade secret if such disclosure is made in confidence to a government official or attorney, indirectly or directly. The provision applies to those reporting violations of law or who file lawsuits alleging employer retaliation for reporting a suspected violation of law, subject to certain specifications (i.e., trade secret information to be used in a retaliation case must be filed under seal). This is significant for employers because it places an affirmative duty on them to give employees notice of this provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information." Employers who do not comply with this requirement forfeit the ability to recoup exemplary damages or attorneys' fees under the DTSA in an action against an employee to whom no notice was ever provided.

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

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

2. EU Trade Secrets Directive

On May 27, 2016, the European Council unanimously approved its Trade Secrets Directive, which marks a sea-change in protection of trade secrets throughout the European Union ("EU"). Each of the EU's 28 member states will have a period of 24 months to enact national laws that provide at least the minimum levels of protections afforded to trade secrets by the directive. Similar to the DTSA, the purpose of the EU's Trade Secrets Directive was to provide greater consistency in trade secrets protection throughout the EU. For further information about the EU's Trade Secrets Directive, please see our webinar "New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive."

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

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

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

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

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

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

4. New State Legislation Regarding Restrictive Covenants

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

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

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

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

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

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

In a case involving alleged violations of the Kansas Uniform Trade Secrets Act ("KUTSA") and the Computer Fraud and Abuse Act ("CFAA"), a Kansas federal district court granted a defendant's motion for summary judgment, holding that (a) payments to forensic experts did not satisfy the KUTSA requirement of showing an "actual loss caused by misappropriation" (K.S.A. 60-3322(a)), and (b) defendant was authorized to access the company's shared files and, therefore, he did not violate the

CFAA. See *Tank Connection, LLC v. Haight*, No. 6:13-cv-01392-JTM (D. Kan., Feb. 5, 2016) (Marten, C.J.).

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

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

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

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

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

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

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

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

6. Forum Selection Clauses

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

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

7. Security Breaches and Data Theft Remain Prevalent

2016 was a record year for data and information security breaches, one of the most notably being WikiLeaks' release of emails purportedly taken from the Democratic National Committee's email server. According to a report from the Identity Theft Resource Center, U.S. companies and government agencies saw a **40% increase** in data breaches from 2015 and suffered over a thousand data breaches. Social engineering has become the number one cause of data breaches, leaks, and information theft. Organizations should alert and train employees on following policy, spotting potential social engineering attacks, and having a clear method to escalate potential security risks. Employee awareness, coupled with technological changes towards better security will reduce risk and exposure to liability. For technical considerations and best practices and policies of attorneys when in the possession of client data, please view our webinar, "A Big Target—Cybersecurity for Attorneys and Law Firms."

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

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

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

2016 Trade Secrets Webinar Series Year in Review Released

By Robert B. Milligan (January 5th, 2017)

Throughout 2016, Seyfarth Shaw'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 11 webinars:

1. 2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Data Security and Trade Secret Protection for Lawyers
3. New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive
4. Protecting Confidential Information and Client Relationships in the Financial Services Industry
5. Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?
6. The Defend Trade Secrets Act: What Employers Should Know Now
7. Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements
8. International Non-Compete Law Update
9. The Intersection of Trade Secrets Violations and the Criminal Law
10. Trade Secret Audits: You Can't Protect What You Don't Know You Have
11. Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches

As a conclusion to this well-received 2016 webinar series, we compiled a list of key takeaway points for each program, which are listed below. For those clients who missed any of the programs in this year's series, the webinars are available on CD upon request, or you may click on the title of each webinar for the online recording. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your groups for CLE credit. Seyfarth will continue its trade secrets webinar programming in 2017, and we will release the 2017 trade secrets webinar series topics in the coming weeks.

2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law

The first webinar of the year, led by Robert Milligan, Jesse Coleman, and Joshua Salinas, reviewed noteworthy cases and other legal developments from across the nation in the areas of trade secret and data theft, non-compete enforceability, computer fraud, and the interplay between restrictive covenant agreements and social media activity, and provided predictions for what to watch for in 2016.

- Data breach is a question of when and not if. Companies should ensure they have implemented sufficient information security policies and a data breach response plan. There are limitations in the law and challenges in international misappropriation cases. The best strategy is to try to prevent breach and misappropriation through effective policies, procedures, and agreements, employee training, technology solutions, and continual assessment and improvement.
- Courts continue to struggle with issues regarding adequacy of consideration for restrictive covenants. Employers who have asked existing employees to sign non-competes or are considering doing the same should evaluate whether consideration was or will be provided for the non-compete to ensure enforcement under applicable law.
- While the circuit court split continues to widen regarding the interpretation of unauthorized access under the Computer Fraud and Abuse Act, the recent decision in *U.S. v. Christensen* (9th Cir. 2015) may provide employers with a civil cause of action in California against employees who misuse company data without permission.

Data Security & Trade Secret Protection for Lawyers

In recent years, the prevalence of data and information security breaches at major corporations have become increasingly more commonplace. While general awareness may be increasing, many companies are still neglecting to address serious information security issues.

In the second installment, Seyfarth attorneys Richard D. Lutkus and James S. Yu were joined by Joseph Martinez, Chief Technology Officer and Vice President of Forensics at Innovative Discovery. This program covered considerations that attorneys should take into account when in possession of any client data. Coverage included both technical considerations, best practices and policies, as well as practical advice to steer clear of ethical violations.

- Whether corporate or outside counsel, there are basic steps that can dramatically increase the security of your or your client's data. Management of data will continue to be a necessity for any entity. Proper policies, protocols, and training should be developed and put into place to protect data in transit and at rest. Use of encryption and access control are both key to proper protection of data.
- Social engineering is the number one cause of data breaches, leaks, and information theft. Organizations should alert and train employees on following policy, spotting potential social engineering attacks, and having a clear method to escalate potential security risks. Employee awareness, coupled with technological changes towards better security will reduce risk and exposure to liability.
- Lawyers have an ethical duty to ensure that reasonable steps are taken to protect their client's and employer's data. Significant statistics have shown that many law firms and practitioners are behind the curve in terms of information security preparedness. Hackers have recently focused their targets on the lax security practices of law firms to obtain client data or inside information.

New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive

In Seyfarth's third installment of its 2016 Trade Secrets Webinar series, Seyfarth attorneys Robert Milligan, Justin Beyer, and Daniel Hart provided attendees with a thorough discussion of the fundamentals as well as updates of the Defend Trade Secrets Act (DTSA) and the proposed EU Trade Secrets Directive. The panel gave insight into the limitations and new benefits of the Act and the proposed Directive.

- With the passage of the Defend Trade Secrets Act, there is now a federal cause of action for trade secrets disapproval. Some of the key provisions in the Act include a three year statute of limitations, the availability of attorneys' fees, exemplary damages, as well as increased criminal penalties for a violation of the Economic Espionage Act. It also includes portions of the DTSA as predicate offenses for the RICO Act.
- The Act also contains language requiring that an employer include information relating to whistleblower immunity for employers to obtain exemplary damages. This only underscores an important point to anyone maintaining employment agreements which contain restrictive covenants: it is imperative for employers to monitor applicable state and federal law to best preserve and maintain their rights and employment agreements.
- The European Commission's directive on trade secret protection will mark a sea-change in protection of trade secrets throughout the European Union. Each of the EU's 28 member states will have a period of 24 months to enact national laws that provide at least the minimum levels of protections afforded to trade secrets by the directive. Look for greater consistency in trade secrets protection throughout the European Union in the years ahead.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

Seyfarth's fourth installment, presented by Scott Humphrey, Marcus Mintz, and Kristine Argentine, focused on trade secret and client relationship considerations in the banking and finance industry, with a particular focus on a firm's relationship with its FINRA members.

- Enforcement of restrictive covenants and confidentiality obligations for FINRA and non-FINRA members are different. Although FINRA allows a former employer to initially file an injunction action before both the Court and FINRA, FINRA—not the Court—will ultimately decide whether to enter a permanent injunction and/or whether the former employer is entitled to damages as a result of the former employee's illegal conduct.
- Address restrictive covenant enforcement and trade secret protection before a crisis situation arises. An early understanding of the viability of your company's restrictive covenants and the steps your company has taken to ensure that its confidential information remains confidential will allow your company to successfully and swiftly evaluate its legal options when a crisis arises.
- Understand the Protocol for Broker Recruiting's impact on your restrictive covenant and confidentially requirements. The Protocol significantly limits the use of restrictive covenants and allows departing brokers to take client and account information with them to their new firm.

Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?

Seyfarth's fifth installment, attorneys Jim McNairy and Marc Jacobs conveyed strategies and best practices to help in-house counsel and HR professionals ensure that company and internal clients are protected.

- The National Labor Relations Act applies to all private sector workplaces—not just unionized facilities. Among other things, the Act protects an employee's right to engage in protected concerted activities, which in general are group action (usually by two or more employees) acting together in a lawful manner, for a common, legal, work-related purpose (e.g., wages, hours and other terms and conditions of employment). Limits on these rights and retaliation against an employee for engaging in protected concerted activity violates the Act. The National Labor Relations Board is aggressively protecting employees' rights to engage in protected

concerted activity. As part of this effort, the NLRB will find unlawful workplace rules, policies, practices and agreements that explicitly restrict Section 7 activities (such as a rule requiring employees to keep their wage rate confidential) or that employees would reasonably believe restricts their Section 7 rights (e.g., a confidentiality agreement or policy that generally includes in the definition of confidential information "personnel information").

- In the 2015 *Browning-Ferris Industries* decision, the NLRB substantially broadened the definition of "joint employer." Under this new expanded definition, an entity can be found to be a joint employer if it has the authority, even if unexercised, to control essential terms and condition of employment. As a result, if one entity has agreements with other entities to provide labor or services, that entity may be a joint employer of the other entities' employees based on the level of control it has over the terms and conditions of employment of the other entities/ employees. One indicia of that control would be requirements for hiring or employment, such as requirements to sign agreements or adopt policies for the protection of confidential information and similar restrictions.
- As a result, and also because of the signing of the federal Defend Trade Secrets Act, now is a critical time for all employers to review their policies, practices, procedures and agreements (1) regarding the protection of confidential information; and (2) with third-party service and labor providers. In reviewing confidential information policies and agreements, the focus should be on narrow tailoring using specifics and examples to protect information that lawfully may be protected in a lawful manner. For agreements with parties, the review should include an analysis of the factors that may show joint employer status so that you can balance the risk of a joint employer finding with the needs to protect your organization.

The Defend Trade Secrets Act: What Employers Should Know Now

In Seyfarth's sixth installment, attorneys Robert Milligan, Daniel Hart, and Amy Abeloff described the key features of the Defend Trade Secrets Act ("DTSA") and compared its key provisions to the state Uniform Trade Secrets Act ("UTSA") adopted in many states. They also provided practical tips and strategies concerning the pursuit and defense of trade secret cases in light of the DTSA, and provide some predictions concerning the future of trade secret litigation.

- The DTSA was passed after many failed attempts at creating trade secret legislation allowing for a federal cause of action for misappropriation. The bill was passed with overwhelming bipartisan, bicameral support, as well as backing from many big name businesses. The DTSA now allows trade secret owners to sue in federal court for trade secret misappropriation, and seek remedies heretofore unavailable.
- The DTSA contains an immunity provision that protects individuals from criminal or civil liability for disclosing a trade secret if such disclosure is made in confidence to a government official or attorney, indirectly or directly. The provision applies to those reporting violations of law or who file lawsuits alleging employer retaliation for reporting a suspected violation of law, subject to certain specifications (i.e., trade secret information to be used in a retaliation case must be filed under seal). The DTSA places an affirmative duty on employers to give employees notice of this provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information," and will only be in compliance with this requirement if the employer cross-references a policy given to relevant employees describing the reporting policy for suspected violations of law. Employers that do not comply with this requirement forfeit the ability to recoup exemplary damages or attorney fees in an action brought under the DTSA against an employee to whom no notice was ever provided.

- Though the passage of the DTSA creates a new federal cause of action for trade secret misappropriation, the passage does not render state law and causes of action irrelevant or unimportant. The UTSA is still an available cause of action in 48 states, and state law on misappropriation still plays a vital role in drafting non-disclosure and non-competition agreements. Though the DTSA can place certain limitations on employees via employment agreements and employers may be able to seek injunctive relief against former employees in the event of misappropriation, such restrictions must comport with relevant state law.

Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements

In the seventh installment of Seyfarth's webinar series, attorneys John Skelton, James Yu, and Dawn Mertineit focused on the importance of state-specific non-compete laws and legislation and recent Federal and State efforts to regulate the use of non-compete agreements; enforcement considerations for the Franchisee when on-boarding and terminating employees; and lessons learned from recent decision regarding enforcing non-compete provisions upon termination and non-renewal.

- As reflected by the May 5, 2016, White House report (Non-Compete Agreements: Analysis of the Usage, Potential Issues, and State Responses), state and federal non-compete legislative proposals and recent enforcement action by the Illinois Attorney General challenging the use of non-compete agreements for lower level employees, Franchisors and Franchisees need to anticipate more regulation and scrutiny.
- With respect to their own employees, Franchisors and Franchisees need to develop and implement on-Boarding, termination and other procedures designed to ensure that both departing and prospective employees understand their ongoing obligations with respect to the company's confidential and proprietary information and trade secrets and that such information is protected throughout the employment relationship.
- The enforceability of non-compete provisions are most often litigated in the context of a request for a preliminary injunction and several recent decisions confirm that to enforce a non-compete against a departing franchisee the franchisor (1) should be able to show harm to actual competition; (2) needs to act promptly and that enforcement delays likely means that any alleged harm is not irreparable; and (3) should develop and implement a post-termination plan beyond simply sending a notice of termination as the franchisor will need to present evidence of actual harm.

International Non-Compete Law Update

In this installment in Seyfarth's 2016 Trade Secrets Webinar Series, International attorney Dominic Hodson focused on non-compete considerations from an international perspective. Dominic discussed general principals and recent international developments in non-compete issues around the globe. Companies who compete in the global economy should keep in mind these key points:

- Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. However, there are some common requirements and issues regarding enforceability based on the region, particularly in common law jurisdictions such as the UK, Canada (excluding Quebec), Australia/New Zealand, and Singapore/Hong Kong. A restrictive covenant is void unless it is reasonable to protect a legitimate interest of the employer; simply wanting to stop competition post-termination is not a legitimate interest.

- Outside of common law countries, there is no uniformity in rules, and every country must be taken separately. There are often detailed statutory rules that the clause must fulfill, but nevertheless there are repeating themes: There must be reasonableness to the non-compete agreement, and you must require proportionality between the clause and the interest sought to be protected.
- With respect to non-common law countries, liquidated damaged are often allowed. Civil law countries tend to be much more forgiving of liquidated damages and don't have the same rules regarding "penalty clauses."

The Intersection of Trade Secrets Violations and the Criminal Law

In this webinar, attorneys Andrew Boutros, Katherine Perrelli, and Michael Wexler focused on criminal liability for trade secret misappropriation. Trade secret misappropriation is increasingly garnering the attention of federal law enforcement authorities. This reality creates different dynamics and risks depending on whether the company at issue is being accused of wrongdoing or is the victim of such conduct.

- The theft of trade secrets is not only a civil violation—it is also a criminal act subject to serious fines and imprisonment. In an ever-increasing technological age where a company's crown jewels can be downloaded onto a thumb drive, victims and corporate violators must be mindful of the growing role that law enforcement plays in this active area. And, in doing so, working with experienced counsel is critical to interfacing with law enforcement (especially depending on which side of the "v." you are on), while still maintaining control of the civil litigation.
- With the advent of the Defend Trade Secrets Act (DTSA), intellectual capital owners have a powerful new tool to both protect assets with as well potentially defend against. As such, processes must be in place to carefully screen new employees as well as provide vigilance over exiting employees so that one can guard against theft and be prepared to address purported theft brought to ones doorstep with a new hire. Finally, it is important to review and update agreements with the latest in suggested and required language to maximize protections, which is best accomplished through annual reviews of local and federal statutes with one's counsel.
- "Protect your own home" by putting tools in place before a trade secret misappropriation occurs. This includes taking a look at your employment agreements to make sure they are updated to comply with the DTSA and that they have been signed. In addition, make sure you have agreements in place with third parties (e.g., clients, vendors, contractors, suppliers) to protect your proprietary information. Finally, secure your network and facilities by distributing materials on a need-to-know basis: Don't let your entire workforce have access.

Trade Secret Audits: You Can't Protect What You Don't Know You Have

In Seyfarth's tenth installment, attorneys Robert Milligan, Eric Barton, and Scott Atkinson focused on trade secret audits. It is not uncommon for companies to find themselves in situations where important assets are overlooked or taken for granted. Yet, those same assets can be lost or compromised in a moment through what is often benign neglect. Experience has shown that companies gain tremendous value by taking a proactive, systematic approach to assessing and protecting their trade secret portfolios through a trade secret audit.

- As part of any trade secret audit, confidentiality agreements should be updated to include the new immunity language required by the Defend Trade Secrets Act (DTSA) to preserve the company's right to exemplary damages and attorney's fees under the DTSA.
- A trade secret audit, and the resulting protection plan, should have three primary goals:
  (1) Ensure that a company's trade secrets are adequately identified and protected from disclosure;
  (2) Ensure that a company has taken adequate steps to protect itself in litigation if a trade secret is misappropriated; and
  (3) Limit the risk of exposure to other companies' claims of trade secret misappropriation.
- As part of a trade secret audit, onboarding and off-boarding procedures are evaluated to ensure that the intellectual property rights of third parties and the company are respected.

Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches

In Seyfarth's final installment in the 2016 Trade Secrets Webinar Series, James McNairy and Justin Beyer, joined by computer forensics expert Jim Vaughn of iDiscovery Solutions, focused on best practices for assembling the evidence most often needed to prosecute a claim for misappropriation of trade secrets.

- The first step in prosecuting trade secret misappropriation starts with identifying your trade secret information, maintaining its confidentiality, and putting in place safeguards such as robust confidentiality agreements, computer use and access policies, and exit interviews that are tailored to flag any exfiltration of data by high risk employees or business partners with whom your company is parting ways. Diligence on the front end will better alert your organization of potential data theft and enable it to secure the data, should it be misappropriated.
- As part of your investigation of potential trade secret misappropriation, remember to conduct a complete audit of devices and sources of data storage and transmission to ensure nothing is overlooked. While doing so, it is critical to maintain the forensic integrity of the devices and data to allow the best chance of admitting the information into evidence in any litigation.
- Efficiently organizing the right team to prosecute trade secret theft is critical. The "team" most often includes human resources professionals (to authenticate key agreements, policies, dates of employment etc.), a senior manager or executive (who can validate the existence of the trade secret, its value, the measures taken to maintain secrecy etc.), senior managers who worked with the suspected misappropriators (who can attest to access, use, and possession of the at issue information), in-house IT professionals (who can lay the foundation for devices, data, and access rights of the suspected misappropriators), and an independent computer forensics expert (who can objectively present the facts concerning data accessed, by whom, through what means, and explain any technical nuance to "connect the technical dots" of the bad actor(s) conduct).

2017 Trade Secret Webinar Series

Beginning in January 2017, we will begin another series of trade secret webinars. The first webinar of 2017 will be "2016 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law." To receive an invitation to this webinar or any of our future webinars, please sign up for our Trade Secrets, Computer

Trading Secrets

Fraud & Non-Competes mailing list by clicking here. Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your groups for CLE credit.

Trade Secrets Legislation

Senate Judiciary Committee to Hold Meeting About Passage of the DTSA

By Amy Abeloff and Robert B. Milligan (January 21st, 2016)

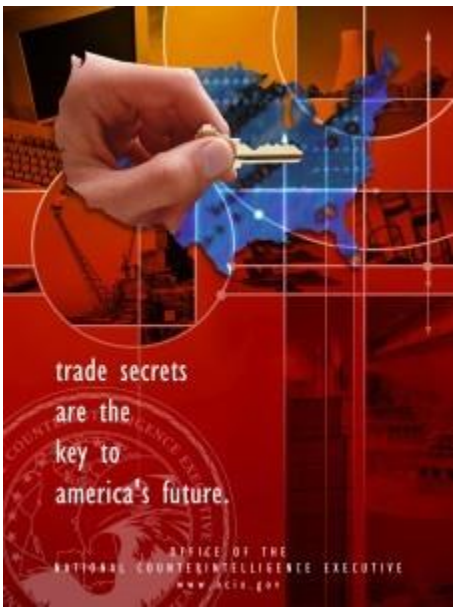
This morning in Washington, the Senate Judiciary Committee will hold a meeting to consider S. 1890, the Defend Trade Secrets Act of 2015 ("DTSA"). The passage of the DTSA would provide a federal civil cause of action for the theft of trade secrets. Trade secret law currently consists of a mix of federal protection through the Economic Espionage Act ("EEA") and the various state versions of the Uniform Trade Secret Act ("UTSA"). Instead of this patchwork-like scenario, the DTSA would create a uniform standard that individuals and companies could use to protect and fight against violations of their highly valuable trade secrets. Trade secrets violations end up being costly not only to these entities, but also to end consumers. Utilizing a protective measure like the DTSA to defend trade secrets could help curb job and revenue losses, resulting in a net benefit to the American economy.

The DTSA was introduced in the House and Senate on July 29, 2015. Since then, the DTSA has enjoyed bipartisan support, as well as broad support in various industries, such as the manufacturing, biotech, software, and agriculture sectors. After gaining more support, careful drafting and negotiation, the DTSA is now ready for markup, which the Senate Judiciary Committee will be doing today.

Currently, S. 1890 has 26 cosponsors in the Senate: Sen. Tammy Baldwin (D-WI), Sen. Chris Coons (D-DE), Sen. Richard Durbin (D-IL), Sen. Jeff Flake (R-AZ), Sen. Thom Tillis (R-NC), Sen. Richard Blumenthal (D-CT), Sen. Roy Blunt (R-MO), Sen. Michael Crapo (R-ID), Sen. James Risch (R-ID), Sen. Kelly Ayotte (R-NH), Sen. Mark Kirk (R-IL), Sen. Amy Klobuchar (D-MN), Sen. David Perdue (R-GA), Sen. Jefferson "Jeff" Sessions (R-AL), Sen. Christopher Murphy (D-CT), Sen. Claire McCaskill (D-MO), Sen. Alan "Al" Franken (D-MN), Sen. Angus King (I-ME), Sen. Susan Collins (R-ME), Sen. Roger Wicker (R-MS), Sen. Deb Fischer (R-NE), Sen. Dean Heller (R-NV), Sen. Mazie Hirono (D-HI), Sen. Dianne Feinstein (D-CA), and the most recent supporters, Sen. Lindsey Graham (R-SC) and Sen. Sheldon Whitehouse (D-RI). The House version of the DTSA, H.R. 3326, currently has 107 cosponsors, including 77 Republicans and 30 Democrats.

Senate Judiciary Committee Votes in Favor of Passage of an Amended Defend Trade Secrets Act

By Amy Abeloff and Robert B. Milligan (January 28th, 2016)



Earlier today, the Senate Judiciary Committee held a voice vote in favor of the passage of the now amended Defend Trade Secrets Act of 2016 ("DTSA"). At this point, the Committee has not yet revealed when the current version of the DTSA will make it to a floor vote, nor has it been announced when and if the House will consider the issue. The House's version of the DTSA was introduced late last July, and now has 107 cosponsors. It remains to be seen whether the House version will include the Senate's amendments.

Below are some highlights from the Senate's amended version of the DTSA:

- The section limiting injunctive relief has been fortified insofar as a court shall not grant such relief if it would prevent a person from entering into an employment relationship. Under the new language, a court could place conditions on that employment relationship only upon a showing through evidence of "threatened misappropriation and not merely on the information the person knows." This language was likely added to guard against "inevitable disclosure" based upon the statute.

- The statute of limitations has decreased from five to three years.

- The Senate has added an immunity provision to protect individuals from criminal or civil liability for disclosing a trade secret if it is made in confidence to a government official, directly or indirectly, or to an attorney, and it is made for the purpose of reporting a violation of law. Moreover, the amended language places an affirmative duty on employers to provide employees notice of the new immunity provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information." An employer will be in compliance with the notice requirement if the employer provides a "cross-reference" to a policy given to the relevant employees that lays out the reporting policy for suspected violations of law. Should an employer not comply with the above, the employer may not recover exemplary damages or attorney fees in an action against an employee to whom no notice was ever provided. **Curiously the definition of employee is drafted broadly to include contractor and consultant work done by an individual for an employer**.

- New language further restricting the *ex parte* seizure ordered now appears in the Senate's DTSA. This language now prohibits copies to be made of the seized property, and requires that the *ex parte* order provide more specific instructions for law enforcement officers performing the seizure, such as when the seizure can take place and whether force may be used to access locked areas.

- A new section was added "Trade Secret Theft Enforcement," which increases the penalties for a violation of 18 U.S.C. §1832 from $5,000,000 to the greater of $5,000,000 or 3 times the value of the stolen trade secrets to the organization, including the costs of reproducing the trade secrets. It also adds a provision that allows trade secret owners to be heard in criminal court concerning the need to protect their trade secrets. It also amends the RICO statute to add a violation of the Economic Espionage Act as a predicate act.

- Exemplary damages have been lowered from three times to two times the amount of actual damages.

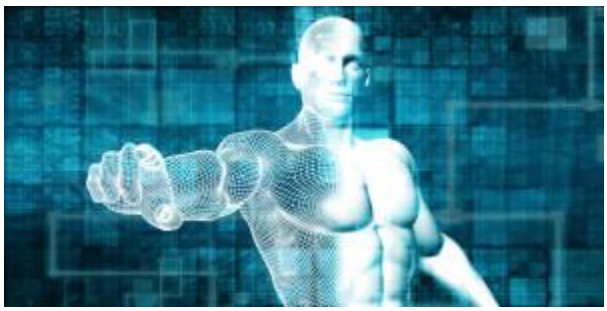
What's Next

- Now that the Senate Judiciary Committee has amended the DTSA and voted (by voice vote) in favor of its passage, the DTSA is poised for presentment on the Senate floor, and potential later for presentment in the House. Even before the amendments, the DTSA enjoyed bipartisan support in both houses, as well as widespread support from companies like DuPont, General Electric, and Microsoft, to name but a few. Stay tuned for further coverage.

- These amendments came just a day after Senators Orrin Hatch (R-Utah) and Chris Coons (D-Delaware) co-authored an article emphasizing the importance of having a federal cause of action for trade secret misappropriation available. The Senators highlighted the difficulties trade secret owners face in protecting their rights, such as appealing to state courts or federal prosecutors, which creates costly and complicated procedural and jurisdictional issues. Moreover, the Senators noted the limited resources the United States Department of Justice has to prosecute trade secrets cases. Without enough resources, trade secret misappropriators can cross state lines, and even destroy evidence of their legal violations, much to the detriment of U.S. businesses and individuals. As the Senators point out in their article, the Senate's version of the DTSA provides business owners the ability to seek court orders (only upon an appropriate showing of trade secret ownership, theft, and lack of harm to third parties upon the issuance of such an order) to stop further theft of their trade secrets, not at all a means to seize information for anti-competitive purposes.

Senate Judiciary Committee Issues Report in Support of Defend Trade Secrets Act

By Amy Abeloff and Robert B. Milligan (March 22nd, 2016)



The Senate Judiciary Committee recently released Senate Report 114-220 regarding the Defend Trade Secrets Act of 2016 ("DTSA"). A background on and recent developments of the DTSA are discussed more fully on our blog.

The Judiciary's most recent report, authored by Senator Chuck Grassley (R-IA), recommended that the recently amended version of S. 1890 pass.

The Report was separated into seven subparts, which discussed the (1) background and purpose of the DTSA; (2) the history of the bill and committee consideration; (3) a section-by-section summary of the bill; (4) a congressional budget office cost estimate; (5) a regulatory impact evaluation; (6) concluding remarks; and (7) changes to existing law that the bill would effect. The most noteworthy sections are discussed below.

Background and Purpose of the DTSA

The Report began by noting the importance of the legal protection of trade secrets, as well as the "economically damaging" effect on their theft. The Report illustrated this damage by comparing the economic loss to the American economy caused by trade secret theft ($300 billion) to the total annual level of U.S. exports to Asia, and by noting that 2.1 million U.S. jobs are lost each year due to such theft. Trade secret theft, the Report acknowledged, is becoming harder to pinpoint as technological advances promulgate. In this regard, the Report recognized the lack of civil remedy at the federal level for trade secret theft, and described how the DTSA would amend the Economic Espionage Act of 1996 ("EEA") to provide for not only a federal criminal remedy, but also for a federal civil remedy for trade secret misappropriation. The DTSA would provide victims of trade secret theft equitable remedies as well as damages awards. Equitable remedies under the DTSA include expedited relief in the form of an *ex parte* seizure, but only in extreme circumstances so as to prevent further dissemination of trade secret information and/or for the preservation of evidence.

The *ex parte* seizure provision has met some adversity. However, the Report sought to mitigate any opposition by recalling that the DTSA balances the seizure provision with the rights of defendants and third parties by: (1) minimizing interruption to business operations of third parties; (2) protecting seized property from disclosure; and (3) setting a hearing date as soon as practicable.

History of the Bill and Committee Consideration

The Report next delineated the history of the DTSA, which includes past bills S. 3389, the Protecting American Trade Secrets and Innovation Act of 2012 (introduced by Senators Kohl, Coons, and Whitehouse), and S. 2267, the Defend Trade Secrets Act of 2014 (introduced by Senators Coons and Hatch). Next, the Report referenced the Committee hearing that occurred on December 2, 2015 (about which we blogged and held a Live Tweet), which featured intellectual property counsel from E.I. DuPont de Nemours and Company and Corning, Incorporated, as well as an expert on trade secret

law, and a professor specializing in trade secret academia. Previous to the December hearing, the Senate Judiciary Committee's Subcommittee on Crime and Terrorism held a hearing in May 2014, entitled ''Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?," which featured testimony from an FBI representative, the Vice President of Intellectual Property Management at the Boeing Company, the President and CEO for the Center for Responsible Enterprise and Trade, the President of Marlin Steel Wire Products, and the Vice President and General Patent Counsel for Eli Lilly and Company.

More recently, in January 2016, Senators Hatch and Coons presented two "groups" of amendments to the DTSA (blogged here), taking into consideration suggestions from other members of the Judiciary Committee. As such, it unanimously adopted both groups of amendments.

The first group of amendments: (1) made it so only a trade secret owner could bring a civil action for misappropriation; (2) changed the statute of limitations from five years to three years; (3) re-defined "trade secret" and "improper means;" (4) clarified that *ex parte* seizures may only be instituted in "extraordinary circumstances" and placed further limitations on the seizures; (5) clarified the appropriate scope of injunctions relating to employment to ensure that court orders are not contrary to applicable state laws; and (6) added language expressing Congress' notion of the importance of balancing the interests of all parties when issuing an *ex parte* seizure, and "instructing the Federal Judicial Center to develop best practices for the execution of seizures and the storage of seized information."

The second group of amendments sought to provide protection to "whistleblowers who disclose trade secrets to law enforcement in confidence for the purpose of reporting or investigating a suspected violation of law," and the "confidential disclosure of a trade secret in a lawsuit, including an anti-retaliation proceeding."

Section-by-Section Summary of the Bill

Much of the substance of the section-by-section summary portion of the Report appears above. That said, below appears a list of additional points of interest presented by section of the bill:

- Section 2 of the bill describes federal jurisdiction for theft of trade secrets. Importantly, it describes the *ex parte* seizure orders and their scope. A portion of the summary is reproduced and discussed below:

    - *Ex parte* seizures will only issue upon a showing that the prerequisites for the issuance of such are present. In other words, a seizure will only issue if an injunction under the rules of civil procedure would be adequate, such as when there is evidence that a defendant is a flight risk or will immediately share the trade secret with third parties. The Report lists further requirements a party must show in order for a seizure order to issue:

(1) a temporary restraining order issued pursuant to Federal Rule of Civil Procedure 65(b) would be inadequate because the party to which the order would be issued would evade, avoid, or otherwise not comply with it;

(2) immediate and irreparable injury will occur if the seizure is not ordered;

(3) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom the seizure is ordered and substantially outweighs the harm to any third parties;

(4) the applicant is likely to succeed in showing that the person against whom the seizure is ordered misappropriated the trade secret by improper means, or conspired to misappropriate the trade secret by improper means, and is in actual possession of it and any property to be seized;

(5) the applicant describes with reasonable particularity the matter to be seized and, to the extent reasonable, identifies the location where the matter is to be seized;

(6) the person against whom the seizure would be ordered, or those working in concert with that person, would destroy, move, hide, or otherwise make such matter inaccessible if the applicant were to provide that person notice; and

(7) the applicant has not publicized the requested seizure.

The Report hypothesized that courts would require a party seeking a seizure order to describe the trade secret at issue with "sufficient particularity," especially in light of the "actual possession" requirement, which aids in protecting third parties from succumbing to the seizure order (like Internet service providers).

- Remedies
    - Equitable remedies are provided for in the bill, but if found appropriate, the bill allows a court to require "affirmative actions to be taken to protect the trade secret" and may "condition future use of the trade secret upon payment of a reasonable royalty" for a determined amount of time.
    - Additional state law remedies are available under the Uniform Trade Secrets Act ("UTSA") of a particular jurisdiction as well as under the DTSA. As such, the DTSA does not preempt state law with regard to remedies, and, with particular regard to equitable remedies, is "intended to coexist with… applicable State law governing when an injunction should issue in a trade secret misappropriation matter."
    - Exemplary damages and attorney's fees are available as well.
- Definitions; Rule of construction; Conforming amendments
    - "Misappropriation" is defined as it is under Section 1(2) of the UTSA; and
    - "Improper Means" is defined as it is under Section 1(1) of the UTSA
- Section 3 of the bill discusses the enforcement of trade secret theft. It sets a maximum penalty for violation of the bill to be "the greater of $5,000,00 or three times the value of the stolen trade secret" to the owner of the trade secret. Such amount includes "expenses for research and design and other costs." Section 3 also amends 18 U.S.C.§ 1961(1) to include portions of the DTSA as "predicate offenses for the Racketeer Influenced and Corrupt Organizations (RICO) Act.
- Section 4 of the bill discusses report on theft of trade secrets occurring abroad and requires the filing of a report by the U.S. Attorney General on several issues, including the "scope and breadth of trade secret theft from United States companies occurring *outside* the United States" (emphasis added).

It remains to be seen whether the Senate's Report will have any effect on the House's bill, H.R. 3326, which currently has 126 co-sponsors, but does not contain some of the changes made to the Senate bill by the Judiciary Committee.

U.S. Senate Passes Bill Creating A Civil Cause of Action in Federal Court for Trade Secret Misappropriation

By Robert B. Milligan (April 5th, 2016)

The U.S. Senate passed on a unanimous 87-0 vote the Defend Trade Secrets Act of 2016 late Monday.

The bill will create a civil cause of action in federal court for trade secret misappropriation and provide remedies that are not available in state court trade secret actions.

Like patents, trademarks, and copyrights, trade secret owners may seek redress for intellectual property theft based on a federal statutory right in federal court should the bill become law. Additionally, the bill provides for the availability of orders that will allow trade secret owners to have law enforcement seize stolen trade secrets without notice to the misappropriator upon a sufficient showing to the federal court.

The Obama Administration has indicated that it supports the Act. In a statement issued Monday, the Executive Office of the President stated that it "strongly supports" the legislation and its "more uniform, reliable, and predictable way to protect … valuable trade secrets."

Attention will now shift to the House where there is strong bi-partisan support for a similar version of the Act. The House bill, sponsored by Reps. Doug Collins (R-Ga.) and Jerrold Nadler (D-N.Y.) presently has 128 sponsors.

Senators Orrin Hatch (R-Utah) and Chris Coons (D-Del.), the leading sponsors of the Senate bill, have indicated that the bill will harmonize federal law and give businesses more consistent legal protections when their trade secrets are stolen.

In their op-ed piece in Politco, Hatch and Coons stated that, "[m]aintaining the status quo is woefully insufficient to safeguard against misappropriation in today's fast-paced innovation economy."

The Senators added:

Trade secrets are the lifeblood of the American economy. Virtually all companies depend on trade secrets to protect their most valuable information and processes. The medical device industry, for example, dedicates enormous resources to the research and development of life-saving products; much of that investment is shielded as trade secrets. Businesses that provide IT infrastructure and data storage—the backbone of the innovation economy—get their competitive edge from proprietary designs and software principally defended by trade secret law. In today's knowledge- and service-based economy, trade secrets are indispensable to protecting confidential, intangible assets. According to some estimates, trade secrets are worth $5 trillion to the U.S. economy, on par with patents. The loss from their misappropriation is substantial—between $160 billion and $480 billion annually.

The bill amends the Economic Espionage Act of 1996 to create a private civil cause of action for trade secret misappropriation.

Specifically, the bill authorizes a trade secret owner to file a civil action in a U.S. district court seeking relief for trade secret misappropriation related to a product or service in interstate or foreign commerce. It establishes remedies, such as an injunction, damages, attorneys' fees and exemplary damages. The statute of limitation is set at three years from the date of discovery of the misappropriation.

A trade secret owner may apply for and a court may grant a seizure order to prevent dissemination of the trade secret if the court makes specific findings, including that an immediate and irreparable injury will occur if seizure is not ordered. A court must take custody of the seized materials and hold a seizure hearing within seven days. Any party harmed by the order may move to dissolve or modify the order and may also seek relief against the applicant of the seizure order for wrongful or excessive seizure.

The Department of Justice must submit to Congress and publish a biannual report on trade secret theft outside the United States.

The bill expresses the sense of Congress that: (1) trade secret theft occurs in the United States and around the world, (2) trade secret theft harms owner companies and their employees, and (3) the Economic Espionage Act of 1996 applies broadly to protect trade secrets from theft.

A new section was also added entitled "Trade Secret Theft Enforcement," which increases the criminal penalties for a violation of 18 U.S.C. §1832 from $5,000,000 to the greater of $5,000,000 or 3 times the value of the stolen trade secrets to the organization, including the costs of reproducing the trade secrets. It also adds a provision that allows trade secret owners to be heard in criminal court concerning the need to protect their trade secrets. It amends the RICO statute to add a violation of the Economic Espionage Act as a predicate act.

We recently conducted a webinar on the Act entitled New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive on Trade Secrets which is now available as a podcast and webinar recording. The webinar provides the fundamentals as well as updates concerning the Defend Trade Secrets Act and the proposed EU Trade Secrets Directive.

House Judiciary Committee Passes Senate's Version of the Defend Trade Secrets Act

By Amy Abeloff and Robert B. Milligan (April 20th, 2016)

On April 4, 2016, the Senate Judiciary Committee passed S. 1890, the Defend Trade Secrets Act of 2016 ("DTSA"). Soon after, House Judiciary Committee Chairman Bob Goodlatte (R-VA) released a statement in which he applauded the Senate's passage of the bill, noting that "trade secrets are an increasingly important form of intellectual property that have become more vulnerable to theft as a result of our globalized economy." The Chairman also indicated his enthusiasm in "moving legislation to protect American trade secrets through the House Judiciary Committee in the coming weeks."

Goodlatte was sure true to his word, as the House Committee approved S. 1890 by voice vote today. Companion legislation was introduced as well by Representative Doug Collins (R-GA). Supporters of the passage included Goodlatte, Collins, as well as Ranking Member John Conyers (D-MI), Courts, Intellectual Property, and the Internet Subcommittee Chairman Darrell Issa (R-CA), Courts, Intellectual Property, and the Internet Subcommittee Ranking Member Jerrold Nadler (D-NY), and Rep. Hakeem Jeffries (D-NY). The supporters emphasized the importance of trade secrets as a form of intellectual property vulnerable to theft as a result of our ever-increasing globalized economy. The supporters characterized S. 1890 as giving "American innovators a powerful new tool which will help them compete in an ever-evolving global market." The bill will now likely go to the House for a vote.

What Does the Passage of the Defend Trade Secrets Act Mean for Your Business?

By Amy Abeloff and Robert B. Milligan (April 27th, 2016)

Congress passed federal trade secrets legislation today. On April 4, 2016, the Senate passed S. 1890, the Defend Trade Secrets Act of 2016 ("DTSA"). Soon after, on April 20, 2016, the House Committee approved S. 1890 by voice vote. Today, the House passed the DTSA. President Obama has voiced his support for the DTSA, which indicates that he will sign it.

What does the passage of the DTSA mean for your company? In a nutshell, it means your company can now pursue claims for trade secret misappropriation in federal court like other forms of intellectual property (i.e., patent, trademark, copyright) and seek remedies such as a seizure order to recover misappropriated trade secrets. It also serves a reminder that trade secrets can be highly valuable to your company and that you should ensure that your company has reasonable secrecy measures in place to protect them.

Below we outline a brief history of the DTSA, describe what legal structure and remedies the DTSA creates, and describe the unique provisions of the DTSA. We also provide tips and strategies in light of the passage of the DTSA.

Brief History of the Defend Trade Secrets Act

On July 29, 2015, with bipartisan and bicameral support, Congressional leaders Senators Orrin Hatch (R-UT), Christopher Coons (D-DE), and Representative Doug Collins (R-GA) introduced bills to create a federal private right of action for the misappropriation of trade secrets. The identical bills, HR 3326 and S. 1890, were then referred to their respective judiciary committee. The proposed legislation, titled the "Defend Trade Secrets Act of 2015" followed an unsuccessful attempt the previous year to pass the "Defend Trade Secrets Act of 2014."

The Senate Judiciary Committee later held a hearing on December 2, 2015 (about which we blogged and held a Live Tweet), which featured intellectual property counsel from DuPont and Corning and a trade secret expert who spoke out in favor of the legislation.

In January 2016, Senators Hatch and Coons presented two "groups" of amendments to the DTSA (blogged here), taking into consideration suggestions from other members of the Senate Judiciary Committee. The Committee unanimously adopted both groups of amendments, and held a voice vote in favor of the passage of the now amended Defend Trade Secrets Act of 2016.

Senator Grassley of the Senate Judiciary Committee authored a Report about the now amended DTSA on March 7, 2016, in which he described the background and purpose of the bill. It describes a "trade secret" as a "form of intellectual property that allow[s] for the legal protection of commercially valuable, proprietary information." The stated purpose of the bill, per the Report, is to allow trade secret owners

to "protect their innovations by seeking redress in Federal court," which would allow them to bring "their rights into alignment with those long enjoyed by owners of other forms of intellectual property."

As noted above, the Senate passed the DTSA on April 4, and the House Judiciary Committee approved the Senate's version of the DTSA on April 20. On April 27, 2016, the House voted in favor of the DTSA. President Obama has indicated that he will sign the bill.

What Does the DTSA Provide?

The DTSA would authorize a civil action in federal court for the misappropriation of trade secrets that is related to a product or service used in, or intended for use in, interstate or foreign commerce. Trade secret claims are presently state law claims, and 48 states have adopted some version of the Uniform Trade Secrets Act (UTSA). New York and Massachusetts, the only two states that have yet to adopt a version of the UTSA, provide civil remedies under the common law for trade secret misappropriation.

The DTSA seeks to do the following: 1) create a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act of 1996 ("EEA") to provide a federal civil remedy for trade secret misappropriation; 2) provide parties pathways to injunctive relief and monetary damages in federal court to prevent disclosure of trade secrets and account for economic harm to companies whose trade secrets are misappropriated, including via ex parte property seizures (subject to various limitations), which means that a plaintiff can seek to have the government seize misappropriated trade secrets without providing notice to the alleged wrongdoer; and 3) harmonize the differences in trade secret law under the UTSA and provide uniform discovery.

The current legislation is the final product of a series of amendments made since the introduction of the Defend Trade Secrets Act of 2014. The significant aspects of the DTSA are summarized below:

- The DTSA provides for actual damages, restitution, injunctive relief, significant exemplary relief (up to two times the award of actual damages), and attorney's fees.
- *Ex parte* property seizures are available to plaintiffs, but subject to limitations. As noted above, an *ex parte* seizure means that an aggrieved party can seek relief from the court against a party to seize misappropriated trade secrets without providing notice to the alleged wrongdoer beforehand. As a measure to curtail the potential abuse of such seizures, the DTSA prohibits copies to be made of seized property, and requires that *ex parte* orders provide specific instructions for law enforcement officers performing the seizure, such as when the seizure can take place and whether force may be used to access locked areas. Moreover, a party seeking an *ex parte* order must be able to establish that other equitable remedies, like a preliminary injunction, are inadequate.
- Injunctive relief for actual or threatened misappropriation of trade secrets is limited in that a court will not grant injunctive relief if it would prevent a person from entering into an employment relationship. A court could further place conditions on that employment relationship only upon a showing through evidence of "threatened misappropriation and not merely on the information the person knows." This language was added to guard against plaintiffs pursuing "inevitable disclosure" claims.
- The statute of limitations is three years. A civil action may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered.
- An immunity provision exists to protect individuals from criminal or civil liability for disclosing a trade secret if it is made in confidence to a government official, directly or indirectly, or to an attorney, and it is made for the purpose of reporting a violation of law. This provision places an affirmative duty on employers to provide employees notice of the new immunity provision in

"any contract or agreement with an employee that governs the use of a trade secret or other confidential information." An employer will be in compliance with the notice requirement if the employer provides a "cross-reference" to a policy given to the relevant employees that lays out the reporting policy for suspected violations of law. Should an employer not comply with the above, the employer may not recover exemplary damages or attorney fees in an action brought under the DTSA against an employee to whom no notice was ever provided. Curiously, the definition of "employee" is drafted broadly to include contractor and consultant work done by an individual for an employer.

- The "Trade Secret Theft Enforcement" provision increases the penalties for a criminal violation of 18 U.S.C. § 1832 from $5,000,000 to the greater of $5,000,000 or three times the value of the stolen trade secrets to the organization, including the costs of reproducing the trade secrets.
- The DTSA also contains a provision that allows trade secret owners to be heard in criminal court concerning the need to protect their trade secrets.
- The DTSA further amends the RICO statute to add a violation of the Economic Espionage Act as a predicate act.

In sum, the DTSA provides aggrieved parties with legal recourse in federal court via a federal trade secret cause of action (whereas previously, relief was only available under the state law UTSA or common law claims), as well as new remedies, including a seizure order. A party can now sue in federal court for trade secret misappropriation and seek actual damages, restitution, injunctive relief, ex parte seizure, exemplary damages, and attorney's fees under the DTSA.

Provisions Unique to the DTSA

The DTSA differs from the UTSA in several important aspects. Before delving into the differences further, it bears noting that the UTSA regime will not be preempted by the DTSA; in other words, UTSA claims will still be available to aggrieved parties. Most notably, it opens the federal courts to plaintiffs in trade secrets cases. The DTSA also allows for an *ex parte* seizure order. A plaintiff fearful of the propagation or dissemination of its trade secrets would be able to take proactive steps to have the government seize misappropriated trade secrets prior to giving any notice of the lawsuit to the defendant. However, the *ex parte* seizure order is subject to important limitations that minimize interruption to the business operations of third parties, protect seized property from disclosure, and set a hearing date as soon as practicable. The proposed seizure protection goes well beyond what a court is typically willing to order under existing state law. Of course, as referenced above, the *ex parte* seizures are limited and may only be instituted in "extraordinary circumstances." The DTSA also contains no language preempting other causes of action that may arise under the same common nucleus of facts of a trade secret claim, unlike the UTSA as interpreted by some states which preempt such claims.

Unlike the UTSA, the DTSA also provides protection to "whistleblowers who disclose trade secrets to law enforcement in confidence for the purpose of reporting or investigating a suspected violation of law," and the "confidential disclosure of a trade secret in a lawsuit, including an anti-retaliation proceeding."

With Passage of the DTSA, What Should An Employer or Business Do?

What is an employer or business to do if it wants to avail itself of this new law? What should employees now be apprised of? Here are some tips and strategies we believe will assist employers and business owners in complying with and taking full advantage of the relief available under the DTSA:

1. **Review:** Have qualified counsel review policies and relevant agreements to ensure that they contain language required under the DTSA, such as proper notice of the immunity provision referenced above. Additionally, ensure that your company is using non-disclosure agreements with your employees and that such agreements have clear definitions of trade secrets and confidential information and are not overly broad.
    1. Should you file suit under the DTSA if your agreement or policy does not contain the required immunity language? If you do not include the necessary immunity language in your employment or confidentiality agreements or policies, your company will not be able to avail itself of all the remedies under the DTSA. In other words, you will not be able to obtain attorney's fees or exemplary damages if you bring a suit under the DTSA.
    2. It is a good practice to include the required immunity language under the DTSA in your agreements and also have clear definitions of trade secrets and confidential information that are not overly broad given the government's enhanced scrutiny of overly broad confidentiality language, such as the NLRB, EEOC, and SEC.
2. **Ensure and Protect:** *Do you have valuable information that could be protected as a trade secret?* First, identify valuable sources of information in your organization. You should then check to see how your company protects such information. You will only be to pursue trade secrets claims if you can show that your company employs reasonable secrecy measures to protect its trade secrets. Check out one of our recent webinars discussing best practices for the proper treatment of trade secret information. We have found that a trade secret audit with the assistance of counsel can be valuable for companies trying to identify and protect their trade secrets.
3. **Prepare:** To pursue and avoid DTSA claims against your company, maintain proper on-boarding and off-boarding procedures and counsel your employees regarding the handling and further protection of your company's confidential and trade secret information, including recurring employee training. Also closely monitor relationships with vendors and contractors who may have access to your company's trade secrets and confidential information and ensure that there are appropriate protections in place.

It will be a brave new world with the passage of the DTSA. Federal courts will likely become the new forum for trade secret litigation. Make sure that your company is ready.

Further Information

Please visit our blog, Trading Secrets, for further coverage of the DTSA. We regularly update our page featuring DTSA developments, and we recently recorded a webinar and podcast featuring the most recent updates (as of April 11, 2016) to the DTSA. We are happy to discuss with you what the DTSA may mean for your company.

President Obama to Sign Defend Trade Secrets Act into Law

By Robert B. Milligan (May 11th, 2016)

Today, President Obama will sign into law the Defend Trade Secrets Act ("DTSA") in a public "pool spray" Oval Office ceremony. The final gathering is set to occur at 3:20 PM Eastern in the Brady Press Briefing Room. The President will sign the DTSA at 3:35 PM Eastern. Stay tuned for further coverage.

President Obama Signs the Defend Trade Secrets Act: Tips for Navigating the New Law

By Robert B. Milligan, Daniel P. Hart, and Amy Abeloff (May 11th, 2016)

Seyfarth Synopsis: *A new federal civil cause of action is now available to trade secrets owners seeking to pursue claims of trade secret misappropriation under the Defend Trade Secrets Act ("DTSA"). To take full advantage of the remedies provided under the DTSA, companies have an immediate obligation to provide certain disclosures in all non-disclosure agreements with employees, contractors, and consultants that are entered into or updated following today. Our post provides a brief history and summary of the DTSA, and, notably, provides business owners a list of tips and strategies to implement in light of the DTSA's passage.*

Today, President Obama signed into law the Defend Trade Secrets Act of 2016, which Congress passed on April 27.

What does the passage of the DTSA mean for your company? In a nutshell, it means your company can now pursue claims for trade secret misappropriation in federal court like other forms of intellectual property (i.e., patent, trademark, copyright) and seek remedies such as a seizure order to recover misappropriated trade secrets. It also serves as a reminder that trade secrets can be highly valuable to your company and that you should ensure that your company has identified such assets and put in place reasonable secrecy measures to protect them.

Below, we provide an overview of the DTSA's key provisions. We also provide tips and strategies in light of the passage of the DTSA.

What Does the DTSA Provide?

The DTSA authorizes a civil action in federal court for the misappropriation of trade secrets that are related to a product or service used in, or intended for use in, interstate or foreign commerce. Prior to the passage of the DTSA, civil trade secret claims were solely a matter of state law, with 48 states having adopted some version of the Uniform Trade Secrets Act ("UTSA") and the remaining states recognizing common law claims for misappropriation of trade secrets. While the DTSA does not displace these state law claims, it provides a federal civil claim above and beyond the state law claims that previously existed.

How Does the DTSA Work?

The DTSA creates a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act of 1996 ("EEA") to provide a federal civil remedy for trade secret misappropriation. The DTSA also provides pathways to injunctive relief, monetary damages, and other remedies in federal court for companies whose trade secrets are misappropriated, including via *ex parte* property seizures (subject to various limitations). Through the *ex parte* seizure provision, a plaintiff can seek to have the

government seize misappropriated trade secrets without providing notice to the alleged wrongdoer. The DTSA further harmonizes the differences in trade secret law under the UTSA and provides more uniform discovery procedures.

What Are the Significant Provisions of the DTSA?

The DTSA provides aggrieved parties with legal recourse in federal court via a federal trade secret cause of action (whereas previously, relief was only available under the state law UTSA or common law claims), as well as new remedies, including a seizure order. Below are the key provisions of the statute:

- The DTSA provides for actual damages, restitution, injunctive relief, significant exemplary relief (up to two times the award of actual damages), and attorney's fees.
- *Ex parte* property seizures are available to plaintiffs, but subject to limitations. As noted above, an *ex parte* seizure means that an aggrieved party can seek relief from the court against a party to seize misappropriated trade secrets without providing notice to the alleged wrongdoer beforehand. As a measure to curtail the potential abuse of such seizures, the DTSA prohibits copies to be made of seized property, and requires that *ex parte* orders provide specific instructions for law enforcement officers performing the seizure, such as when the seizure can take place and whether force may be used to access locked areas. Moreover, a party seeking an *ex parte* order must be able to establish that other equitable remedies, like a preliminary injunction, are inadequate.
- Injunctive relief for actual or threatened misappropriation of trade secrets is available in federal court. However, a court will not enjoin a person from entering into an employment relationship unless there is a showing through evidence of "threatened misappropriation and not merely on the information the person knows." This language was included in the DTSA to guard against plaintiffs pursuing "inevitable disclosure" claims.
- The statute of limitations is three years. A civil action may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered.
- A whistleblower immunity provision exists to protect individuals from criminal or civil liability for disclosing a trade secret if it is made in confidence to a government official, directly or indirectly, or to an attorney, and it is made for the purpose of reporting a violation of law. Similarly, a related provision states that an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding as long as the individual files any document containing the trade secret under seal and does not disclose the trade secret, except pursuant to court order.
- The immunity provision places an affirmative duty on employers to provide employees notice of the new immunity provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information." This notice provision applies to contracts and agreements that are entered into or updated after the date of DTSA's enactment (May 11, 2016).
- An employer will be in compliance with the notice requirement if the employer provides a "cross-reference" to a policy given to the relevant employees that lays out the reporting policy for suspected violations of law. Should an employer not comply with the above, the employer may not recover exemplary damages or attorney fees in an action brought under the DTSA against an employee to whom no notice was ever provided. Curiously, the definition of "employee" is drafted broadly to include contractor and consultant work done by an individual for an employer.

- The "Trade Secret Theft Enforcement" provision increases the penalties for a criminal violation of 18 U.S.C. § 1832 from $5,000,000 to the greater of $5,000,000 or three times the value of the stolen trade secrets to the organization, including the costs of reproducing the trade secrets.
- The DTSA further amends the RICO statute to add a violation of the Economic Espionage Act as a predicate act.

What Distinguishes the DTSA from the UTSA?

Because claims may still arise under states' varied versions of the UTSA , it is important to highlight the important ways in which the DTSA differs from the UTSA. Most notably, the DTSA opens the federal courts to plaintiffs in trade secrets cases. The DTSA also allows for an *ex parte* seizure order. A plaintiff concerned about the propagation or dissemination of its trade secrets would be able to take proactive steps to have the government seize misappropriated trade secrets prior to giving any notice of the lawsuit to the defendant.

Nevertheless, the *ex parte* seizure order is subject to important limitations that minimize interruption to the business operations of third parties, protect seized property from disclosure, and set a hearing date as soon as practicable. As referenced above, the *ex parte* seizures are limited and may only be instituted in "extraordinary circumstances."

The DTSA also contains no language preempting or displacing other causes of action that may arise under the same common nucleus of facts of a trade secret claim, unlike the UTSA as interpreted by some states which preempt such claims.

As also noted above, unlike the UTSA, the DTSA also provides protection to "whistleblowers who disclose trade secrets to law enforcement in confidence for the purpose of reporting or investigating a suspected violation of law," and the "confidential disclosure of a trade secret in a lawsuit, including an anti-retaliation proceeding."

Why Employers or Businesses Should Care and What They Should Do

Here are some tips and strategies we believe will assist employers and business owners in complying with and taking full advantage of the relief available under the DTSA:

1. **Update:** Starting immediately, all non-disclosure agreements with employees, contractors, and consultants that are entered into or updated following today must contain disclosures of the DTSA's immunity provisions (either set forth directly in the agreement or in a policy that is cross-referenced in the agreement). Employers who fail to provide these disclosures cannot recover exemplary damages or attorney fees in an action brought under the DTSA against an employee to whom no notice was provided. Consequently, employers should immediately update their standard agreements to include the required disclosure language. Remember that employee is broadly defined under the DTSA to include contractor and consultant work done by an individual for an employer.
2. **Review:** Have qualified counsel review policies and relevant agreements to ensure that they contain the required language noted above. Additionally, ensure that your company is using non-disclosure agreements with your employees and that such agreements have clear definitions of trade secrets and confidential information and are not overly broad.
3. **Ensure and Protect:** *Do you have valuable information that could be protected as a trade secret?* First, identify valuable sources of information in your organization. You should then check to see how your company protects such information. You will only be able to pursue

trade secrets claims if you can show that your company employs reasonable secrecy measures to protect its trade secrets. Check out one of our recent webinars discussing best practices for the proper treatment of trade secret information. We have found that a trade secret audit with the assistance of counsel can be valuable for companies trying to identify and protect their trade secrets.

4. **Prepare:** To protect your company's trade secrets and avoid DTSA claims against your company, maintain proper on-boarding and off-boarding procedures and counsel your employees regarding the handling and further protection of your company's confidential and trade secret information, including recurring employee training. Also closely monitor relationships with vendors and contractors who may have access to your company's trade secrets and confidential information and ensure that there are appropriate protections in place.

It will be a brave new world with the passage of the DTSA. Federal courts will likely become the new forum for trade secret litigation. Make sure that your company is ready.

Further Information

Please visit our blog, Trading Secrets, for further coverage of the DTSA. We regularly update our page featuring DTSA developments, and we recently recorded a webinar and podcast featuring coverage of the DTSA updates (as of April 11, 2016). We will also be hosting a webinar on Monday, May 16. The webinar will describe the key features of the DTSA and compare its key provisions to the state Uniform Trade Secrets Act ("UTSA") adopted in many states. The webinar will also provide practical tips and strategies concerning the pursuit and defense of trade secret cases in light of the DTSA, and provide some predictions concerning the future of trade secret litigation.

We are happy to discuss with you what the DTSA may mean for your company.

Webinar Recap! The Defend Trade Secrets Act: What Employers Should Know Now

By Robert B. Milligan, Daniel P. Hart, and Amy Abeloff (June 16th, 2016)

We are pleased to announce the webinar "The Defend Trade Secrets Act: What Employers Should Know Now" is now available as a podcast and webinar recording.

In Seyfarth's sixth installment, attorneys Robert Milligan, Daniel Hart and Amy Abeloff, described the key features of the Defend Trade Secrets Act ("DTSA") and compared its key provisions to the state Uniform Trade Secrets Act ("UTSA") adopted in many states. They also provided practical tips and strategies concerning the pursuit and defense of trade secret cases in light of the DTSA, the handling of employment relations, and provided some predictions concerning the future of trade secret litigation.

As a conclusion to this well-received webinar, we compiled a summary of three takeaways that were discussed during the webinar:

- The DTSA was passed after many failed attempts to pass trade secret legislation allowing for a federal cause of action for misappropriation. The bill was passed with overwhelming bipartisan, bicameral support, as well as backing from many significant companies in several business sectors. The DTSA now allows trade secret owners to sue in federal court for trade secret misappropriation, and seek remedies heretofore unavailable, including an *ex parte* seizure order.
- The DTSA contains an immunity provision that protects individuals from criminal or civil liability for disclosing a trade secret if such disclosure is made in confidence to a government official or attorney, indirectly or directly. The provision applies to those reporting violations of law or who file lawsuits alleging employer retaliation for reporting a suspected violation of law, subject to certain specifications (i.e., trade secret information to be used in a retaliation case must be filed under seal). The DTSA places an affirmative duty on employers to give employees notice of this provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information" that is entered into or updated after May 11, 2016. Employers that do not comply with this requirement lose the ability to recoup exemplary damages or attorney fees in an action brought under the DTSA.
- Though the passage of the DTSA creates a new federal cause of action for trade secret misappropriation, the passage does not render state law and state causes of action irrelevant or unimportant. The UTSA is still an available cause of action in 48 states, and state law still plays a vital role in drafting non-disclosure and non-competition agreements. Additionally, under the DTSA, employers may be able to seek injunctive relief against former employees in the event of misappropriation, but such injunctive restrictions must comport with relevant state law.

Federal Court Rejects Defend Trade Secrets Act Whistleblower Immunity Defense on a Motion to Dismiss and Orders Employee to Return Stolen Trade Secrets

By Erik Weibust, Andrew Stark, and Robert A. Fisher (December 19th, 2016)

This past Spring, we reported on the recently enacted Defend Trade Secrets Act ("DTSA"), which provides a new federal civil cause of action to trade secret owners seeking to pursue claims of trade secret misappropriation. Last week, the U.S. District Court in Massachusetts addressed the whistleblower immunity provision of the DTSA, which protects anyone who discloses a trade secret in confidence to a government official or an attorney "solely for the purpose of reporting or investigating a suspected violation of law." In denying an employee's motion to dismiss his employer's DTSA claim, the district court held that a defendant must present evidence to justify the immunity. The case is *Unum Group v. Loftus*, No. 16-cv-40154-TSH (D. Mass. December 6, 2016).

Summary of the Case

Timothy Loftus was employed by Unum Group as the Director of Individual Disability Insurance Benefits, which exposed him to a significant amount of confidential information, including Unum's trade secrets. In September 2016, Loftus was captured on video leaving Unum's office building with two boxes and a brief case. Two days later, Loftus was again captured on video exiting the office building with a shopping bag full of documents. When Unum investigated Loftus's removal of documents, he refused to cooperate, and was subsequently seen leaving the office with his company laptop and a full shopping bag.

After Unum made received only Loftus's laptop after numerous requests for both the laptop and documents, it filed suit in federal court under the DTSA and the Massachusetts Trade Secrets Act, and for conversion. Unum sought a preliminary injunction to enjoin Loftus from copying the documents, and to compel him to return all of the documents and make a mirror-image copy of the laptop as they had previously agreed. Unum claimed that it was highly likely that the documents that Loftus took contain confidential customer and employee information and/or trade secrets, including protected health insurance information.

Loftus moved to dismiss Unum's federal and state law claims for trade secret misappropriation on the grounds that he had turned over the documents that he removed from Unum to his attorney to report and investigate a violation of law, invoking the whistleblower immunity provision of the DTSA, 18 U.S.C. § 1833(b).

The district court deemed Loftus's DTSA immunity defense an affirmative defense and stated that, as a general rule, a properly raised affirmative defense can only be decided at the motion to dismiss stage if "the facts establishing the defense are definitively ascertainable from the complaint and the other allowable sources of information," such as public records that the court can take judicial notice of and "those facts suffice to establish the affirmative defense with certitude." Upon examining the complaint, the court denied Loftus's motion to dismiss, holding that "the record lacks facts to support or reject his affirmative defense at this stage of litigation. There has been no discovery to determine the significance of the documents taken or their contents and Loftus has not filed any potential lawsuit that could be supported by information in those documents" of which the court could take judicial notice. The court further stated that "it is not ascertainable from the complaint whether Loftus turned over *all* of Unum's documents to his attorney, which documents he took and what information they contained, or whether he used, is using, or plans to use, those documents for any purpose other than investigating a potential violation of law. Taking all facts in the complaint as true, and making all reasonable inferences in favor of Unum, the court finds the complaint states a plausible claim for trade secret misappropriation and declines to dismiss Counts I and II."

The court then weighed the factors presented by Unum regarding Loftus's conversion of its documents, including Loftus's concession at the hearing that Unum has stated a colorable claim for conversion, and granted the motion for preliminary injunction. Among other things, the court ordered Loftus and his attorney to return all of the removed documents and destroy all copies made. The court found that the conversion claim alone is sufficient to warrant the injunction that Unum sought and did not address the merits of its trade secret misappropriation claim.

Trade Secrets

Charities Take Note: Ninth Circuit Reaffirms CA Attorney General's Entitlement to Sensitive Donor List

By Seyfarth Shaw LLP (January 15th, 2016)

With an apparent thumbs up from the U.S. Supreme Court, the Ninth Circuit Court of Appeals[1] once again upheld the position of the California Attorney General (AG) requiring that charities located or operating in California must provide a copy of their unredacted Form 990 Schedule B, including the names, addresses and contribution amounts for all donors listed.[2] While the court has preliminarily prevented the AG from making the information publicly available, the ruling is unwelcome news for charities concerned about protecting donors' identities. The collection of sensitive donor information from charities appears to be a growing trend by state Attorneys General.

Affected charities, including out-of-state charities soliciting or otherwise operating in California, should review their donor confidentiality policies and disclosures to ensure that their donors are aware of such requirements.

Regulation of Charities Located or Operating in California

Most California charities and certain out-of-state charities are required to register and file an annual report (Form RRF-1) with the AG's Registry of Charitable Trusts. Religious organizations, educational institutions, hospitals and health care service plans are exempt from this registration and reporting.

A copy of the charity's annual information return (Form 990 or Form 990-EZ) must be included with the annual report. The AG recently began treating annual reports submitted without Schedule B (or with a redacted Schedule B) as incomplete. Failure to file a complete report generally results in penalties, fees and the loss of California income tax exemption.

Several states, including New York, have a similar filing requirement. Both the California and New York AGs note that it is not their policy to disclose Schedule B to the public. In fact, in December of 2015, the California AG proposed amendments to state regulations to provide that donor information exempt from public inspection pursuant to the Internal Revenue Code will be maintained as confidential by the AG subject to certain limited exceptions.[3]

However, there is no guarantee that such disclosure policies (whether codified or not) will not change in the future and it is unclear if the donor information, once in the possession of a state attorney general, would be subject to a request for disclosure under that state's public records act.

Schedule B – Donor Disclosure

Schedule B to the Form 990 is used to disclose to the IRS the reporting organization's significant donors (generally those who contribute over $5,000 in cash or property), including their names, addresses, and contribution amounts. Tax-exempt organizations are generally required to make available for public inspection and copying their three most recent annual returns, including copies of all schedules, attachments and supporting documents filed with these returns. Most such returns are posted and publicly available at no cost on third-party websites, such as Guidestar.org.

However, except for private foundations (Form 990-PF filers) and section 527 political organizations, public disclosure of the names and addresses of contributors set forth on Schedule B generally is not required, and the Schedules B of those organizations typically do not appear when posted online.

Center for Competitive Politics v. Harris

In an earlier case, Center for Competitive Politics, a Virginia nonprofit registered with the California AG, challenged the AG's unredacted Schedule B filing requirement. It argued that the disclosure violates its and its supporters' First Amendment rights to freedom of association and that certain nondisclosure rules under federal law preempt the state requirement.

The U.S. Court of Appeals for the Ninth Circuit rejected the Center's arguments, concluding that the disclosure requirement bears a substantial relation to a sufficiently important government interest and is facially constitutional, and the U.S. Supreme Court denied the Center's petition for the case to be reviewed.[4]

However, the Ninth Circuit left open the possibility that a future litigant could show a reasonable probability that the compelled disclosure of its contributors' names will subject them to threats, harassment or reprisals that would warrant relief on an "as-applied" challenge.

Americans for Prosperity Foundation v. Harris

Two nonprofits, Americans for Prosperity Foundation and Thomas More Law Center, brought such a challenge, resulting in preliminary injunctions issued by the Federal District Court prohibiting the AG from demanding the plaintiffs' unredacted Schedules B.

The plaintiffs argued that confidential disclosure to the AG itself chills protected conduct or would lead to persecution and harassment of their donors by the state or the public. Second, they argued that, notwithstanding the AG's voluntary policy against disclosing Schedule B forms to the public, the AG may change its policy or be compelled to release the forms under state law, and that the resulting public disclosure would lead to harassment of their donors by the public, chilling protected conduct.

However, the Ninth Circuit vacated the injunctions and rejected the plaintiffs' arguments.[5] The Court noted that neither plaintiff had shown anything more than broad allegations or subjective fears that *confidential* disclosure to the AG would chill participation or result in harassment of its donors by the state or the public. Neither plaintiff was able to show to the Court's satisfaction that the disclosure had actually chilled protected conduct or would be likely to do so, or that there was a reasonable probability of harassment at the hands of the state or the public due to such disclosure.

The Court did, however, issue a new injunction preventing the AG from publicly disclosing the Schedule B information, consistent with the AG's stated position and the proposed regulations.

This decision, upholding the AG's confidential disclosure requirements, coupled with the AG's recent proposal to amend state regulations to generally prohibit the AG's disclosure of Schedule B information, appears to close the book on any new confidentiality exceptions to California's filing requirement. It would seem unlikely for the U.S. Supreme Court to agree to review the *Americans for Prosperity Foundation* case after having declined a review of the *Center for Competitive Politics* case.

Conclusion

These court decisions exemplify what we expect to be a growing trend by state Attorneys General to demand sensitive donor information from charities operating or soliciting in those states. Charities should continue to heed the Schedule B instructions and not include Schedule B in filings with states that do not specifically require it, as those states may inadvertently disclose the charity's donor information to the public.[6]

In addition, out-of-state charities that are (1) "doing business" in California for charitable purposes or (2) "holding property" in California, and are not currently registered with the AG's Registry of Charitable Trusts, may wish to consider contacting local counsel for advice regarding their California operations to avoid or minimize potential penalties.[7]

[1] *Americans for Prosperity Foundation v. Harris*, No. 15-55446 (9th Cir. Dec. 29, 2015).

[2] For our prior article on this subject matter, please visit http://www.seyfarth.com/publications/CA060115-TEO.

[3] The AG has proposed to amend sections 310 and 999.1 of the California Code of Regulations Title 11, Division 1. The text of the proposed amendments and related materials may be found on the AG's website: http://oag.ca.gov/charities/notice-prop-amend-regs.

[4] *Center for Competitive Politics v. Harris*, No. 14-15978 (9th Cir. May 1, 2015), cert. denied (November 9, 2015).

[5] *Americans for Prosperity Foundation v. Harris*, No. 15-55446 (9th Cir. Dec. 29, 2015).

[6] Schedule B, Page 5 (General Instructions: Public Inspection), available at http://www.irs.gov/pub/irs-pdf/f990ezb.pdf.

[7] For a detailed discussion of California requirements that extend to out-of-state charities, see Mancino, "California Regulation of Out-of-State Charities," 17 Taxation of Exempts 6 (May/June 2006).

Oil-And-Gas Services Companies Argue Over Trial Court's Authority to Exclude Corporate Representatives Under New Texas Trade Secret Law

By Jesse M. Coleman (January 19th, 2016)

On January 13, before the Texas Supreme Court, two major oil-and-gas-services companies disputed whether Texas's new trade secret laws require a trial court to exclude a party's corporate representative from a hearing at which trade-secret testimony from the opposing party is given.

Jeff Russo is a former employee of M-I SWACO, a Schlumberger subsidiary, who left to work for National Oilfield Varco (NOV) in early 2014. Russo filed suit against in April 2014, seeking a declaratory judgment on his non-compete agreement. M-I SWACO counterclaimed for breach of contract and misappropriation of trade secrets and further sued NOV as a defendant. The parties entered into an agreed protective order and engaged in expedited discovery.

At a temporary injunction hearing, M-I SWACO sought to present evidence of its trade secrets through oral testimony and asked the trial court to temporarily clear the courtroom of everyone except the parties' counsel, their experts, and Russo. The trial court denied the request, stating "I am not going to exclude a representative of a party that you're making claims against from [the courtroom]," and adding that it would be "a total violation of due process." To protect M-I SWACO's alleged secrets, the trial court instead issued a gag order for NOV's representative prohibiting disclosure or use of anything heard in the courtroom. This mandamus followed.

At issue in the appeal is the trial court's authority under the newly-enacted Texas Uniform Trade Secrets Act (TUTSA) to "preserve the secrecy of an alleged trade secret by reasonable means." Tex. Civ. Prac. & Rem. Code §134A.006.

M-I SWACO argued that, in order to preserve the secrecy of its trade secrets, "reasonable means" required in this case disclosing the alleged secrets in the presence of NOV's attorneys and experts, and in front of Russo, but not in front of NOV itself. The trial court's order, M-I SWACO argued, "created a needless dilemma" in which, "one way or the other," NOV would be given access to M-I SWACO's trade secrets through NOV's corporate representative.

NOV argued, however, that the trial court's gag order directed at NOV's corporate representative is sufficient protection for the alleged trade secrets, and that TUTSA permits nothing more. "Not only does TUTSA not authorize the relief M-I SWACO seeks, it expressly authorizes courts to issue the relief the trial court ordered here," NOV argued in its brief. "Although that is not exactly what M-I SWACO wanted, it cannot constitute an abuse of discretion as a matter of law."

At oral argument before the Texas Supreme Court, M-I SWACO's counsel argued that there would be times when a gag order such as the one the trial court entered in this place would be appropriate, but only in those situations where the competitor already knew the trade secret.

NOV's counsel argued at the hearing, however, that excluding the defendant from the court room during the hearing would constitute a radical departure from the American processes of jurisprudence.

TUTSA became effective in Texas on September 1, 2013. The parties appeared to agree that the matter before the Texas Supreme Court was a matter of first impression.

The parties briefs before the Texas Supreme Court can be accessed here.

Access to the oral hearing can be found here.

Webinar Recap! Data Security & Trade Secret Protection for Lawyers

By Richard Lutkus and James Yu (March 8th, 2016)

We are pleased to announce the webinar "Data Security & Trade Secret Protection for Lawyers" is now available as a podcast and webinar recording.

In the second installment, Seyfarth attorneys, Richard D. Lutkus and James S. Yu, was joined by Joseph Martinez, Chief Technology Officer and Vice President of Forensics at Innovative Discovery. This program covered considerations that attorneys should take into account when in possession of any client data. Coverage included both technical considerations, best practices and policies, as well as practical advice to steer clear of ethical violations.

As a conclusion to this well-received webinar, we compiled a list of brief summaries of the more significant cases that were discussed during the webinar:

- Whether corporate or outside counsel, there are basic steps that can dramatically increase the security of your or your client's data. Management of data will continue to be a necessity for any entity. Proper policies, protocols, and training should be developed and put into place to protect data in transit and at rest. Use of encryption and access control are both key to proper protection of data.

- Social engineering is the number one cause of data breaches, leaks, and information theft. Organizations should alert and train employees on following policy, spotting potential social engineering attacks, and having a clear method to escalate potential security risks. Employee awareness, coupled with technological changes towards better security will reduce risk and exposure to liability.

- Lawyers have an ethical duty to ensure that reasonable steps are taken to protect their client's and employer's data. Significant statistics have shown that many law firms and practitioners are behind the curve in terms of information security preparedness. Hackers have recently focused their targets on the lax security practices of law firms to obtain client data or inside information.

Webinar Recap! New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive

By Robert B. Milligan, Justin K. Beyer, and Daniel P. Hart (April 11th, 2016)

We are pleased to announce the webinar "New Year, New Progress: 2016 Update on Defend Trade Secrets Act & EU Directive" is now available as a podcast and webinar recording.

In Seyfarth's third installment of its 2016 Trade Secrets Webinar series, Seyfarth attorneys Robert Milligan, Justin Beyer, and Daniel Hart, provided attendees with a thorough discussion of the fundamentals as well as latest updates on the Defend Trade Secrets Act and the proposed EU Trade Secrets Directive. The panel gave insight into the limitations and benefits of the Act and the proposed Directive.

Below are three takeaways from the well-received webinar:

- With the passage of the Defend Trade Secrets Act, there is now a federal cause of action for trade secrets disapproval. Some of the key provisions in the Act include a three year statute of limitations, the availability of attorneys' fees, exemplary damages, as well as increased criminal penalties for a violation of the Economic Espionage Act. It also includes portions of the DTSA as predicate offenses for the RICO Act.

- The Act also contains language requiring that an employer include information relating to whistleblower immunity for employers to obtain exemplary damages. This only underscores an important point to anyone maintaining employment agreements which contain restrictive covenants: it is imperative for employers to monitor applicable state and federal law to best preserve and maintain their rights and employment agreements.

- The European Commission's directive on trade secret protection will mark a sea-change in protection of trade secrets throughout the European Union. Each of the EU's 28 member states will have a period of 24 months to enact national laws that provide at least the minimum levels of protections afforded to trade secrets by the directive. Look for greater consistency in trade secrets protection throughout the European Union in the years ahead.

Webinar Recap: Protecting Confidential Information and Client Relationships in the Financial Services Industry

By J. Scott Humphrey, Marcus Mintz, and Kristine Argentine (May 5th, 2016)

We are pleased to announce the webinar "Protecting Confidential Information and Client Relationships in the Financial Services Industry" is now available as a podcast and webinar recording.

Seyfarth's fourth installment, presented by Scott Humphrey, Marcus Mintz, and Kristine Argentine, focused on trade secret and client relationship considerations in the banking and finance industry, with a particular focus on a firm's relationship with its FINRA members.

As a conclusion to this well-received webinar, we compiled a list of takeaways:

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

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

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

Drones & Trade Secrets – How Low Can They Go?

By Wayne Bond (May 9th, 2016)

This Blog first addressed the threats drones pose to the protection of Trade Secrets in June of 2014.[1] Since then, drones continue to proliferate at a dizzying pace. Everybody and their brother has one, and drones are becoming much more sophisticated and advanced. [2] The challenge is for the law to keep up with the technology, and so far, the law has not done a very good job.

In many ways, the challenge to protect trade secrets from drones is similar to the challenge to comply with legal data privacy obligations. In both situations, bad guys keep coming up with new ways to invade privacy and misappropriate secrets. The legal obligations remain generally the same, but the playing field keeps changing as technology advances.

For data privacy, there is no clear federal law,[3] but state laws frequently use language such as "reasonable security procedures and practices to protect the information from unauthorized access." For trade secrets, the legal standard is found in the Uniform Trade Secrets Act (UTSA) adopted by 48 states[4] and there should soon a federal version with the Defend Trade Secrets Act of 2016 (DTSA).[5] The UTSA says two things relevant to drones. In order to be a trade secret, the information must not be publicly available, and a business must take reasonable steps to keep the information confidential.

Trade secrets are only protected as long as they remain secret. If a trade secret becomes known, it is like trying to push toothpaste back into the tube — you can't do it. All you can do is seek legal recourse. But in order to be successful in seeking such recourse, you must be able to show the information was not "publicly available" and you took "reasonable steps" to keep your secrets secret.

This leads us back to drones. In law school, we learned the common law principle of "*ad coelum*," which says property rights extend vertically up and down.[6] Aviation changed upward vertical rights (a landowner's rights no longer extend to the "heavens"), but it is still not clear where they stop. In 1946, the U.S. Supreme Court declared airspace is now a "public highway," but consistently flying noisy planes 83 feet above a chicken farm can be an unlawful taking of property.[7] In 1970, the 5th Circuit held DuPont didn't voluntarily disclose its trade secrets to someone spying via aerial photography on a methanol plant that was under construction.[8] It has been a long time since these two cases were decided, and there has been very little case law on these issues since then. How relevant are these cases today in the age of modern drone technology when the standard for protecting trade secrets is "reasonable"?

Federal law remains unclear regarding the height at which a landowner can express exclusive dominion. Some have advocated that landowners should be allowed to exclude drones from airspace above their land up to a height of 500 feet.[9] State laws are starting to come out and they naturally vary,[10] while states are taking a wait-and-see approach. New legislation has been proposed to protect privacy rights,[11] and much has been written about Fourth Amendment ramifications and our "reasonable expectation of privacy,"[12] but how does this impact business owners and their trade secrets? What can a business do to protect its trade secrets in an increasingly invasive drone age?

Indeed what *must* a business do to protect its legal right to claim its confidential information is a trade secret at all.

And what if the drone is flying really low? What if the drone is just outside your office window? Does it matter if your office is ground level or on the 25th floor?

Rapidly advancing drone technology changes things for business owners. While satellites with sophisticated cameras can read the screen on a laptop while the user is sitting on a park bench, satellites with this capability are not in the hands of the typical business competitor — at least not yet — but drones are.

So what reasonable steps must businesses take to protect their trade secrets from drones?

As tempting as it may be,[13] shooting drones down is not a good option. Federal law makes it a crime to destroy a civil aircraft , and there are several reports of state and local criminal charges being filed against property owners who shot at drones like they were sporting clays.[14]

Signal jamming is one possibility.[15] The Secret Service started experimenting with this after a drone crashed on the White House lawn.[16] However, this presents legal problems for private citizens since federal law prohibits using jamming equipment that interferes with cellular services, police radar, and GPS, and Wi-Fi.[17]

Geo Fencing is another option. Airports increased their research in this area after a drone recently collided with a passenger plane landing at Heathrow Airport outside London.[18] This technology prevents drones from flying over geographic locations by blocking the GPS coordinates. But this only affects drones that need GPS equipment to operate. It won't prevent someone from flying by line of sight.

Other technologies include sophisticated listening equipment able to detect and locate drones based on the sounds they make. Specialized radar technology is being tested that works differently from standard radar which has difficulty spotting slow-moving objects. Drone spoofing is a technology that involves sending fake GPS signals to the drone. Hijacking (or "skyjacking") drones involves taking over their navigational control systems. One company is even experimenting with security drones that are able to capture spy drones in nets that dangle from the security drones.[19] Drones armed with "net guns" were used during last year's Boston Marathon to capture any drones violating an airspace ban along the race course.[20]

Basic window covering should also be examined. While many states have "Peeping Tom" laws that make it illegal to look in windows, their applicability to drones spying on places of business is largely untested. In the new drone landscape, businesses should consider blocking all visibility through windows to interior spaces where confidential information exists and might be viewed with powerful new cameras — especially now that drones can bring those powerful new cameras even closer.

Finally, consider whether "good" drones should be used to proactively protect trade secrets, instead of just worrying about defending against "bad" drones controlled by competitors. Good drones could be effective enhancements to traditional surveillance systems already being used by businesses concerned about protecting their trade secrets.

Businesses must strike a balance between getting work done freely without restrictions and doing what is necessary to protect company secrets. Make sure your next trade secret audit includes the exposures created by modern drone technology and reasonable countermeasures available to

minimize such exposure, while also considering proactive ways drones might be used to enhance a business' overall security.

[1] See "Josh Salinas Explains How Drones Could Pose a Threat to the Protection of Trade Secrets"

[2] See, e.g., New announcements such as wearable cameras that can fly to take selfies, and the proliferation of indoor drones.

[3] There is no comprehensive federal law providing a uniform compliance standard for information security best practices. U.S. businesses must comply with 47 different states' laws governing such issues.

[4] The UTSA, published by the Uniform Law Commission (ULC) and amended in 1985, was recently adopted by Texas, which became the 48th state to enact some version of the UTSA. New York and Massachusetts are the only states that have not enacted the UTSA.

[5] Congress passed the Defend Trade Secrets Act of 2016 in April. The DTSA has strong bipartisan support, and President Obama has indicated he will sign it into law.

[6] Taken from the *Latin Cuius est solum eius est usque ad coelum (et ad inferos)* meaning "for whoever owns the soil, it is theirs up to Heaven (and down to Hell)."

[7] *United States v. Causby*, 328 U.S. 260 (1946).

[8] *E.I. DuPont deNemours & Co. V. Christopher*, 431 F.2d 1012 (5th Cir. 1970)

[9] Rule, T. A. (2015). Airspace in an Age of Drones. *Boston University Law Review*, 95(1), 155-208, at p. 159

[10] E.g., Nevada prohibits drones from flying less than 250 feet.

[11] E.g., Sen. Edward Markey (D-MA) is pushing legislation known as the Drone Aircraft Privacy and Transparency Act.

[12] See, e.g., Matiteyahu, Taly, (2015). Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy, *Columbia Journal of Law and Social Problems*, 48, 265-308.

[13] The Colorado town of Deer Trail made national headlines when it called for a vote on issuing hunting licenses for drones.

[14] See, e.g., http://www.cnn.com/2015/09/09/opinions/schneier-shoot-down-drones/

[15] See, e.g., http://makezine.com/2015/10/16/research-company-takes-aim-uavs-portable-anti-drone-rifle/

[16] See http://www.popsci.com/secret-service-tries-jamming-drone-signals-near-white-house

[17] See https://www.fcc.gov/general/jammer-enforcement

[18] See https://www.theguardian.com/technology/2016/apr/18/drones-government-labour-ba-rules-drones-heathrow-incident

[19] See “Copping a ‘copter” in the May 2, 2015 issue of *The Economist*

[20] https://www.bostonglobe.com/metro/2015/04/21/boston-marathon-drone-detection-firm-brought-net-guns/2oSp9Brfn5rFOIYqRJmP3H/story.html

Texas Supreme Court: Company Representative May Be Excluded from Trade Secret Hearing

By Jesse M. Coleman (May 31st, 2016)

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

A former employee of M-I L.L.C. ("M-I"), a Schlumberger subsidiary, left to work for National Oilfield Varco (NOV) in early 2014. The employee then filed suit against NOV in April 2014, seeking a declaratory judgment on his non-compete agreement. M-I counterclaimed for breach of contract and misappropriation of trade secrets and further sued NOV as a defendant.

At a temporary injunction where M-I sought to present evidence through oral testimony of its purported trade secrets, M-I asked the trial court to exclude from the courtroom NOV's designated representative. The trial court categorically denied this request, concluding that it would be a denial of due process to prohibit the representative from attending. The Court of Appeals then denied M-I's writ of mandamus.

The Texas Supreme Court held, however, that the trial court failed to conduct the necessary due-process analysis balancing NOV's right to have its representative attend the hearing and M-I's right to protect its trade secrets from someone who could have been a competitive decision-maker at NOV. Specifically, the Court held that the balancing test required the trial court to determine, e.g.,

- the degree of competitive harm M-I would have suffered from the dissemination of its alleged trade secrets to NOV's representative; and
- the degree to which NOV's defense of M-I's claims would be impaired by the representative's exclusion.

This analysis may ultimately result in permitting NOV's representative to attend the hearing, the Court stated, but the failure of the trial court to conduct any such analysis constituted an abuse of discretion.

The Court further concluded that TUTSA allows a trial court to exclude a company representative from portions of the hearing where trade secrets are being discussed. Specifically, the Court held the provision of the statute allowing for "in camera hearings" should be interpreted as proceedings where a party or its representatives may be excluded, such as the injunction hearing at issue. Tex. Civ. Prac. & Rem. Code §134A.006. This interpretation, the Court concluded, was appropriate because "it best gives effect to [TUTSA's] directive to take reasonable measures to protect trade secrets, and its

express authorization for protective orders with provisions 'limiting access to confidential information to only the attorneys and their experts.'"

Interestingly, the Court also noted that when conducting the balancing due-process test regarding NOV's corporate representative, the trial court must consider that "even when acting in good faith, [the representative] could not resist acting on what he may learn." In support of this position, the Court cited to a federal case from the Court of Appeals for the D.C. Circuit which held that "it is very hard for the human mind to compartmentalize and selectively suppress information once learned, no matter how well-intentioned the effort may be to do so." *FTC v. Exxon Corp.*, 636 F.2d 1336, 1350 (D.C. Cir. 1980). This analysis appears to lend support to interpreting TUTSA to adopting in some form the "inevitable disclosure" doctrine, which has not been otherwise officially recognized in Texas. This doctrine generally holds that a former employer is entitled to enjoin a former employee if the new employment would result in "inevitable disclosure" of confidential information.[1]

TUTSA became effective in Texas on September 1, 2013.

[1] *See, e.g.,* Harell, Alex, *Is Anything Inevitable? The Impending Clash between the Inevitable Disclosure Doctrine and the Covenants Not to Compete Act*, 76 Tex. B.J. 757 (2013).

When Stealing in Baseball Can Land You in Jail: Computer Fraud Sentencing Announced in MLB Case

By Erik Weibust (July 20th, 2016)

Although stealing bases, and even signs, in baseball may be part of the game, stealing another team's trade secrets can land you in federal prison, as one executive recently learned the hard way.

As we previously reported, the FBI has been investigating the St. Louis Cardinals for hacking into the Houston Astros' internal computer network and stealing proprietary information, including internal discussions about trades, proprietary statistics, and scouting reports. The investigation has now concluded, the Cardinals' former director of baseball development, Chris Correa, pleaded guilty to five counts of unauthorized access of a protected computer in January, and he has now been sentenced to 46 months in federal prison. He also must pay $279,038 in restitution. According to NPR, "U.S. District Judge Lynn Hughes, as she sentenced Correa, noted that the crime has resulted in stricter security at other baseball teams, according to a press release from the Justice Department. When Correa apologized and called his actions 'reckless,' [Judge] Hughes replied, 'No, you intentionally and knowingly did these acts.'"

As the Department of Justice reported at the time of Correa's plea:

The plea agreement details a selection of instances in which Correa unlawfully accessed the Astros' computers. For example, during 2013, he was able to access scout rankings of every player eligible for the draft. He also viewed, among other things, an Astros weekly digest page which described the performance and injuries of prospects who the Astros were considering, and a regional scout's estimates of prospects' peak rise and the bonus he proposed be offered. He also viewed the team's scouting crosscheck page, which listed prospects seen by higher level scouts. During the June 2013 amateur draft, he intruded into that account again and viewed information on players who had not yet been drafted as well as several players drafted by the Astros and other teams.

Correa later intruded into that account during the July 31, 2013, trade deadline and viewed notes of Astros' trade discussions with other teams.

Another set of intrusions occurred in March 2014. The Astros reacted by implementing security precautions to include the actual Ground Control website address (URL) and required all users to change their passwords to more complex passwords. The team also reset all Ground Control passwords to a more complex default password and quickly e mailed the new default password and the new URL to all Ground Control users.

Shortly thereafter, Correa illegally accessed the aforementioned person's e mail account and found the e mails that contained Ground Control's new URL and the newly-reset password for all users. A few

minutes later, Correa used this information to access another person's Ground Control account without authorization. There, he viewed a total of 118 webpages including lists ranking the players whom Astros scouts desired in the upcoming draft, summaries of scouting evaluations and summaries of college players identified by the Astros' analytics department as top performers.

On two more occasions, he again illicitly accessed that account and viewed confidential information such as projects the analytics department was researching, notes of Astros' trade discussions with other Major League Baseball teams and reports of players in the Astros' system and their development.

The parties agreed that Correa masked his identity, his location and the type of device that he used, and that the total intended loss for all of the intrusions is approximately $1.7 million.

Michael McCann provides a good analysis of the sentence for Sports Illustrated and describes potential penalties Major League Baseball may pursue against the Cardinals.

Federal Precedents Under the DTSA Have Arrived

By Kevin Mahoney (August 1st, 2016)

While the Defend Trade Secrets Act of 2016 ("DTSA") has only been in effect for a few months, the first wave of cases raising DTSA claims have started to generate federal decisions. In what appears to be the first substantive ruling under the Act, the Northern District of California illustrated some the advantages – and limitations – of DTSA claims in the context of injunctive relief.

Henry Schein, Inc. ("HSI"), a manufacturer of medical, dental and veterinary supplies, sued its former employee, Jennifer Cook, under the DTSA and a host of other California state law claims. *Henry Schein, Inc. v. Cook*, 16-cv-03166-JST (N.D. Cal.). Cook, a former sales associate, is alleged to have taken HSI's trade secrets (including customer information) to her new employer, a competing dental supply company, despite her confidentiality agreements with HSI. HSI sought a temporary restraining order and, later, a preliminary injunction under both the DTSA and California state law claims. The court entered a temporary restraining order and preliminary injunction prohibiting Cook from disclosing HSI's trade secrets to her new employer, but refused to enter a preliminary injunction that would prevent Cook from contacting or doing business with her former HSI customers in light of California's policy against non-compete agreements.

Perhaps the most striking aspect of the court's ruling was ultimately how little effect the DTSA had upon it. The DTSA has been widely viewed as an avenue for plaintiffs to bring trade secret claims in federal court, but HSI already had diversity jurisdiction for its state law claims and, as noted by the Court, HSI's California Uniform Trade Secrets Act claims closely mirror those brought under the DTSA. In other words, HSI could have brought its state law trade secret misappropriation claims against Cook in federal court even if the case had been filed before the passage of the DTSA, with little impact upon the court's ruling. The Court noted at several points, in both the TRO and PI orders, the similarities between the DTSA and California's Uniform Trade Secrets Act, and considered HSI's claims under both statutes without distinguishing between the two.

The court's rulings also serve as a reminder that the DTSA does not supplant state law concerning the enforceability of non-compete agreements. California's longstanding adverse treatment of non-compete agreements was the basis for the court's refusal to enjoin Cook from "contracting or doing business with her clients," especially when HSI had failed to show "specific evidence that Cook was utilizing trade secret information to solicit customers." While not the explicit basis for the court's ruling, the DTSA requires "evidence of threatened misappropriation," and not merely a showing that the individual has information in their possession, before the issuance of an injunction under the Act. 18 U.S.C. § 1836(b)(3)(A)(i)(I).

While the court's decision in *HSI* may not go into great detail in its consideration of the DTSA, it is worth noting why the court did not have to do so. DTSA claims will, in many cases, closely track claims under state law. The plaintiff in HSI already had an avenue to federal court based on the complete diversity of the parties, but other litigants will undoubtedly have to rely on the DTSA as their basis for

federal jurisdiction. The DTSA's most striking feature – its ex parte seizure provision – remains untested in federal court.

We Traced The Trade Secret Leak … It's Coming From Inside The Business

By James D. McNairy and Michael Cross (August 3rd, 2016)

Cross Posted from California Peculiarities.

Seyfarth Synopsis: *Protecting trade secrets from employee theft requires more than using an NDA when onboarding employees. If businesses want to protect confidential information, they need a cradle-to-grave approach, reiterating employee obligations regularly, including during exit interviews. (Yes, you need to do exit interviews!)*

Headline stories in intellectual property theft tend to involve foreign hackers engaged in high-tech attacks to pilfer vast troves of data stored by big businesses or government entities, such as those involving Russian government hackers or the Chinese military. The losses are staggering. In 2009, McAfee estimated that cybercrime cost worldwide economies $1 Trillion. That number was cited by (a then-youthful) President Obama in his first speech on cybersecurity. Since that time, attacks by professionals and nation states have remained at the forefront of both news reports and the public perception. Since then, hack attacks have remained at the forefront of both news reports and the public perception.

But despite the disproportionate attention given to high value, high-tech attacks by outsiders, many U.S. businesses recognize that threats from the inside are just as costly as revealed by a 2014 PricewaterhouseCoopers survey. Nevertheless, "only 49%" of organizations surveyed had "a plan for responding to insider threats."

Trade secrets are particularly susceptible to theft because they, by definition, consist of secret information with economic value. Company insiders often find that information too tempting to be leave behind when changing employers, or when seeking new employment. Therein lies the problem.

Trade secret theft by employees may not grab as many headlines as neo-Cold War espionage, but the data suggest that employees, not outsiders, pose the greatest threat of loss from trade secret theft. The good news is that a little proactivity by employers will go a long way toward keeping them out of the 49% who lack a plan to prevent leaks.

Of course, in California, obtaining protection is not all that simple. Non-compete agreements are, with very limited exceptions, a non-starter under Business and Professions Code § 16600, so you need special steps to keep your trade secret house in order. And because a California trade secret plaintiff (e.g., a former employer suing its former employee) likely must identify its trade secrets with reasonable particularity before commencing discovery, it pays to invest time on the front end to identify and inventory your trade secret information before litigation arises.

So, what *can* employers do?

Update Non-Disclosure Agreements to Comply With the DTSA, and See That Employees Know Why NDAs Are Important

Almost all employers (we hope) have confidential/non-disclosure and trade secret protection provisions in their employment agreements. But have these agreements been updated to comply with the recently

enacted Defend Trade Secrets Act ("DTSA") and its important employee/whistleblower notification provisions? And what are employers doing to help ensure compliance with their agreements? Rolling out new agreements is relatively easy. Making sure they are effective takes some doing.

Remember, your organization will not even have trade secrets to protect unless it has made "efforts reasonable under the circumstances" (under the California Uniform Trade Secrets Act) or has taken "reasonable measures" (under the DTSA) to maintain the secrecy of the information it claims to be a trade secret. Cal. Civ. Code § 3426.1(d); 18 U.S.C. § 1839(3)(A).

Implement Computer Use and Social Media Agreements and Policies

Most trade secret theft occurs via electronic device. Make sure your company has computer use and access policies and agreements that:

- Set forth that company computers, network, related devices, and information stored therein belong to the company;
- Indicate that access to company computers and networks are password-protected, with access authorized only for work-related purposes;
- Make use of data storage/access hierarchies, with the most valuable information being accessible on only a need-to-know basis, with security access redundancies (housed in a highly secure database that requires unique user credentials distinct from the log-in credentials the employee uses to access a computer workstation);
- Identify which devices are allowed in the workplace—BYOD practices have become popular, but also present challenges in regulating information flow and return. If employees use their own devices to perform work for the company, make clear that the company data on those devices belong to the company;
- Notify employees that the company reserves the right to inspect devices used for work to ensure that no company data exist on the devices upon termination of employment;
- Define whether cloud storage may be used by employees, under what terms, and what happens when employment ends;
- Define whether external storage devices (e.g., thumb drives) are allowed and under what terms; and
- Identify whether and how employees may use social media associated with their work—trade secrets must never be publicly disclosed, but beware of any overreach that would suppress employee communications protected by the National Labor Relations Act.

Build a Culture of Confidentiality—Make Sure Employees Know What The Company Regards as Confidential and Then Remind Them Routinely

Employees need to understand what information your company considers confidential. Educating employees on this subject should start at the beginning of employment, continue throughout employment, and recur at the end of employment. Tools that can help in this regard include:

- Onboarding procedures to emphasize the importance of company confidential information;
- Including in NDAs an express representation that the employee does not possess and will not use while in your employ confidential information belonging to any former employer or other third party;
- Using yearly (or more frequent) brief interactive e-modules emphasizing the importance of maintaining the confidentiality of company information;
- Requiring that the employee sit for an exit interview; and

- Requiring that the employee certify in writing, during exit interviews, that they have returned all company information and property (the employee may provide property on the spot or make statements about what will be returned—you should inventory all such indicated property and information).

Properly Exiting Employees—Particularly for High Risk Employees—Matters!

Not all employees present the same risk of loss. Generally, the loftier an employee is in the corporate hierarchy the greater the threat that that employee will expose company confidential information. The following recommendations are for mid-to-high risk departing employees:

- The person conducting the exit interview must be prepared—use a checklist;
- "Preparedness" for higher-risk employees will include (1) identifying, before the exit interview, the trade secret and confidential information the employee routinely accessed and used during employment, (2) reviewing for unusual activity the departing employee's computer and work activities (including card key facility access data, where available) in the days and weeks leading up to their exit, (3) using an exit certification as noted above, and (4) inquiring where the employee is going and what position the employee will hold;
- Where initial investigation warrants, discreetly interview company-friendly co-workers of the departing employee to identify potentially suspicious conduct;
- Immediately shut down the departing employee's access to company computers, networks, and other data repositories (e.g., cloud or other off-site storage). Cutting off access to company computer and data may be warranted before exiting the employee, depending on the perceived risk of data theft;
- Send a reminder-of-obligations letter to the now former employee, reciting ongoing obligations to the company and attaching, where useful, a copy of the NDA the employee has signed;
- Consider notifying the new employer, but tread carefully here to avoid overstepping or providing a basis to be accused of interfering with the employment relationship between your former employee and the new employer; and
- Depending on the threat level you perceive, consider having a departing employees' emails preserved and their electronic devices forensically imaged.
- With best practices in place, protecting your company's trade secrets should be more like routine, but vigilant maintenance, than preparing to do cyber battle with foreign states. Organizations understandably focus on creating the next "big thing," increasing sales, and building investor value, but slowing down enough to be purposeful in protecting intellectual property is a must.

What To Do About Employee Thieves—Catch Them If You Can!

By Kristen Peters (August 10th, 2016)

Cross Posted from California Peculiarities.

***Seyfarth Synopsis**: When employee theft occurs, employers must be cautious in investigating, avoiding self-help, and in deciding if and how to terminate the offending employee.*

Companies work hard to hire trustworthy employees, but employee theft can occur in any business. Employee theft takes different shapes—you may discover an employee is stealing products, supplies, confidential information or money from the company; an employee may steal more surreptitiously by padding time on a time sheet; or an employee may intentionally fail to enter vacation time taken in order to get paid for that time when they quit. Whether subtle, or as brazen as a famous thief (see https://en.wikipedia.org/wiki/Catch_Me_If_You_Can), any form of employee theft hurts your business and can present you with a difficult management situation.That's why we're here to help with the following tips.

1. "An Honest Man Has Nothing to Fear"—Background Checks:

Inquiring into an applicant's history can be a useful tool to identify people with a propensity toward dishonesty, but if you use background checks, make sure you follow the rules about collection and use of information.

a) California law prohibits use of consumer **credit reports** for employment purposes except when hiring for certain specified positions, such as managers, peace officers, positions that involve regular access to personal and banking information of individuals, access to $10,000 or more of cash, or access to confidential or proprietary information of the employer. (Labor Code § 1024.5.)

b) State and local agencies (as well as employers in San Francisco and Richmond) cannot use information about **criminal history** unless and until a decision about the candidate's minimum qualifications has already occurred. (See. e.g., Labor Code 432.9 and San Francisco Fair Chance Ordinance.)

c) In addition, under federal law, criminal history may not present an automatic barrier to employment; there must be a relationship between the criminal activity and the important elements of the job, and employers should consider the number of convictions, their nature and seriousness, how recent they are, and evidence of rehabilitation.

For the kinds of background inquiries that **are** permitted, make sure that you provide the appropriate disclosures, get permission from the prospective employee, and provide a copy of the background check report if requested. See our prior posts on California background check requirements here.

A thorough pre-employment background check should include:

- criminal history (if permitted) for crimes involving violence, theft, and fraud (in California you can only check back 7 years; you cannot ask about marijuana-related convictions that are more than 2 years old, or arrests that did not result in conviction)
- civil history for lawsuits involving collections, restraining orders, and fraud
- driver's license check for numerous or serious violations
- education verification for degrees from accredited institutions
- employment verification of positions, length of employment, and reasons for leaving.

2. "People Only Know What You Tell Them"—Verify Past Employment:

Even though most employers will verify only position and dates of employment, a prospective employer may be able to tell by the tone of voice whether the former employer had issues with the employee. A prospective employer should consistently ask previous employers whether the applicant is eligible for rehire.

3. "Don't Break the Rules"—Provide Clear Written Policies Prohibiting Theft:

Develop a written policy regarding timekeeping, with specific instructions on the duty of honesty and prohibition against timekeeping fraud. You should also have an employee handbook that covers the policy and the penalties for theft. In addition, it is a good idea to have clear written policies posted in the workplace regarding stealing, what types of acts constitute stealing and the consequences that will be enforced if an employee is caught stealing. Translate your policies into the languages spoken by your workforce. Have your employees acknowledge in writing that they have read and know the policies.

What to Do (and Not Do) If You Think an Employee Is Stealing

1. Investigate … *With Care* and Document Results.

An allegation of theft is serious and an employer should be very careful in planning, carrying out and documenting the investigation. There should always be at least two individuals involved in the investigation and, ideally, at least one of the investigators should not know the accused. If the company has a protocol for an investigation, follow it closely. Let the accused employee tell his or her story and include it as part of the record of investigation.

2. Do Not Withhold Missing Amounts of Money From the Employee's Paycheck.

An employer can lawfully withhold amounts from an employee's wages only under very limited circumstances, and employee theft or suspected theft is not one of them. (Labor Code Sections 221 and 224.) In fact, court decisions and the IWC Wage Orders specifically regulate an employer's ability to deduct amounts from an employee's wages due to cash shortages, breakage or loss of equipment. So, if you lose some equipment or merchandise, or find that cash is missing, resist the urge to take an offset against the suspected offending employee's wages, and instead find out how to respond correctly.

3. To Terminate or Not To Terminate?

This determination depends heavily on how strong the evidence is against the employee. If the evidence is not conclusive, you may want to be careful about telling an employee that he or she is being fired for theft, dishonesty, or suspicion of theft. Accusing an employee of a crime may be considered defamatory and should not be done unless the employer is 100% certain. Instead, the cautious employer will cite to lack of trust, or loss of confidence as the reason for termination. Or, even better, connect the termination to a violation of policy or procedure. Even this less dangerous road can contains land mines, as inconsistent enforcement of a work rule could potentially lead to claims of discrimination.

Workplace Solutions: "Don't Be a Stranger" when it comes to consulting your counsel regarding the appropriate response to employee theft, including whether to terminate an employee for stealing. In the event you find yourself depending against any resulting claims, you will want to make sure your actions were well thought out and well documented.

Texas Appellate Court Affirms Injunctive Relief and $2.8 Million Award in Attorney's Fees Against Former Employee in Trade Secret Misappropriation Case

By Jesse M. Coleman (September 1st, 2016)

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

Patrick Daugherty was a partner and senior executive at Highland Capital Management, L.P. (Highland), until he left to start a competing business. Highland presented evidence at trial that, after leaving Highland, Daugherty forwarded Highland documents to his personal email address, kept printouts of other emails, and kept 40,000 documents on his laptop that he only submitted for forensic remediation after trial. The documents on his laptop included portfolio and pricing information as well as documents regarding Highland's internal management and operations.

Ultimately the jury found that the information Daugherty took did not meet the definition of "trade secret" but did constitute "Confidential Information" as that term was defined in Daugherty's employment agreement. The jury then found that Daugherty had breached his employment agreement and related buy/sell by using or disclosing confidential information and other information. Nevertheless, the jury awarded Highland $0 in damages but did find Highland was entitled to $2.8 million in attorney's fees. The trial court upheld these findings and issued a permanent injunction against Daugherty preventing him from retaining or disclosing Highland's confidential information.

Daugherty appealed, arguing that the Texas statute awarding attorney's fees for breach of contract-Texas Civil Practices and Remedies Code § 38.001(8) – only does so when there is a finding of damages. Daugherty also argued that the award of $0 in damages, and Highland's efforts to recover a specific dollar amount, foreclosed the possibility of imminent harm, irreparable injury, and no adequate remedy at law, all of which were necessary for a permanent injunction to issue.

The Dallas Court of Appeals rejected these arguments and affirmed the jury verdict and trial court injunction. First, the Court held that Highland had adequately pleaded and presented evidence that the agreements Daugherty breached entitled Highland to and assessment of fees against him independent of § 38.001(8), and that the contract provisions did not require a finding of damages.

The Court further held that the damages question posed to the jury only involved lost profits. Highland presented extensive evidence, meanwhile, that Daugherty's actions resulted in long-term

unquantifiable harm, including the ability of competitors to replicate Highland's business strategies. Highland also presented evidence that Daugherty's actions may have resulted in the loss of trust from Highland's clients. The Court further noted that Daugherty's contracts with Highland also allowed for injunctive relief as a result of breach.

Daugherty v. Highland Capital Mgmt., L.P., No. 05-14-01215-CV ,2016 WL 4446158 (Tex. App. – Dallas, Aug. 22, 2016).

Trading Secrets

You get to write the script for this story…

By Michael Tamvakologos and Justine Giuliani (October 26th, 2016)

Cross Posted from [Workplace Law and Strategy.]

Effective restraints of trade protect businesses which rely heavily on human capital from damage that sometimes can't be undone. These restraints – usually sitting in an employment contract – can be a key business asset.

Others might think about it as an insurance policy. The capacity to preserve customer connections, protect confidential information and discourage key executives from setting up their own business or moving to a competitor can be critical to information rich businesses operating in a competitive market. As we pointed out in our previous blog piece on post-employment protections, The difference between winning and losing restraint litigation is often good housekeeping, ensuring the currency of your restraint provisions is an important exercise in risk management.

Our experience in this area is that one key distinction separates cases where restraints are successfully upheld and those where compromise outcomes are required. When seeking to enforce a restraint, an employer will need to demonstrate to the court there is a protectable interest capable of supporting the restraint. In successful cases, typically, the restraint provision has been drafted quite neatly around the key protectable interests. This is the first limb of the test for enforceability. The scope, duration and geographical operation of the restraint are logically tied to the protectable interest (see our map, above). An employer will need to make out each of these elements to meet the second limb of the test.

This success can be attributed to the practice of regularly revisiting the questions of which key executives or employees should be subject to restraints, and how those restraints should operate. Think about their knowledge and relationships (their human capital) as key business assets that have to be protected – or protected against. The yearly promotion, pay rise or management re-shuffle cycles are perfect opportunities to update restraint provisions. Often, this is when operational changes (such as the make-up of roles) become effective, so restraints can be tweaked to align with these changes. A promotion or pay rise can be tied to a new contract or restraint provision.

Instead of adopting a one-size-fits-all approach when an employee first joins the business, employers can increase the likelihood that a restraint will be enforceable by showing it was the subject of specific negotiation during the employment.

Webinar Recap! The Intersection of Trade Secrets Violations and the Criminal Law

By Andrew S. Boutros, Katherine Perrelli, and Michael Wexler (October 28th, 2016)

We are pleased to announce the webinar "The Intersection of Trade Secrets Violations and the Criminal Law" is now available as a webinar recording.

In Seyfarth's eighth installment in the 2016 Trade Secrets Webinar Series, attorneys Andrew Boutros, Katherine Perrelli and Michael Wexler focused on criminal liability for trade secret misappropriation. Trade secret misappropriation is increasingly garnering the attention of federal law enforcement authorities. This reality creates different dynamics and risks depending on whether the company at issue is being accused of wrongdoing or is the victim of such conduct.

As a conclusion to this well-received webinar, we compiled a summary of three takeaways that were discussed during the webinar:

- The theft of trade secrets is not only a civil violation — it is also a criminal act subject to serious fines and imprisonment. In an ever-increasing technological age where a company's crown jewels can be downloaded onto a thumb drive, victims and corporate violators must be mindful of the growing role that law enforcement plays in this active area. And, in doing so, working with experienced counsel is critical to interfacing with law enforcement (especially depending on which side of the "v." you are on), while still maintaining control of the civil litigation.

- With the advent of the Defend Trade Secrets Act, intellectual capital owners have a powerful new tool to both protect assets with as well potentially defend against. As such, processes must be in place to carefully screen new employees as well as provide vigilance over exiting employees so that one can guard against theft and be prepared to address purported theft brought to ones doorstep with a new hire. Finally, it is important to review and update agreements with the latest in suggested and required language to maximize protections which is best accomplished through annual reviews of local and federal statutes with one's counsel.

- "Protect your own home" by putting tools in place *before* a trade secret misappropriation occurs. This includes taking a look at your employment agreements to make sure they are updated to comply with the Defend Trade Secrets Act (DTSA) and that they have been signed. In addition, make sure you have agreements in place with third parties (e.g., clients, vendors, contractors, suppliers) to protect your proprietary information. Finally, secure your network and facilities by distributing materials on a need-to-know basis: Don't let your entire workforce have access.

CFTC Proposes New Rule Allowing it to Obtain Trading Firm's Trade Secrets Without Due Process

By Erik Weibust and Andrew Stark (November 10th, 2016)

As the Obama administration winds down, its regulators are showing no signs of letting up. Last week the Commodities Futures Trading Commission (CFTC) decided that it should no longer be constrained by its subpoena power when it seeks to obtain highly confidential and propriety algorithms used by electronic trading firms. In a 2-1 vote, the CFTC commissioners proposed a new rule under which a majority of the commissioners could vote to issue an order that requires CFTC-regulated companies to hand over the source code to their complex mathematical models that drive their trading decisions. The power would allow the agency to force automatic trading companies to hand over what is seemingly their most valuable assets and closely held secrets upon the mere suspicion of wrongdoing and without the need to show any probable cause. As noted in the Wall Street Journal, "[t]his is like asking Apple to turn over the source code for the iPhone."

The majority vote was led by Chairman Timothy Massad and Commissioner Sharon Bowen, with Commissioner Christopher Giancarlo dissenting. Massad reasoned that the current rules favor automatic trading firms over traditional trading companies, as the former are able to simply "hide behind their machines" to avoid agency surveillance. Dissenting Commissioner Giancarlo criticized the majority for seeking to go above and beyond the subpoena process, thereby eliminating any due process protection that the companies may have under the Constitution.

The new rule would also require algorithmic trading firms to register with the CFTC if they trade on average 20,000 futures contracts a day over a six-month period. This would broaden the agency's coverage and potentially its ability to obtain highly coveted secrets that form the foundation for some firms. And there is reason for concern. Some may recall in 2001 when Senator Bernie Sanders released confidential CFTC data on oil trading positions, and it is not a far reach to think that a firm's proprietary algorithms could similarly be used for political purposes.

While this proposed rule may only impact a small industry at the moment, that other agencies may now seek the same power is worrisome. With Obama on his way out the door and Trump on the way in, it is yet to be seen whether this type of power grab will continue. We will continue to monitor and report the development and public comment on this proposed rule.

Webinar Recap! Trade Secret Audits: You Can't Protect What You Don't Know You Have

By Robert B. Milligan, Eric Barton, and Scott E. Atkinson (November 17th, 2016)

We are pleased to announce the webinar "Trade Secret Audits: You Can't Protect What You Don't Know You Have" is now available as a webinar recording.

In Seyfarth's ninth installment in the 2016 Trade Secrets Webinar Series, attorneys Robert Milligan, Eric Barton, and Scott Atkinson focused on trade secret audits. It is not uncommon for companies to find themselves in situations where important assets are overlooked or taken for granted. Yet, those same assets can be lost or compromised in a moment through what is often benign neglect. Experience has shown that companies gain tremendous value by taking a proactive, systematic approach to assessing and protecting their trade secret portfolios through a trade secret audit.

As a conclusion to this well-received webinar, we compiled a summary of three takeaways that were discussed during the webinar:

- As part of any trade secret audit, confidentiality agreements should be updated to include the new immunity language required by the Defend Trade Secrets Act (DTSA) to preserve the company's right to exemplary damages and attorney's fees under the DTSA.
- A trade secret audit, and the resulting protection plan, should have three primary goals:

(1) Ensure that a company's trade secrets are adequately identified and protected from disclosure;

(2) Ensure that a company has taken adequate steps to protect itself in litigation if a trade secret is misappropriated; and

(3) Limit the risk of exposure to other companies' claims of trade secret misappropriation.

- As part of a trade secret audit, onboarding and off-boarding procedures are evaluated to ensure that the intellectual property rights of third parties and the company are respected.

Webinar Recap! Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches

By James D. McNairy and Justin K. Beyer (December 27th, 2016)

We are pleased to announce the webinar "Proving-Up Trade Secret Misappropriation: Best Practices and Tales from the Trenches" is now available as a webinar recording.

In Seyfarth's final installment in the 2016 Trade Secrets Webinar Series, James McNairy and Justin Beyer, joined by computer forensics expert Jim Vaughn of iDiscovery Solutions, focused on best practices for assembling the evidence most often needed to prosecute a claim for misappropriation of trade secrets

As a conclusion to this well-received webinar, we compiled a summary of three takeaways that were discussed during the webinar:

1. The first step in prosecuting trade secret misappropriation starts with identifying your trade secret information, maintaining its confidentiality, and putting in place safeguards such as robust confidentiality agreements, computer use and access policies, and exit interviews that are tailored to flag any exfiltration of data by high risk employees or business partners with whom your company is parting ways. Diligence on the front end will better alert your organization of potential data theft and enable it to secure the data, should it be misappropriated.

2. As part of your investigation of potential trade secret misappropriation, remember to conduct a complete audit of devices and sources of data storage and transmission to ensure nothing is overlooked. While doing so, it is critical to maintain the forensic integrity of the devices and data to allow the best chance of admitting the information into evidence in any litigation.

3. Efficiently organizing the right team to prosecute trade secret theft is critical. The "team" most often includes human resources professionals (to authenticate key agreements, policies, dates of employment etc.), a senior manager or executive (who can validate the existence of the trade secret, its value, the measures taken to maintain secrecy etc.), senior managers who worked with the suspected misappropriators (who can attest to access, use, and possession of the at issue information), in-house IT professionals (who can lay the foundation for devices, data, and access rights of the suspected misappropriators), and an independent computer forensics expert (who can objectively present the facts concerning data accessed, by whom, through what means, and explain any technical nuance to "connect the technical dots" of the bad actor(s) conduct).

Challenge to ITC's Extraterritorial Authority over Trade Secret Dispute Launched by Chinese Corporation

By Marcus Mintz (December 28th, 2016)

The United States International Trade Commission ("ITC") is an independent, quasijudicial Federal agency with broad oversight over trade matters. In addition to trade practices such as dumping and subsidies, the ITC adjudicates matters involving the misappropriation of trade secrets and theft of intellectual property. Specifically, Section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337(a)(1)(A), prohibits "unfair methods of competition and unfair acts in the importation of articles … into the United States."

In 2012, the Federal Circuit—which has jurisdiction over all ITC matters—was asked to consider whether the ITC had authority to investigate the misappropriation of trade secrets protected by domestic law when the misappropriation occurred exclusively in China. *See Tianrui Group Co. Ltd. v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011). The Federal Circuit answered in the affirmative and held that the ITC had authority to "investigate and grant relief based in part on extraterritorial conduct insofar as it is necessary to protect domestic industries from injuries arising out of unfair competition in the domestic marketplace." *Tianrui*, 661 F.3d at 1324. Following *Tianrui*, domestic companies have used the ITC to redress misappropriation of trade secrets far from American shores so long as the misappropriation resulted in the importation of products into the US causing domestic injury. For further background on the *Tianrui* decision, please see our prior post here.

The ITC's extraterritorial authority established in *Tianrui* is once again being challenged. Recently, in another case involving the misappropriation of American trade secrets in China, the Supreme Court was asked to decide whether Section 337 of the Tariff Act does, in fact, authorize the ITC to investigate misappropriation that occurred entirely outside the United States. *See Sino Legend (Zhangjiangang) Chemical Co. Ltd. v. ITC*, cert petition available here. The crux of Sino Legend's argument is that for a statute to apply abroad, there must be express congressional intent. Not surprisingly, Sino Legend argues that such intent is missing from Section 337 of the Tariff Act. In *Tianrui*, the Federal Circuit held that such intent was manifest in the express inclusion of "the importation of articles .. into the United States" which evidenced that Congress had more than domestic concerns in mind. *Tianrui*, 661 F.3d at 1329. To prevail, Sino Legend must convince the Supreme Court to not only hear its case, but to overrule *Tianrui*'s holding that such intent is evident from the "importation of articles" clause in the Act.

Sino Legend's petition comes at an interesting time. The Supreme Court is only 8 justices following the death of Justice Scalia, perhaps making it even more difficult for cert to be granted. At the same time, trade with China was a repeat theme of President-Elect Trump's presidential campaign. Companies with operations abroad should closely monitor the progress of *Sino Legend*, as reversal of *Tianrui* will result in the removal of a powerful tool in a trade secret owner's arsenal against extraterritorial misappropriation of trade secrets.

Computer Fraud and Abuse Act

Ninth Circuit Poised to Address the "Without Authorization" Debate under the Computer Fraud and Abuse Act Again

By Amy Abeloff (January 13th, 2016)

Background

Imagine if you could manage all of your social media platforms on one app. Believe it or not, there *was* an app for that (or, at least a website), created by a company named Power Ventures ("Power"). Back in 2008, Power instituted its "Power 100" campaign, which offered its users the chance to win $100 if they invited 100 friends to join. After asking its users' permission, Power would access its users' Facebook accounts to send messages to friends of its users to encourage them to join Power. These messages were sent to friends of Power users from email addresses containing Facebook in the source name (e.g., amy@facebookmail.com), thus giving the impression that the messages came from Facebook personnel, not from Power.

Lo and behold, the "real" Facebook became aware of Power's plan and tried to stop it through the use of an IP block, which Power was able to overcome. Facebook continued combatting Power's activity by sending cease and desist letters, reiterating how Power's activities went beyond the scope of its authorized use, but Power failed to act in compliance with these requests. Thereafter, Facebook slapped Power with a lawsuit, alleging (among other things) a violation of the Computer Fraud and Abuse Act ("CFAA"), primarily based on Power's unauthorized use of Facebook data and systems. Four years later in 2012, the U.S. District Court for the Northern District of California found that Power indeed violated Section (a)(2)(C) of the CFAA. The following year, the district court issued an order granting not only a permanent injunction against Power, but also prescribed damages in excess of $3 million to be paid to Facebook.

Status of the Case

As perhaps any party would do following such a dismal outcome at district court, Power decided to appeal to the Court of Appeals for the Ninth Circuit. Oral arguments were heard in December, and a Ninth Circuit court opinion is expected to come down in the coming months.

Ninth Circuit Oral Argument

At oral argument, counsel for Power argued that Power could not have violated the CFAA because it never owned the data at issue in the case. As such, it was beyond Facebook's power to grant or deny authorization to user accounts to third-parties. Counsel pressed that acting with authorization means one has authorization *from the owner of the data*; Facebook, according to Power's counsel, explicitly disclaimed ownership of such data. In other words, because individual Facebook users granted Power

access to their accounts, Power was acting within the scope of authorization, and is therefore not liable to Facebook under the CFAA.

From another standpoint came Power's former CEO, Steve Vachani, who made a statement that Facebook, now a social media giant, is acting anti-competitively by still litigating this case after seven years. Counsel for Facebook disagreed, saying that his client was not being anti-competitive, but rather acting in compliance with its legal obligations.

Third-Party Perspectives

This is not the only CFAA-related case the Ninth Circuit has faced as of late. Some time ago, the court heard oral arguments for the *U.S. v. Nosal* case, blogged here. Given the recent interest in this CFAA line of cases, commentators have piped up and expressed their thoughts on the CFAA and its application to password sharing scenarios.

For instance, the Electronic Frontier Foundation ("EFF") wrote as *amici* in support of Power's position, noting that Facebook's use of the CFAA is "dangerous to follow-on innovators and consumers and would criminalize widely accepted Internet behavior."

Additionally, Professor Orin Kerr appears to support curbing the interpretation and application of the CFAA to password sharing scenarios and believes any user of a *personal* account may authorize a third-party agent to access the account, but such would not be the case if the individual were acting within the scope of employment. In other words, if the individual gave her *employer's* account credentials to a third-party agent for the third-party's own purposes, that would not constitute authorization because it would be beyond the employer's grant of authorization to its employee.

Takeaways

Given the compensatory and equitable damages awarded to Facebook at the district court level, it will be especially interesting to see if the Ninth Circuit upholds the district court findings and damages, especially against a now defunct company. Upholding the district court's damages award will certainly call practitioners and their clients to attention.

It will also be interesting to see if the Ninth Circuit somehow consolidates its rationale in *Nosal* into this case, and finally carves a distinction between password sharing in the workplace and personal password sharing scenarios.

Computer Fraud and Abuse Act Not Violated Unless Plaintiff Shows Defendant Had Intent To Defraud

By Paul E. Freehling (February 9th, 2016)

In a recent Computer Fraud and Abuse Act case, the Seventh Circuit Court of Appeals affirmed the district court's conclusion that the plaintiff had produced no evidence refuting the defendant's contention that it honestly believed it was engaging in lawful business practices rather than intentionally deceiving or defrauding the plaintiff. Accordingly, entry of judgment for the defendant was appropriate. *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, Case No. 4:13-CV-4021 (7th Cir., Jan. 21, 2016).

Summary of the Case

Fidlar licenses technology to county governments enabling them quickly to scan and digitize real estate transaction documents. The county-licensees pay Fidlar a fee for using its technology. In turn, county-licensees making the digitized documents available on line charge an access fee. Persons who access the digitized documents *and print copies* must remit copying fees to Fidlar.

LPS gathers, analyzes and sells data concerning real estate transactions. It developed software that permits the company, in exchange for a monthly payment to the county-licensees, to harvest and download *en masse* documents digitized by the counties using Fidlar's technology. The software enables LPS to analyze the digitized data *without printing the documents* and, thereby, to avoid paying copying fees which otherwise would have been owed to Fidlar. When Fidlar learned what LPS was doing, Fidlar accused LPS of computer fraud in violation of the CFAA. LPS denied wrongdoing and prevailed in court on summary judgment.

The Parties' Contentions

According to Fidlar, LPS defrauded Fidlar because LPS knew about the copying fee and had to know that its system for harvesting the information contained in the digitized real estate transaction documents allowed it to benefit from Fidlar's technology without paying anything to that company. LPS responded that, far from intending to deceive or defraud, its business practices were driven by its need to access and analyze data quickly and efficiently, and that printing copies of the documents was unnecessary.

Did LPS intend to defraud Fidlar?

Counties pay a fee to Fidlar for using its technology in order to digitize the contents of documents. LPS pays a fee to counties for enabling its computers to access the digitized data. LPS avoided remunerating Fidlar by not printing copies of the information. And, significantly, there was neither disruption nor destruction of Fidlar's computer system or intellectual property. Fidlar apparently failed to anticipate, and therefore did not forbid, LPS' access to and use of the data in this manner.

The CFAA criminalizes fraudulently accessing a computer or computer system with the intent of deceiving or cheating. In opposition to LPS's summary judgment motion, Fidlar maintained that whether LPS intended to defraud Fidlar is a question of fact requiring a trial. However, both the lower and appellate tribunals said that the entry of summary judgment was appropriate because Fidlar was required, but failed, to demonstrate that there was evidence in the record supporting Fidlar's claim that LPS had a fraudulent intent.

Takeaways

Proving a CFAA violation requires evidence of an intentional fraud. Even though Fidlar's technology did not expressly *permit* third parties to access the digitized records and use the information without printing copies, thereby avoiding payment of fees to Fidlar, such access and use were not *prohibited*. Fidlar lost the case because it failed to design its software to require payments to the company by third parties who figured out how to make use of the data without printing it.

Recent Decision Highlights Important Pleading Requirements for Computer Fraud and Abuse Act Claims

By Eric Barton (February 18th, 2016)

Ever since *Iqbal* and *Twombly*, it has become imperative that a complaint filed in federal court contains "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 554, 570 (2007)). The Eastern District of Michigan recently reiterated this point in the context of an alleged violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. As detailed below, failure to include the requisite factual allegations can and will result in the dismissal of potential CFAA claims.

Summary

In *Fabreeka International Holdings, Inc. v. Robert Haley and Armadillo Noise & Vibration LLC*, 2015 U.S. Dist. LEXIS 154869 (E.D. MI, Nov. 17, 2015), Fabreeka Intl. Holdings filed suit against its former employee, Robert Haley, and his new employer, alleging that Haley unlawfully accessed its computers to obtain confidential information in violation of the CFAA. Specifically, Fabreeka alleged that: (1) during the period of his employment, Haley accessed confidential business information stored on Fabreeka's servers; (2) Haley did not return all of Fabreeka's confidential information at the time of his resignation; and (3) Haley authored or assisted in authoring proposals for his new employer using Fabreeka's confidential information for the purpose of undercutting Fabreeka's prices.

Fabreeka contended that its allegations establish violations under three sections of the CFAA: 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), 1030(a)(5)(B) and (C).

- Subsection (a)(2) prohibits (1) intentionally accessing a computer (2) without authorization or exceeding authorized access and (3) thereby obtaining information (4) from any protected computer (if the conduct involved an interstate or foreign communication) where (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value.

- Subsection (a)(4) prohibits (1) accessing a "protected computer" (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) furthering the intended fraud and obtaining anything of value, causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

- Subsection (a)(5)(B) prohibits (1) intentionally accessing (2) a protected computer (3) without authorization, and (4) as a result of such conduct, recklessly causes damage. 18 U.S.C. § 1030(a)(5)(B).

- Subsection (a)(5)(C) prohibits (1) intentionally accessing (2) a protected computer (3) without authorization, and (4) as a result of such conduct, causing damage and loss. 18 U.S.C. § 1030(a)(5)(C).

The District Court dismissed each of these CFAA claims for the following reasons:

1. There was no dispute that Haley was authorized to access information on the Fabreeka's servers, including sales and manufacturing data, during his employment at Fabreeka. Since the facts pled established Haley had authorization, the Court held that Fabreeka's claims subsections (a)(5)(B) and (a)(5)(C), requiring the access be "without authorization," should be dismissed. This left Fabreeka's remaining CFAA claims, which the Court said could proceed so long as Fabreeka pled facts that establish Haley exceeded his authorized access.

2. Fabreeka's Complaint asserted that Haley misappropriated confidential information based solely on the similarity of proposals submitted by Fabreeka and his new employer. Based off those proposals, Fabreeka offered unsupported conclusions that Haley stole confidential files and assisted in authoring the competitor's proposal. The Court held that because "[a] pleading must include factual allegations that exceed mere speculation, *see Twombly*, 550 U.S. at 555, and Fabreeka's CFAA allegations fail to meet this standard."

In addition, the Court noted that a complaint must state sufficient facts to "raise a reasonable expectation that discovery will reveal evidence" of a claim's required elements. Although Fabreeka's Complaint alleged that Haley and his new employer's owner communicated on Fabreeka's computer during Haley's employment, the Court found that the mere fact that the two discussed Haley joining Armadillo does not support a plausible inference that the two colluded to misappropriate confidential information. Thus, the Court held that it did " not feel" that Fabreeka's Complaint "pled sufficient facts to raise a reasonable expectation that further evidence of a CFAA violation will be revealed in discovery."

3. Fabreeka's Complaint implied that the company considers all non-public information confidential. Defendants, on the other hand, claimed that Fabreeka's proposals cannot be considered confidential because they are transmitted to third parties without any steps to protect the proposals or the information they contain. The Court noted that the Sixth Circuit previously stated, in the context of trade secrets, that if a company did not take reasonable steps to maintain the confidentiality of alleged trade secrets, a misappropriation claim properly fails. *See BDT Products, Inc. v. Lexmark Int'l, Inc.*, 124 F. App'x 329, 333 (6th Cir. 2005). Accordingly, the Court held that insofar as Fabreeka's allegations address confidential material taken, the company's proposals submitted to customers may not be properly considered secret or confidential.

4. Finally, the Court held that Fabreeka's Complaint did not allege that the "damage and loss" allegedly suffered arose from the cost of responding to or from investigation into Haley's alleged violation. Instead, the Complaint merely recited the elements of the CFAA and asserted there had been "damage and loss." The Court held this was insufficient.

Takeaway

When asserting claims under the CFAA, it is critical to not only review and pled the necessary elements that form the claims, but to also include the sufficient factual allegations to support those claims. The *Fabreeka* decision highlights how more and more courts are cracking down on insufficient pleading, particularly in the context of CFAA suits. As a plaintiff, do not fall victim to poor or lazy drafting and, as

a defendant, carefully review a complaint's factual allegations with an eye towards a possible motion to dismiss.

Federal Court Rejects Employer's Trade Secret and Computer Fraud and Abuse Act Claims

By Paul E. Freehling (February 29th, 2016)

An ex-employee's former employer sued him for alleged violations of the Kansas Uniform Trade Secrets Act (KUTSA) and the federal Computer Fraud and Abuse Act (CFAA). The first claim was based on the company's hunch that he had misappropriated trade secrets and thereby breached his non-disclosure agreement. Two forensic experts were paid $38,000 to examine the computers and flash drives he had used, looking for evidence that he had used or disclosed confidential information. The second claim centered on his admission that, shortly before resigning from the company, he had read a top-secret file which was, but should not have been, accessible to employees. He moved for summary judgment on both claims. The court granted the motion, holding that (a) payments to the experts did not satisfy the KUTSA requirement of showing an "actual loss caused by misappropriation" (K.S.A. 60-3322(a)), and (b) he was authorized to access the company's shared files and, therefore, he did not violate the CFAA. *Tank Connection, LLC v. Haight*, No. 6:13-cv-01392-JTM (D. Kan., Feb. 5, 2016) (Marten, C.J.).

Summary of the Case

Haight was International Sales Manager of Tank Connection, a manufacturer of large storage tanks. He signed a confidentiality agreement (but not a non-compete). With the company's consent, he downloaded confidential information onto the laptop and flash drives provided to him by the company. However, he also downloaded company data onto his own flash drives. Further, he reviewed — but did not copy — the company's president's confidential computer file. Following his resignation, he returned the company's laptop and what he asserted were all of its flash drives. Further, he insisted that he had neither disclosed the company's secrets to his new employer nor used the information, and that he had deleted all of Tank Connection's data from his personal flash drives. Concluding that Tank Connection had produced no evidence contrary to his disavowal of trade secret misappropriation, and that reading the shared file was not a violation of the CFAA, the court entered judgment for Haight.

Why the Claim of Trade Secret Misappropriation Failed

Tank Connection's expert witnesses determined that, shortly before Haight's resignation, he accessed the company's server and transferred to the company's laptop and flash drives, and to his own flash drives, a lot of confidential information. The company contended that "harvesting" of that data circumstantially supported the claim that he had used proprietary information improperly and/or had disclosed it to his new employer. However, Chief Judge Marten ruled that without any hard evidence of wrongdoing, and in the face of Haight's unqualified denial of culpability, Tank Connection's speculation of improper conduct was insufficient to create KUTSA liability.

Tank Connection alleged that its damages from Haight's "misappropriation" aggregated $1,238,000: $1.2 million that the company had expended for creating, developing and updating the computer programs, plus $38,000 it had paid to the experts. Chief Judge Marten rejected the $1.2 million claim because the company did not show any loss of data, damage to its computers or programs, unfair competition, or unjust enrichment. Further, the statutory alternative of assessing "a reasonable royalty" was inapplicable due to the absence of proof that Haight disclosed or used confidential information.

Finally, the court held that payments to computer forensic experts retained by Tank Connection to investigate an alleged but unproved theft of trade secrets were not an "actual loss caused by misappropriation." The judge said that the question has not been decided by Kansas judges, and that Connecticut Appellate and Virginia Supreme Court rulings are in diametric opposition to each other. Concluding that the payments were "not within the traditional realm of tort damages," and that they were incurred merely in an attempt to ascertain *if* there had been a theft, the court held that they were not compensable losses under KUTSA.

Why the Claim of a CFAA Violation Failed

A few days before Haight resigned, a co-worker brought to his attention a computerized folder containing highly sensitive information intended solely for the eyes of the company president and one administrator. The company was unaware that incorrect security settings for the folder enabled employees such as Haight to access it. He admitted that he had looked at it, which constituted a CFAA violation according to Tank Connection, but he insisted that he and other employees regularly viewed shared files in the course of their work and that he did not copy, disclose or use the folder's contents.

Chief Judge Marten observed that the president's folder was in a shared file, and there was no evidence that Tank Connection told its employees not to open the folder. He said that, therefore, Haight clearly did not violate the statutory prohibition against *accessing* a computer "without authorization." The difficult question under the CFAA was whether Haight *exceeded* his authorized computer access. The judge found persuasive *U.S. v. Valle*, 807 F.3d 508 (2nd Cir. 2015), which held that an employee's authority to access a computer file is dispositive in determining that the CFAA has not been violated, regardless of the use to or purpose for which the file is accessed. Thus, summary judgment was granted on the CFAA claim as well.

Takeaways

Haight prevailed on the trade secrets misappropriation claim largely because he was authorized to use Tank Connection's confidential data in the course of his employment, and the company had no evidence that he disclosed or used the data other than for company business. In the absence of a smoking gun or an eye witness to wrongdoing (Tank Connection had neither), employers often have difficulty disproving an ex-employee's denial of culpability. Perhaps Tank Connection might have strengthened its case if it had examined Haight's personal flash drives before he deleted all of the information on them.

The ruling declining reimbursement of Tank Connection's expenses for computer forensic experts seems to have been driven by the company's inability to prove that any misappropriation occurred. A number of courts have held that amounts paid to such experts, for tasks associated with a pretrial investigation launched because of suspected trade secret theft, are recoverable damages. However, in those cases typically, the experts concluded that the company's suspicion was well-founded. *Tank Connection* is unusual because reimbursement was sought in the face of a failure to prove any impropriety. Under these circumstances, the expenses did not qualify as an "actual loss caused by misappropriation."

Chief Judge Marten's ruling regarding the scope of the CFAA is another in the litany of disputes pitting a narrow statutory interpretation against a broader one. *Compare* such decisions as *Valle* cited by the court (holding that the Act only prohibits computer hacking by an outsider), *with, e.g., Epic Systems Corp. v. Tata Consultancy Services Ltd.,* No. 14-cv-748 (W.D. Wis., Nov. 18, 2015) (opining that the CFAA also criminalizes "insider hacking," that is, unauthorized *use* of data by someone authorized to *access* the computer). The conflict in these decisions probably can only be resolved by Congress or the U.S. Supreme Court.

Computer Fraud and Abuse Act Ruling: Did the Ninth Circuit Just Criminalize Password Sharing?

By Scott E. Atkinson (July 13th, 2016)

Not exactly. A divided Ninth Circuit panel recently affirmed the conviction of a former employee under the Computer Fraud and Abuse Act ("CFAA"), holding that "[u]nequivocal revocation of computer access closes both the front door and the back door" to protected computers, and that using a password shared by an authorized system user to circumvent the revocation of the former employee's access is a crime. *United States v. Nosal*, ("*Nosal II*") Nos. 14-10037, 14-10275 (9th Cir. July 5, 2016). The dissenting opinion raised concerns that the majority opinion would criminalize password-sharing in a wide variety of contexts where the password was shared by an authorized user but in violation of a service provider's terms of service, such as for email or social networking.

An Inside Job

David Nosal was a recruiter employed by the executive search firm Korn/Ferry. To serve its clients and help place executives in response to talent searches, Korn/Ferry maintained a confidential, proprietary database containing detailed personal information about over one million executives. Nosal left Korn/Ferry and launched a competing firm with two other Korn/Ferry colleagues. Korn/Ferry revoked Nosal and his colleagues' authorization to access its database. After Nosal and his colleagues left Korn/Ferry, Nosal's colleagues accessed the database at his behest using the log-in credentials of Nosal's former executive assistant, who remained employed at Korn/Ferry and who was authorized to access the database. They used the assistant's valid credentials in order to run searches for candidates and thereby compete with Korn/Ferry. Nosal was convicted of violating the CFAA on a theory of accomplice liability based on his colleagues' actions. He was ordered to pay a sizeable restitution award to Korn/Ferry.

What does "without authorization" mean, anyway?

The CFAA imposes criminal penalties on whoever "knowingly and with intent to defraud, *accesses a protected computer without authorization, or exceeds authorized access*, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ." 18 U.S.C. § 1030(a)(4) (emphasis added). In a previous appeal in the *Nosal* case ("*Nosal I*"), the Ninth Circuit held that the "exceeds authorized access" prong makes criminal conduct out of "violations of [a company's] use restrictions." The Ninth Circuit's decision in *Nosal II*, however, focused entirely on the "without authorization" prong of the CFAA.

The majority concluded that "without authorization" is unambiguous, and that the Ninth Circuit's ruling in *LVCR Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) applied to Nosal's conduct: "[A] person uses a computer 'without authorization' under [the CFAA] . . . when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." The court stated

that refusing to apply the CFAA to circumstances where an authorized user shared log-in credentials with a person whose credentials had been revoked by the owner of a protected computer system would "remove from the scope of the CFAA any hacking conspiracy with an inside person. That surely was not Congress's intent."

So is password-sharing now a crime?

Judge Reinhardt dissented from the majority's opinion, expressing concerns that the ruling would criminalize "password sharing." Judge Reinhardt warned that the majority opinion "threatens to criminalize all sorts of innocuous conduct" and does not provide "a workable line which separates the consensual password sharing in this case from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners" like email service providers or social networking sites. Judge Reinhardt asserted that, in order to avoid criminalizing such commonplace conduct, the "best reading of 'without authorization' in the CFAA is a narrow one: a person accesses an account 'without authorization' if he does so without having the permission of *either* the system owner *or* a legitimate account holder." (Emphasis original.)

It will be left to future cases to ascertain the outer boundaries of the majority's holding. It seems unlikely that the Ninth Circuit would uphold a CFAA conviction of a person who watched Netflix using a friend's login credentials, but Judge Reinhart correctly points out that there is no inherently limiting language in the statute itself. So, future litigants may focus on the *Nosal II* majority's discussion of "revocation of access" as a means to distinguish simple password sharing. It would be one thing for a person to use a friend's Netflix account to watch movies; it would be another thing if the person had previously had a Netflix account revoked for downloading and selling pirated copyrighted works, then used a friend's account to circumvent the "revocation of access" and continue such piracy. The problem is, the statute's language does not make any distinctions based on "revocation of access." It remains to be seen whether *Nosal II* provides a workable rule for applying the CFAA in future cases.

Practical Implications for Employers

Setting aside the great password-sharing debate, *Nosal II* makes clear that criminal sanctions can be imposed against former employees who improperly access their employer's systems after their authorization to do so is revoked by the employer. Whether former employees use their old log-in credentials or use those of current employees who are themselves authorized to use the employer's systems, *Nosal II* means that any such access is "without authorization" under the CFAA.

Facebook, Inc. v. Power Ventures, Inc.: Shotgun-Toting Borrowers of Jewelry From Bank Safe Deposit Boxes and the CFAA. Wait. What?

By James D. McNairy (July 19th, 2016)

On July 12, 2016, the Ninth Circuit filed its published opinion in *Facebook, Inc. v. Power Ventures, Inc., et al.*, Case No. 13-17154 (*"Power Ventures"*). *Power Ventures* is the latest in a series of decisions from the Ninth Circuit relating to the type of activities potentially giving rise to liability under the Computer Fraud and Abuse Act (18 U.S.C. §1030) ("CFAA"). *Power Ventures* has potentially important implications for the ways that businesses create, store, and monetize data through computers and web-based applications. Unlike the court's *Nosal* line of decisions, *Power Ventures* is focused more on internet-based conduct that may violate the CFAA.

The underlying legal dispute between the parties began in 2008, when Facebook filed suit against Power Ventures, Inc. ("Power") in the USDC for the Northern District of California. Power, which aggregated data from different social networking sites using, among other things, automated scripts (i.e., "scraping"), enabled people with various social media accounts to access all of their information in one place. Power used user-provided social media log-in information to import people's information to a Power portal. In an effort to promote itself and attract users, Power then contacted via e-mail Facebook users' friends, making it appear as if the e-mails came from Facebook.

Upon learning of Power's activities, Facebook sent Power a cease and desist letter and used IP blocks in an attempt to prevent Power from obtaining Facebook data (IP blocking is a process by which a computer or network is directed to ignore all communications from a particular IP address). But Power continued to copy Facebook data and took measures to evade the IP blocks.

Although the Ninth Circuit analyzed whether Power's conduct violated the federal CAN-SPAM Act (finding that it did not, and reversing District Court Judge Lucy Koh), the court's analysis of the CFAA issues are most noteworthy. The court first walked through its *United States v. Nosal* CFAA decisions (from 2012 and July 5, 2016; see our coverage of these decisions here and here) to "distill two general rules" in analyzing the issue of authorized access under the CFAA:

(1) "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly" (noting that "once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability"); and

(2) "a violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA."

Applying these rules, the court noted that Power users "arguably gave Power permission to use Facebook's computers to disseminate messages" (further stating that "Power reasonably could have

thought that consent from *Facebook users* to share the [Power promotion] was permission for Power to access *Facebook's* computers") (emphasis in original). Importantly, the court found that "[b]ecause Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's computers 'without authorization' within the meaning of the CFAA."

The court declined, in a footnote, to "decide whether websites such as Facebook are presumptively open to all comers, unless and until permission is revoked expressly" (citing to a law review article asserting that "websites are the cyber-equivalent of an open public square in the physical world").

Instead, the court found that a cease and desist letter sent to Power by Facebook expressly rescinded the permission granted by Facebook users to Power and put Power on notice that it "was no longer authorized to access Facebook's computers." The letter informed Power that, in Facebook's view, Power had violated Facebook's Terms of Use and directed Power to cease using Facebook content or otherwise interacting with Facebook through automated scripts.

Power continued to access Facebook and took steps to evade the IP blocks that Facebook put in place. The court noted discovery from the trial court that appears to reflect a concerted effort by Power to wire around Facebook's countermeasures and a likely awareness that Power's conduct implicated the CFAA.

To explain its finding that the Facebook cease and desist letter had revoked Power's permission to access Facebook, the court analogized the circumstances to a person who wanted to borrow a friend's jewelry held in a bank safe deposit box. The court said that the borrower would need permission from the bank and the safe deposit box holder to access the box if the bank had determined that it did not want the borrower on its premises (in the court's example, because the borrower brought a shotgun to the bank when entering to access the safe deposit box).

Although the court's analogy might have helped it better understand the technology and information flow at issue in *Power Ventures*, it lacks the nuance that can swirl around alleged "scraping" scenarios where there are sometimes questions concerning whether "access" under the CFAA has occurred and whether there is a protectable or property interest in the data scraped (in the court's analogy, the jewelry was the safe deposit box holder's property, but what was the data equivalent in *Power Ventures* and, under different facts, what might be the bank's property interest?).

The court then went on to distinguish *Power* from its *Nosal* decisions and, in doing so made some interesting observations (arguably in dictum) about the legal effect of Facebook's Terms of Use. The court observed that "Facebook and Power had no direct relationship, and it does not appear that Power was subject to any contractual terms that it could have breached." It is unclear whether, by making this statement, the court is saying that, by its conduct, Power and Facebook had not entered into a contract (e.g., the Facebook Terms of Use) or rather there simply were no terms within the Terms of Use that prohibited Power's conduct.

Notably, Facebook does not appear to have pleaded a breach of contract claim in the trial court.

In any event, whether a website's terms of use will apply to and bind a party that attempts to "scrape" data from the website is likely to be further litigated as the intersection of traditional contact formation principles meet the evolving standards under "browser-wrap" and "click-wrap" agreements.

This much is clear from *Power Ventures*: Those who use websites to conduct business would be well-served to (1) carefully consider the drafting and use of website terms of use; (2) diligently monitor their websites and associated computers/servers for any access, and the means of access, by anyone other than authorized users; and (3) where unauthorized access is detected, to act promptly to notify in

writing those who have potentially made such access of the conduct alleged to be improper/unlawful and demand that such conduct cease.

Cyberspace and e-commerce law will continue to evolve rapidly, so banks best keep an eye out for those skilled in the programming arts along with shotgun-toting borrowers of jewelry.

What Underlying Facts are Required to Assert a Valid CFAA Claim Based on "Exceeds Authorized Access" in Georgia?

By Eric Barton (November 7th, 2016)

The Computer Fraud and Abuse Act ("CFAA") gives rise to an actionable claim if someone "knowingly access[es] a computer without authorization or exceed[s] authorized access." 18 U.S.C. § 1030(a)(1). The term "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). In recent years, plaintiffs have attempted to argue that someone "exceeds authorized access" under the CFAA when they access work related information on their employer issued computer for non-work related reasons. In Georgia, courts appear to be divided on whether such an allegation gives rise to a valid CFAA claim.

For example, in *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010), the Eleventh Circuit adopted a broad view of the definition "exceeds authorized access," holding that when an employer has a policy limiting an employee's computer access to that done for business purposes, an employee who accesses that information for non-business purposes exceeds authorized access. In *Rodriguez*, the defendant worked for the Social Security Administration, which had a policy that the use of its databases to obtain personal information was authorized only when done for business reasons. 628 F.3d at 1263. The defendant conceded that his access of personal information at issue was not done in furtherance of his duties as a teleservice representative. *Id.* As such, the court ruled that the defendant had exceeding his authorized access under the CFAA.

The following year, the Northern District of Georgia applied *Rodriguez*'s broad interpretation of "exceeding authorized access," holding that an employee's e-mailing of confidential employer information to herself without a business purpose exceeded any authorized computer access and, therefore, violated the CFAA. *See Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F.Supp.2d 1302, 1315 (N.D. Ga. 2011) ("[T]here is no question that [an employee] exceeded any authority she had when she sent [documents] to herself after accepting a position at [another company] for use in competing with [the plaintiff].")

Since *Rodriguez* and *Amedisys*, however, several district courts in the Eleventh Circuit, including in at least one in Georgia, have applied a more narrow definition of "exceeds authorized access," concluding that if a defendant has full administrative access to a computer, a claim for unauthorized access cannot be stated under the CFAA. *See,* e.g., *Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc.*, 953 F.Supp.2d 1290, 1297 (S.D. Ga. 2013); *Enhanced Recovery Co. LLC v. Frady*, No. 3:13-cv-1262-J-34JBT, at *26 n.7 (M.D. Fla. Mar. 31, 2015).

The *Power Equip.* decision is particularly instructive on the issue, explaining that:

the CFAA focuses on an individual's unauthorized access of information rather than how a defendant used the accessed data. More specifically, the proper inquiry is whether an employer had, at the time, both authorized the employee to access a computer and authorized that employee to access specific information on that computer. 953 F.Supp.2d 1290, 1295 (S.D. Ga. 2013) (emphasis in original).

The court further held that the CFAA

does ***not*** confer upon employers the ability to sue their employees in federal court for violations of company policy regarding computer usage… [It] does ***not*** speak to employees who properly accessed information, but subsequently used it to the detriment of their employers: ***either one has been granted access or has not.*** Employers cannot use the CFAA to grant access to information and then sue an employee who uses that information in a manner undesired by the employer.

Id., at 1296 (emphasis added). Other courts in the Eleventh Circuit have held the same. *See Trademotion, LLC v. Marketcliq, Inc.*, 857 F.Supp.2d 1285, 1291 (M.D. Fla. 2012) (concluding that plaintiff failed to state a claim under CFAA because plaintiff admitted that defendant had "full administrative access" to plaintiff's computer system).

Takeaway

When deciding whether to assert a cause of action under the CFAA based on "exceeding authorized access," the safest course of action in Georgia is to only do so when the facts demonstrate that the individual in question did not have permission to access the information in question. If the individual was given access to the information in question, but you believe accessed that they accessed that information for a non-work related purpose, consider relying on alternative theories of liability, such as conversation, breach of contract, or misappropriation.

Trading Secrets

Non-Competes & Restrictive Covenants

Five Easy Tips for Improving Your Company's Non-Compete and Confidentiality Agreements and Related Practices Now

By Robert B. Milligan (February 10th, 2016)

As January quickly passed by and new projects increase by the day, there is still a golden opportunity to capitalize on some low-hanging fruit to immediately improve your company's practices and add immediate value to your company. The opportunity lies in improving your company's restrictive covenant and confidentiality agreements and confidentiality policies. Below are five tips that you can employ immediately to improve your company's agreements/policies and practices.

First, make sure your company is using confidentiality agreements and confidentiality policies with your employees. You may be surprised to learn how many companies do not ask their employees to sign such agreements. When those companies later seek to explore their options against employees who have joined competitors, their options are significantly narrowed. Also, your company should not rely solely on employee handbook policies or other similar policies. While your company may not use non-compete or non-solicitation covenants with your workforce, at a minimum, companies should use non-disclosure agreements with their employees. There is really no excuse not to ask employees to sign such agreements.

Additionally, companies should consider using the maximum legally permissible restrictive covenants in their jurisdictions, including non-competes and non-solicitation of customers and employees as applicable, with their workforces; otherwise, companies are leaving a competitive advantage at the table. While some companies may elect not to use non-compete agreements because such covenants are viewed as not supportive of their company "culture," companies should carefully survey what their competitors are doing and determine whether they are putting themselves at a disadvantage in the talent market.

Second, spend some time with the business leaders in departments that create your company's confidential information to make sure that your company's non-disclosure agreement provides sufficient descriptions of the information that each department considers high value confidential information. Oftentimes, companies give little thought to the categories of information described in the non-disclosure agreement or have no description of the information whatsoever. While your company should not provide the secret information in the agreement, your company should at least describe the category of information in which it belongs and some specifics so that the category is easily identifiable by employees. The value in describing the information in more detail is that the employee then understands what the company deems confidential, and it also provides the company a better chance in the courtroom to hold a former employee accountable if he or she misappropriates such information.

Third, review your company's restrictive covenant and confidentiality agreements to make sure that they do not unnecessarily limit the company's rights. In one recent case, an employer lost its trade secret suit because its non-disclosure agreement defined confidential information as only that information which had been marked confidential. The court found that the trade secret claim failed because the information in dispute had not been marked confidential. The trade secret claim may have proceeded if the contract had not unnecessarily restricted the term "confidential" information to only signify information labeled confidential. While labeling information as confidential indicates that such information may be subject to reasonable secrecy measures to support a classification as a trade secret, it is typically not dispositive as to whether contract and trade secret claims can be pursued for the theft of company information.

Additionally, companies operating in states that permit non-compete and non-solicitation agreements should consider using such agreements with their employees in those states even if those companies' corporate headquarters are in jurisdictions where non-competes are typically void in the employment context, such as California. Simply put, just because your company is headquartered in California does not mean that you should not ask your employees in Florida to sign non-compete and non-solicitation agreements governed by Florida law. Additionally, some companies have been successful in using forum selection and choice of law provisions to bind employees who work in jurisdictions where restrictive covenants are limited to non-competes and non-solicitation covenants in the company's home forum, particularly where such employees are provided access to trade secrets and maintain well-established relationships with company clients. A company should also consider whether to use a prevailing party provision for attorney's fees and costs for actions brought on or related to the agreement.

Fourth, take into account some recent developments in state non-compete law to make sure that your company's agreement is compliant. For example, Oregon has limited the duration of employee non-competes to two years effective January 1, 2016. Hawai'i has banned the use of non-compete and non-solicit agreements with technology works effective July 1, 2015. Alabama has made it easier to enforce non-compete agreements with a revised statute that became effective January 1, 2016. Also, in Alabama, non-competes of one year will now be presumed to be enforceable. Additionally, Illinois and Pennsylvania have special requirements for the roll-out of non-compete agreements with existing employees, including providing consideration apart from continued employment alone, to enforce such agreements. The Wisconsin Supreme Court recently has found that continued employment was adequate consideration for non-compete agreements entered into after the inception of employment. There are also active movements in Utah and Washington to restrict the use of non-compete agreements.

Fifth, critically examine which employees and third parties your company asks to sign restrictive covenant and confidentiality agreements and be mindful of third-party scrutiny. Regulators, legislators, and employee groups are scrutinizing the use of restrictive covenant agreements. While some employers may not be using such agreements enough, particularly with the right people (i.e., executives, engineers, R&D personnel, sales representatives, among others), other companies may be accused of overreaching in asking all employees to sign non-compete agreements. While the janitor does not necessarily need to sign a non-compete, he or she probably should sign a non-disclosure agreement in certain instances. Also, your company should perform an audit or ensure one has been performed to see if your company has signed agreements with key employees, particularly high level executives and employees who may be flight risks.

Companies should think critically about who they *are* asking to sign such agreements and who they *should* be asking to sign such agreements (e.g., appropriate restrictive covenants and non-disclosure agreements with vendors and contractors). We have found that while some companies may have solid agreements with employees, the same high value information may be provided to contractors and

vendors without similar protections, which erodes the confidentiality protections placed on the information. Government agencies such as the NLRB, SEC, and EEOC are actively scrutinizing employer confidentiality restrictions, so companies should be mindful to provide examples of confidential information instead of broad undefined labels, to not prohibit disclosure of information protected by Section 7 of the National Labor Relations Act (such as concerted activity involving discussions of conditions of employment or wages), and to not prohibit participation in government investigations or including similar provisions which impede the ability of employees to act as whistleblowers.

As many have already broke their New Year's resolutions as we move into February, there is still an opportunity for you to add value to your organization by addressing these critical issues and providing useful recommendations to your organization. Don't wait. Act today and reach for this low-hanging fruit.

Webinar Recap! 2015 National Trade Secret, Non-Compete and Computer Fraud Law Year in Review

By Robert B. Milligan, Jesse M. Coleman, and Daniel Joshua Salinas (February 17th, 2016)

We are pleased to announce the webinar "2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law" is now available as a podcast and webinar recording.

In Seyfarth's first installment of its 2016 Trade Secrets Webinar series, attorneys Robert Milligan, Jesse Coleman, and Joshua Salinas reviewed noteworthy cases and other legal developments from across the nation this past year in the areas of trade secrets , non-competes and other restrictive covenants, computer fraud and data theft, as well as provided their predictions for what to watch for in 2016.

As a conclusion to this well-received webinar, we compiled a list of brief summaries of the more significant cases that were discussed during the webinar:

- Data breach is a question of when and not if. Companies should ensure they have implemented sufficient information security policies and a data breach response plan. There are limitations in the law and challenges in international misappropriation cases. The best strategy is to try to prevent breach and misappropriation through effective policies, procedures and agreements, employee training, technology solutions, and continual assessment and improvement.

- Courts continue to struggle with issues regarding adequacy of consideration for restrictive covenants. Employers who have asked existing employees to sign non-competes or are considering doing the same should evaluate whether consideration was or will be provided for the non-compete to ensure enforcement under applicable law.

- While the circuit court split continues to widen regarding the interpretation of unauthorized access under the Computer Fraud and Abuse Act, the recent decision in *U.S. v. Christensen* (9th Cir. 2015) may provide employers with a civil cause of action in California against employees who misuse company data without permission.

Ex-Employee Hit With Six-Figure Judgment For Violating His Non-Competition Agreement By Helping His Son Compete

By Paul E. Freehling (March 10th, 2016)

A long-running non-compete clause dispute has reached the Louisiana Court of Appeal three times. Last month, the court affirmed a $600,000 judgment, plus attorneys' fees and costs, against an ex-employee who assisted his son's start-up company compete with his father's former employer. *Pattridge v. Starks*, No. 50,351-CA (Louisiana Court of Appeal, Feb. 24, 2016) (*Endurall III)*.

Summary of the Case

Endurall, Inc. — a Louisiana manufacturer and seller of rod guides used in the oil and gas industry to prevent well tubing leaks — terminated the employment of corporate officers Billy Joe Edwards and Jimmy Starks, two of its three 33% stockholders. The company and the owners of the other 34% sued Billy Joe, Starks and others in a Louisiana state court alleging, in part, that Billy Joe violated his non-competition agreement by helping his son Gregory Edwards make and sell rod guides.

After a trial, the judge ruled that Billy Joe violated his non-compete agreement, that the company's four shareholders were irreconcilably deadlocked, and that their stock should be auctioned. That order was affirmed on appeal (149 So.3d 820 (2014) (*Endurall I*). Next, the trial judge permanently enjoined Billy Joe from, or assisting others in, competing in the rod guide industry. That decision also was upheld (*Endurall II*). The trial court then presided over an evidentiary hearing on damages and awarded $600,000 to the plaintiffs. In *Endurall III*, the Court of Appeal affirmed.

The Non-Compete and Confidentiality Agreements

At the time Endurall was created, each shareholder signed a confidentiality agreement. They acknowledged that the non-competes were an essential condition of their stock purchases, and each promised not to participate in any competitive business for two years after he ceased to own Endurall stock

Billy Joe's Alleged Breach of his Non-Compete

In 2012, Billy Joe, his son Gregory, and Starks formed Vector Energy Solutions. Billy Joe was elected vice-president of development. When Endurall and its other two shareholders learned about Vector, they accused Billy Joe and Starks of disclosing Endurall's confidential information to Vector.

At the court-ordered auction of Endurall's stock in 2013, the successful bidders were its two shareholders who were not involved with Vector. They paid Billy Joe and Starks $1.1 million each for

their stock. Billy Joe went to work for Skye Petroleum which made paraffin products for the oil and gas industry. He and his wife loaned their son Gregory hundreds of thousands of dollars to start DHE, LLC.[1] Billy Joe helped to acquire the building (a few blocks from Endurall) where both he and DHE had their offices, and he touted DHE to his Skye Petroleum customers who had a need for rod guides. In addition, Gregory wrote a letter announcing the creation of his new company, made reference to his work experience with his father, and stated that DHE's rod guides were superior to those made by Endurall. Quickly losing customers and sales representatives to DHE, Endurall filed suit.

Damages Calculation

The plaintiffs called an expert damages witness; the defendants did not. The witness testified that Endurall was injured as "a result of impaired operations" caused by DHE. He said that the damages amount could be determined by (1) comparing the company's performance before and after the impairment, or (2) using a discounted future earnings approach. The "before and after" method, the expert said, considered Endurall's sales history and gross profits, minus (a) avoidable costs, and (b) variable costs incurred but not due to lost sales. The discounting approach extrapolated sales data for six years from late 2014, assumed a 14% annual volume increase, and used an "aggressive" time-value-of-money discounting rate.

The expert was cross-examined "rigorously" according to the trial judge, and "ably and thoroughly" in the words of the Court of Appeal. The expert admitted that, among other suppositions, he presumed that Endurall's current cost of production would not change and that customers lost to DHE would never return to Endurall. He conceded that a 14% annual sales increase was not supported by Endurall's history, and he acknowledged that DHE's actual sales volume was substantially less than the amount of sales Endurall claimed to have lost to DHE. However, he said that over time and on average the model he used would be supported. He concluded that, regardless of which method was employed, Endurall lost approximately $900,000 in profits as a result of sales to customers poached by DHE.

The trial judge decided to award damages only through 2016, not all the way to 2020 as the plaintiffs' expert witness proposed. The court reasoned that technological advances might render rod guides obsolete and, in the appellate tribunal's words, the trial judge "recognized the significant uncertainty and generous assumptions built into [Endurall's] damages model," "the volatile nature of Endurall's business," and that the "projected sales over time were speculative." Even though the trial judge admitted that his computation was "somewhat arbitrary," the Court of Appeal affirmed because "the record reveals no manifest error . . ., [the] damage award was based on . . . the evidence presented and not on mere speculation," and "no abuse of discretion" was detected. By awarding 33% less than the expert's calculation of lost profits, moreover, the trial court adequately took into account the complexity of computing damages.

Billy Joe contended that damages should not have been awarded beyond 2015 when the two-year non-compete expired. The Court of Appeal disagreed. It explained that DJE's early entry into the market gave Endurall no time to prepare for the competition, and that Billy Joe could have mitigated Endurall's losses by delaying assistance to his son.

Takeaways

Endurall III contains several important lessons.

First, a signatory to a non-competition agreement who assists someone else to compete can be found liable for violating it notwithstanding the signatory's apparent lack of a personal profit motive.

Second, the decision provides a thoughtful analysis of the difficulties faced by a trial court called upon to compute damages sustained by a well-established market leader at the hands of a start-up competitor assisted by a knowledgeable alleged non-compete clause violator.

Third, the opinion reminds us that calling a damages expert to testify is not always required just because the adversary has such a witness. Without calling an expert witness, Billy Joe apparently was able to provide "rigorous", "able" and "thorough" cross-examination of the plaintiffs' damages expert. Billy Joe avoided incurring the expense of a testifying expert who, in any event, might have been unnecessary or even potentially counter-productive.

[1] Coincidentally or otherwise, Endurall's original name was Down Hole Enterprises.

Extensive Training Of Ex-Employee By Former Employer Not Enough For Injunction Against Competition

By Paul E. Freehling (March 21st, 2016)

Although an employer spent many hours assisting an employee to obtain a real estate appraiser's license, the Tennessee Court of Appeals held recently that the employee's restrictive covenants were unenforceable. *Davis v. Johnstone Group, Inc.*, No. W2015-01884-COA-R3-CV (Mar. 9, 2016).

Summary of the Case

The ex-employee, Davis, had no prior real estate appraisal experience in 1998 when he started work at Johnstone Group, Inc. (JGI), a Tennessee appraisal firm. In order to become licensed as a Certified General Real Estate Appraiser, he was required to complete 180 hours of classroom instruction. He did so at his own expense. In addition, he had to have 3,000 hours of supervised appraisal practice. Mr. Johnstone, the owner of JGI, provided that supervision. Davis signed restrictive covenants when he became employed by JGI and again in 2005, after satisfying his classroom and supervised appraisal requirements, and receiving his license.

According to the Court of Appeals, at trial JGI failed to prove that it provided secret or unique training to Davis or that he possessed confidential business data. Accordingly, both the trial and appellate tribunals held that a ruling for JGI would restrain ordinary competition.

Background Facts

The two sets of restrictive covenants were similar. Both stated that Davis would not, for two years after termination, provide real estate appraisal, consulting or comparable services within 150 miles of JGI, would not assist any of its customers or solicit any of its employees, and would not divulge any of the company's proprietary information. In 2015, Davis resigned from JGI and shortly thereafter went to work for a competitor.

The Litigation

Upon receipt of a threat from JGI that the company would take legal action to enforce the covenants, Davis filed a preemptive lawsuit in a Tennessee chancery court. He alleged that the non-compete was unenforceable because the company had not given him any specialized training or access to confidential information. JGI answered and counterclaimed, asserting that the covenants were "reasonable and necessary to protect [its] legitimate business interests." It asked for injunctive relief and damages.

Decisions Below and on Appeal

The trial court granted the declaratory judgment Davis sought and denied the relief requested by JGI. The company appealed. According to the Court of Appeals, under Tennessee law an employer seeking to enforce a restrictive covenant must demonstrate "special facts" which give the ex-employee "an unfair competitive advantage." Here, however:

- There was no evidence that Davis took with him JGI's confidential client information, business records, or secret bidding or pricing data that could be used by a competitor.
- The knowledge and skill provided to Davis during his training was not unique but, rather, was similar to that which anyone interested in becoming a licensed real estate appraiser would receive.
- JGI did not have a secret method of appraising.
- With only a few exceptions, Davis did not have a "special relationship" with JGI's customers, and the company knew about all of his relationships because Mr. Johnstone signed off on all of Davis's appraisals.

Takeaways

JGI had an uphill battle to reverse the trial court and obtain the relief the company sought. First, lately courts seem to be denying enforcement of non-compete clauses except in extraordinary cases. Second, the Court of Appeals mentioned twice in its opinion that no transcript or summary of the evidence was included in the record on appeal. The court said that therefore, under applicable law, it "must presume that there was sufficient evidence before the trial court to support its judgment" and could "only conclude that JGI has failed to prove any facts . . . that would warrant enforcement of the non-competition" covenant.

Third, judicial decisions are not uniform on the subject of what facts must be proved to warrant injunctive relief for an employer. The appellate opinion reminds us, however, that extensive training of an employee is not adequate by itself to justify enforcement of a non-compete. Here, although some facts supported the case for injunctive relief, some did not. The impact on the Court of Appeals' decision of the hole in the record cannot be determined.

Leave No E-mail Unturned in Trade Secret and Non-Compete Cases

By Eric Barton (March 30th, 2016)

A recent verdict in the Superior Court of Fulton County, Georgia is an excellent reminder of the importance of conducting thorough discovery in unfair competition cases. Earlier this year, after a four day trial, a Georgia jury awarded telecom company Cost Management Group ("CMG") $282,001 in damages, $300,000 in attorneys' fees, and $200,000 in punitive damages, finding that CMG's former president, Daniel Bommer, breached his contract by operating a competing company, as well as siphoning employees and business away from CMG to a second competing company, all while employed by the plaintiff.

Interestingly, this particular case was preceded by a separate 2009 action, in which CMG filed suit against another one of its former officers, who it also accused of diverting CMG's accounts and agents to a competing business. According to court filings, CMG prevailed in that case as well and was awarded more than $120,000 in damages. The added "bonus," however, was a cache of e-mails discovered on CMG's former chief operating officer's server (who was not even named in the lawsuit). Among those e-mails were communications in which Bommer allegedly requested the competing business "destroy all evidence of past and future email communications between [itself] and Bommer." In large part based on the information secured in these retrieved e-mails, CMG proceeded with filing suit against Bommer, alleging claims for breach of fiduciary duty, usurpation of corporate opportunities, unfaithful agent, conversion/theft of corporate property, breach of the securities and exchange agreement and fraud, as well as a claim for punitive damages.

Perhaps even more importantly, as a direct result of CMG's discovery in the first case, prior to trial against Bommer, CMG filed a motion for sanctions, claiming Bommer spoliated critical evidence. The court agreed and granted CMG's motion, completely striking Bommer's answer and counterclaim. Accordingly, at trial, the only remaining issue for the jury was a determination of damages — always a position plaintiffs' lawyers love to find themselves.

Had CMG's counsel not conducted thorough and sifting discovery in the original case, including seeking electronic discovery from non-parties, it is quite possible that CMG may have never located the evidence of spoliated e-mails. By doing so, CMG was able proceed directly a trial on damages, without ever having a jury even establish liability. Had CMG's lawyers not located this information, the trial undoubtedly would have been much more complicated and certainly gone on for much longer than four days. Again, the case is a superb testament to leaving no stone unturned during the discovery process in unfair competition matters — particularly electronic stones.

The case is *Cost Management Group v. Bommer*, Civil Action File No. 2009CV168191, Fulton County Superior Court, Georgia.

New Utah Law Limits Restrictive Covenants to a One-Year Period

By Arielle Eisenberg (March 31st, 2016)

On March 9, 2016, Utah enacted the Post-Employment Restrictions Amendments, which limits restrictive covenants to a one-year time period from termination. Any restrictive covenant that is entered into on or after May 10, 2016, for more than one year will be void. Notably, the new law does not provide for a court to blue pencil an agreement, rather the agreement as a whole will be deemed void.

Employers should be wary of enforcing an invalid restrictive covenant. Under the new law, if a court or arbitrator deems a restrictive covenant unenforceable, the employer will be liable for court or arbitration costs, attorney fees, and actual damages.

The new law has carved out several exceptions. It does not apply to (1) a "reasonable severance agreement," (2) any restrictive covenants stemming from the sale of a business, (3) nonsolicitation agreements, (4) nondisclosure agreements, and (5) confidentiality agreements. However, these exceptions are still subject to common law restrictions.

Going forward, employers should take a close look at their standard non-compete clause and make the appropriate changes to ensure that any non-compete agreements entered into starting May 10, 2016, are in compliance with the new one-year time limit.

North Carolina Courts Are Forbidden To "Blue Pencil" An Unenforceable Non-Compete

By Paul E. Freehling (April 4th, 2016)

Reversing a 2-1 decision of the North Carolina Court of Appeals, the state's Supreme Court held unanimously that an assets purchase-and-sale contract containing an unreasonable territorial non-competition restriction is unenforceable. Further, a court in that state must strike, and may not modify, the unreasonable provision. *Beverage Systems of the Carolinas, LLC v. Associated Beverage Repair, LLC*, No. 316A14 (N.C. Sup. Court, Mar. 18, 2016). The Court of Appeals' decision, now reversed, is published at 762 S.E.2d 316 (2014) and was the subject of a *Trading Secrets* blog dated August 27, 2014.

Status of the Case

The trial court entered summary judgment for the defendants as to all claims. That ruling, which was reversed by the Court of Appeals, has been reinstated.

The Purchase-and-Sale Transaction

Thomas Dotoli owned Imperial Unlimited Services which serviced soft drink dispensers in parts of North and South Carolina. His wife and their son, Loudine, owned Elegant Beverage Products which sold premium coffee and tea in the same areas. In 2009, the three Dotolis sold Imperial and Elegant to a new company, Beverage Systems of the Carolinas, which was owned by Loudine Dotoli's wife, Cheryl. In connection with the purchase-and-sale transaction, the sellers executed a five-year non-compete covenant, encompassing the entirety of North and South Carolina, for which they were paid $10,000. The covenant provided that a court could revise the temporal and geographic limits if they were deemed unreasonable.

Competition, and a Lawsuit, Ensue

When Associated Beverage began installing and servicing beverage dispensing machines in North and South Carolina, Beverage Systems sued Cheryl, her company, and Loudine. He was accused of breach of contract. All of the defendants were charged with tortious interference and unfair and deceptive practices. The defendants responded that the covenant was unenforceable because of its allegedly overbroad temporal and territorial restrictions.

Ruling of the Trial Court

Agreeing with the defendants that the covenant included geographic restrictions beyond those necessary to maintain the plaintiff's customer relationships, the trial court entered summary judgment against Beverage Systems.

Reversal by the Appellate Court

The Court of Appeals reversed and remanded. The appellate court's majority okayed the five-year restriction but held that the trial court should have blue-penciled the unreasonable territorial limitation. Further, the appeals court majority said disputed issues of material fact precluded summary judgment. Dissenting, one appellate jurist stated that the contract only allowed blue-penciling as "permitted by law," that North Carolina judges can strike — but are not authorized to rewrite — unreasonable restrictions, and that there were no contested factual disputes. The dissenter would have affirmed.

The Supreme Court's View

The Supreme Court emphasized that, in the instance of the sale of a business, a geographic restriction limited to the locations where the seller operates is permissible. Here, however, the restricted territory encompassed what the Court called "large swaths" of both North and South Carolina in which Beverage Systems had no customers. The Court held that territorial limitations are enforceable "as written or not at all." Since striking the unreasonable provision results in "no territory left within which to enforce the covenant not to compete, . . . blue-penciling cannot save the Agreement." Nor could the parties "contract to give a court power that it does not have."

Rejecting Beverage Systems' allegations of interference with contract, the Supreme Court stated there was no evidence of contracts between Beverage Systems and its customers. Rather, the jurists held that the evidence only showed general business relationships. Thus, the defendants "were free to engage in routine business competition with Beverage Systems."

Takeaways

The blue-pencil doctrine has significant variations in different states.

- Judges in a few jurisdictions are *not permitted to modify* contracts under any circumstances.
- In states that do permit blue-penciling, courts reason that the parties' intent to have a contractual relationship sometimes is furthered by *substituting* reasonable terms for unreasonable ones (but judges sometimes decline to assist the drafters of contracts containing unduly onerous provisions).
- In North Carolina and several other jurisdictions, blue-penciling can only be used to *strike* contractual provisions, not to alter them. In *Beverage Systems*, striking the geographical limitations invalidated the non-compete.

Because of these significant variations, companies that have multi-state operations need to understand each relevant jurisdiction's blue-penciling and other rules of contract interpretation. In order to enforce similar contracts in different jurisdictions, some terms may have to be tailored to fit the law of the places where litigation may ensue.

Further, in any given jurisdiction a particular restrictive covenant in contracts for the sale of a business may be enforceable whereas the same provision is unenforceable in employment contracts.

For all of these reasons, consultation with experienced legal counsel is advised.

You Can't Put Lipstick On This Pig: Beauty Company's Non-Compete Deemed Unenforceable

By Erik Weibust and Andrew Stark (April 7th, 2016)

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

Summary of the Case

Elizabeth Grady sought a preliminary injunction to enforce the non-compete provision in the employment agreements of former employees, who trained as aestheticians and massage therapists at its day spa in Burlington, Massachusetts. While at Elizabeth Grady, the employees had signed agreements that prevented them from, among other things, copying, taking, disclosing or using any confidential information following their termination of employment, and from soliciting its customers or working for a competitor within 25 miles for one year following termination. Upon resigning from Elizabeth Grady, the employees went to work at a skin care salon and day spa within the 25-mile radius.

In denying the requested injunction, the court noted that Elizabeth Grady presented no evidence that either former employee had copied, taken, disclosed, or used any confidential information, nor did the record even remotely suggest that the retail-level employees would have enjoyed access to sensitive materials of that nature. The court further noted that there was likewise no evidence that the former employees had solicited any of Elizabeth Grady's employees. Therefore, the court focused Elizabeth Grady's cause of action on the twenty-five mile non-compete restriction.

The focus of the court's analysis was on the nature of employee's duties and the training they received from Elizabeth Grady. Specifically, the court indicated that although the Company alleged that it had trained its employees "in its skin care service techniques, client management procedures, and such other business methods as salon dress codes, gift certificates, appointments, and sales promotions," it failed to present any evidence, or "even a common-sense inference," that any of that information is truly proprietary to Elizabeth Grady, or was maintained in confidence. The court stressed that although the Company's agreement summarily asserted certain product development plans, marketing initiatives, and other business strategies represented confidential information to be protected, Elizabeth Grady did not present any evidence that showed that the former employees themselves actually enjoyed access to such information and therefore were in a position to exploit it. Further undercutting Elizabeth Grady's need to protect any of these trainings, which it referred to as the "Elizabeth Grady way," as confidential was the fact that it taught a great deal of this training it now claimed to be proprietary to the public at its Elizabeth Grady Schools.

Lastly, recognizing that Elizabeth Grady enjoys a business reputation in the skin care industry, and its products and services draw clients to its salons on a repeat business, the court nevertheless found that there was no evidence that the former employees had any ongoing relationships with Elizabeth Grady clients or were otherwise soliciting or threatening to take business away from the Company. Notably, the court stressed that even if there was evidence showing that Elizabeth Grady's clients had begun to migrate to the former employees' new day spa, "such evidence would still not (standing alone) permit a reasonable inference that the *Company's* good will is being improperly appropriated." Rather, such evidence would show that, by traveling a greater distance to access the employees' services, the customers feel loyal to the *employees*, and that true good will belongs to the employees as opposed to the Company. The court likened this to *Joymark v. Lockward*, and *Lunt v. Campbell*, two other cases in which courts held that, in the hairdressing industry, the goodwill logically belongs to the stylist.

Accordingly, the court held that Elizabeth Grady had not presented any evidence to demonstrate that its non-compete agreement safeguards a legitimate business interest, such as the former employees possessed or exploited trade secrets, confidential information, or customer good will belonging to the Company. Rather, the Company was simply attempting "to thwart ordinary competition from conventionally skilled service providers."

Takeaway

Elizabeth Grady Face First, Inc. v. Garabedian reminds us that no matter how pretty you try to make a non-compete agreement, to be enforceable it must protect a legitimate business interest, not merely ordinary job skills and knowledge.

Court Won't Enjoin Physician Who Breached Non-Compete Covenant And Consented To Injunction

By Paul E. Freehling (April 8th, 2016)

A physician signed a non-compete covenant, agreed to be enjoined if he breached, and allegedly did breach. But when his former employer asked a Providence, Rhode Island Superior Court judge to enter an injunction, he refused to prevent patients from being treated by a doctor of their own choosing. *Medicine & Long Term Care Associates, LLC v. Khurshid*, Civil Action No. PC-2015-0458 (Mar. 29, 2016) (Silverstein, J.).

Summary of the Case

MLTC is a Rhode Island provider of health care services principally to nursing home residents. When Dr. Khurshid went to work for MLTC, he signed an employment agreement with a non-competition covenant. Along with reasonable temporal and geographic limitations, it included (a) Dr. Khurshid's acknowledgement that a violation would cause irreparable harm to MLTC, and (b) his consent to entry of an injunction in the event of a breach. Several years later, he left MLTC but continued treating its clients. The company sued him and sought, among other prayers, entry of an order preventing him from competing with MLTC. Judge Silverstein ruled, however, that the requested order would violate Rhode Island public policy.

The Judge's Reasoning

Judge Silverstein found that MLTC "alleged facts and presented evidence which otherwise might entitle it to injunctive relief." However, the judge said that case law in Rhode Island provides that courts may refuse to enter injunctions which "would injure members of the public." Further, he observed that Massachusetts has a statute precluding the entry of an injunction against doctors who sign restrictive covenants, and that courts in that state have described the statute as supportive of the "strong public interest in allowing patients to consult the physician of their choice."

Rhode Island has no such statute, but Judge Silverstein ruled that the state's public interest is similar to the one in Massachusetts. He noted that in 2000 a Rhode Island Superior Court judge held that enforcement of a non-compete clause signed by a veterinarian would not impose "an undue hardship on the pets of Rhode Island." Judge Silverstein added that MLTC could "seek legal redress for its injuries" if it proved its allegation that Dr. Khurshid's breach caused substantial monetary losses to the company.

Takeaways

The judge found that, even though the subject has not previously been addressed by Rhode Island's courts or its legislature, he would not enter an injunction against physicians who sign non-compete covenants. He added that MLTC could seek compensatory damages from Dr. Khurshid. Might the risk

of facing a large monetary judgment for violation of a non-compete discourage a breach and, thereby, lead to almost the same result as an injunction?

Issues that Judge Silverstein might have mentioned, but did not, include the following:

Courts in a majority of states probably would not agree with *Khurshid*. According to the Supreme Court of Tennessee in *Murfreesboro Med. Clinic, P.A. v. Udom*, 166 S.W.3d 674, 680 (2005), most states "continue to apply a reasonableness standard in evaluating non-compete agreements between physicians, similar to the evaluation of covenants in commercial contexts." Only a few states — Colorado (Colo. Rev. Stat. 8-2-113), Delaware (6 Del. Code § 2707), and New Mexico (N. Mex.. Stat. 24-11.2) — have enacted laws similar to the Massachusetts statute.

Several state legislatures recently have rejected Massachusetts-type statutes. Bills providing that physician non-compete covenants are unenforceable have been introduced in the last year or two in Connecticut, Hawaii, Missouri, and Washington State, among others, but have failed to pass.

The AMA discourages, but permits, doctors to sign non-competes. Section E-902 of the American Medical Association's Code of Ethics provides that doctors "*should not* enter into [restrictive] covenants that . . . do not make reasonable accommodation for patients' choice of physician" (emphasis added). Section E-902 does not prohibit such covenants.

MLTC had a protectable interest in an injunction. The non-compete covenant provided that irreparable damage would result to MLTC in the event of a breach. In other words, the parties agreed that compensatory relief alone would be inadequate. Further, the public policy seemingly would have been honored if the court had permitted Dr. Khurshid to continue seeing only those patients he previously treated.

The *Khurshid* decision suggests a number of questions. For example, would Rhode Island's public interest allow patients to choose healthcare providers who executed a non-compete with a prior employer but who do not have a medical degree? Does the state's public policy protect freedom of choice with respect to learned professionals other than healthcare providers, such as an investment advisor who signed a non-compete with a previous employer? Perhaps future cases will provide answers.

California Court Gives Two Thumbs Down and Voids Non-Compete in Actor's Agreement

By Robert B. Milligan, Daniel Joshua Salinas, and Amy Abeloff (April 20th, 2016)

***Seyfarth Synopsis**: Limitation on an actor's ability to work in certain films struck down as an unlawful restraint of trade.*

California, mecca of the film and media production industries in the U.S., is notorious for outlawing non-compete agreements. It is one of the few states that generally prohibits the unlawful restraint of one's profession or business, with limited exceptions. (See Cal. Bus. & Prof. Code § 16600 et seq.). Last year's decision in ITN Flix, LLC v. Hinojosa, 2015 WL 10376624 (C.D. Cal. May 13, 2015), illustrates that courts may strike down such unlawful non-competes, even outside the traditional employer-employee context.

What is this Case About?

In 2004, film producer Gil Medina met actor Danny Trejo, who had worked on several successful films with director Robert Rodriguez (think *Sin City* and the *Spy Kids* franchise). Medina approached Trejo with an opportunity to star in a multiple picture action feature film franchise built around a "vigilante character" to be portrayed by Trejo. The following fall, Medina and an independent production company, ITN Flix, LLC produced the film, entitled *Vengeance*.

Thereafter, Trejo and Medina/ITN Flix (who went on to become the Plaintiffs in the legal case) entered into a "Master License Agreement" ("MLA") and an "Acting Agreement" ("AA"). The contracts purported to limit Trejo in playing vigilante characters in other films or appearing in films "similar" to *Vengeance*, and imposed a term of "at least" eight years on these (and other) contractual obligations. The contracts also (ambiguously) paved the way for Medina/ITN Flix to recover as commission part of the proceeds of the commercial exploitation of certain rights.

Vengeance was subsequently released, but only to a few small markets. By 2009, the film still had no significant release date. Even a 2012 collaboration with Steve Wozniak (the co-founder of Apple) and his wife, Janet, whereby the Wozniaks would appear in several new scenes that would be added to the film and also be included in a mobile application game entitled *Vengeance: Woz with a Coz,* failed to bring commercial success to the ill-fated *Vengeance*.

The legal trouble began in 2010, when director Rodriguez released a film called *Machete*, in which Trejo starred as—wait for it—a "vigilante character." Unlike *Vengeance, Machete* garnered much acclaim and commercial success. Then, in 2013, director Rodriguez released a sequel to *Machete* entitled *Machete Kills*, which was not as successful, but still raked in millions of dollars.

In November 2014, viewing the success of the *Machete* films as their failure, the Plaintiffs (Medina and ITN Flix) sued Rodriguez, Gloria Hinojosa (talent agent who helped broker Trejo's appearance in the *Machete* films) and their affiliated entities for, among other things, intentional interference with contract, violation of the Lanham Act, and unjust enrichment. Plaintiffs argued that Trejo's appearance in the

films without Rodriguez's and his affiliates' disclosure of Plaintiffs' business relationship with Trejo constituted breach of contract, and further argued that Rodriguez and had a "legal and/or contractual duty" to disclose the business relationship between Plaintiffs and Trejo to third-party investors of *Machete*.

Hinojosa and entities related to her requested dismissal of the entire action in early 2015, followed by Rodriguez's Motion to Strike Pursuant to California's Anti-SLAPP statute and Motion to Dismiss the Lanham Act claim.

How California Law Made This Case More Peculiar Than It Already Was

The court first assessed the viability of the motion to dismiss, which alleged that the MLA and AA were so vague so as to be unenforceable, and constituted unlawful restraints of trade in violation of Section 16600 of the California Business and Professions Code. In response, the Plaintiffs argued that the contracts were not vague, and insisted that Utah law governed the contracts, so the "restraint" clause was enforceable. Even if California law applied, Plaintiffs argued that it was "widely recognized" that certain reasonable exclusivity agreements could be enforceable, especially as regards contracts in the entertainment industry. The court did not buy Plaintiffs' argument in any way, shape, or form.

First, Section 16600 maintains that "[e]very contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extend void." The court harkened back to the California case *Edwards v. Arthur Anderson LLP*, which noted that California courts have "consistently affirmed that section 16600 evinces a settled legislative policy in favor of open competition and employee mobility," because the statute is designed to protect "the important legal right of persons to engage in businesses and occupations of their choosing."

Second, the court highlighted California's peculiar approach to restraint provisions in contrast to overarching Ninth Circuit law on the topic. California does **not** adopt the "narrow-restraint exception" to Section 16600, as other courts in the Circuit have adopted. California courts have emphasized the public policy behind disallowing such an exception, and have maintained that the "policy of the state… should not be diluted by judicial fiat." Instead, the court pointed out, California courts have entirely relegated to the State Legislature the task of altering the reach of Section 16600.

Third, the court analyzed whether the restraint provision would pass muster even in a Utah court. Usually, Utah courts may uphold a covenant not to compete so long as it is reasonable. For such a covenant to be valid and enforceable, it must be supported by consideration, completely free of bad faith dealing during negotiations, and must be necessary to protect the goodwill of the business. Notwithstanding such provisions, the court found that under both California and Utah law, the contracts were unenforceable, primarily because the restraints were not reasonable or narrow, and to the extent they were, *any* and *all* restraints are illegal under Section 16600. Further, the court found it "clearly unreasonable" for Plaintiffs to place an almost decade-long restraint on Trejo's career.

The court also considered whether the provision regarding Plaintiffs' ability to collect commissions on commercial exploitations of its "licensed rights" (i.e., a license to Trejo's name and likeness in "vigilante character" films) constituted a restraint on Trejo's career, and answered affirmatively. Trejo is a particular character actor, not cast in a wide variety of types of films and is "most recognizable for portraying, characters that operate outside the justice system and dispense justice or injustice." Such an actor, the court concluded, is particularly vulnerable to the type of restraint present in the MLA and AA contracts. Further, the court rejected the assumption that charging a fee or commission is not a "restraint" and saw no reason Plaintiffs should be able to charge Trejo a fee for engaging in conduct (i.e., acting in a particular type of movie as a particular type of character) that they could not otherwise

prohibit. As such, the court found the commission provision to be an unlawful restraint on trade under *both* California and Utah law.

What This Means in Terms of Employee Mobility in California

ITN Flix teaches the importance of taking care to draft contract provisions that limit or purport to limit an individual's exercise of his business or trade, regardless of the individual's industry. Such care is needed when drafting agreements with independent contractors as well as with employees at the beginning or end of employment.

ITN Flix also illustrates that California's general public policy against non-competes is not limited to the traditional employer-employee scenario. Indeed, a divided Ninth Circuit Court of Appeals panel in *Golden v. California Emergency Physicians Medical Group* recently held that a "no re-hire" provision in a settlement agreement could, under certain circumstances, constitute an unlawful restraint of trade under California law.

Without the backstop of non-compete agreements, California employers can nonetheless employ some best practices to ensure their employees do not share any valuable information with competitors. Such best practices include:

- Robust confidentiality and invention assignment agreements.
- Effective entrance and exit interview protocols.
- Employee education programs that create a culture of confidentiality whereby employees understand the value of protecting company data.
- Effective trade secret protection measures that take into account new technologies and threats, including cyber threats and social media/cloud computer issues.

Please see our recorded webinar on Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours for more details.

U.S. Treasury Department Suggests That Non-Compete Reform is Necessary

By Erik Weibust and Andrew Stark (April 28th, 2016)

The U.S. Department of Treasury recently released a study on the effect of non-compete agreements, taking a hard line with respect to their social and economic benefits and purported harms. Specifically, while the authors of the study acknowledge that in some cases non-compete agreements can promote innovation, they ultimately conclude that the potential harm of misuse by employers outweighs those benefits.

Recent Research

According to the study's authors, recent research suggests that about 18 percent of American employees, amounting to nearly 30 million people, are currently covered by non-compete agreements; and nearly 37 percent of workers report having worked under one at some point during their career. Workers bound by non-compete agreements are not just limited to the highly educated or compensated. In fact, 15 percent of workers without a four-year college degree and 14 percent of workers earning less than $40,000 per year are bound by them.

Purported Costs vs. Benefits of Non-Compete Agreements

Although the authors of the Treasury Department study acknowledge that non-compete agreements can have social benefits in some situations, such as (1) protecting trade secrets, thereby promoting innovation; (2) reducing the probability of employees resigning, thereby increasing employers' incentives to provide costly training; and (3) allowing employers with historically high turnover to use non-competes to match with workers who have a low desire to switch jobs in the future, they place greater emphasis on what they believe to be serious downsides to non-compete agreements as well. Specifically, according to the authors, non-compete agreements can (1) result in lower wages after the agreement is signed; (2) discourage workers from re-entering their field in its entirety once they are terminated, thereby foregoing accumulated training and experience in certain fields; and (3) reduce job churn, which helps raise labor productivity by achieving a better matching of workers and employers.

The authors go on to express concern that a growing body of evidence suggests that employers are taking advantage of their employees' incomplete understanding of such agreements, resulting in a purported lack of transparency and fairness. For example, employers often require workers to sign non-compete agreements in states that refuse to enforce them, such as California. Other employers fail to inform candidates about the existence of such agreements in their job offers. Further, according to the authors of the study, only 10 percent of workers with non-compete agreements report bargaining over the terms of their non-compete agreements, with 38 percent of those not even realizing that they could have negotiated the agreement.

The authors of the Treasury Department study also suggest that while protection of trade secrets undoubtedly seems to be a legitimate justification for these agreements, about 18 percent of workers bound by non-compete agreements are in fields like personal services and installation and repair, in

which such purportedly should not be a concern. The authors of the study question the legitimate business purpose of imposing non-competes on employees such as fast food restaurant workers, as it is not likely that they will possess any trade secrets or proprietary training. Along those lines, we recently reported on a case in which a trial court struck down a beauty salon's non-compete agreement because it lacked a legitimate business purpose.

These characteristics, the authors of the study suggest, may have a negative impact on the national economy by reducing job mobility, and lowering wage growth and initial wages. According to the authors, research has shown the stricter the non-compete enforcement to be in a particular state, the lower the wage growth and initial wages. Given that job switching is generally associated with substantial wage increases, the resulting increased difficulty of switching jobs would purportedly reduce wage growth over time.

The Study's Recommendations

Based on the foregoing, the authors of the Treasury Department study recommend that (1) policy makers should inject more transparency into the world of non-compete agreements; and (2) employers should only use enforceable non-competes, align them with legitimate social purposes like the protection of trade secrets, and require consideration for workers to be bound by such agreements, such as severance packages. This would purportedly better protect the employer's business interests, limit the harm to workers, but most important it would preserve the more socially valuable agreements and chip away the least valuable, as employers would be hesitant to incur costs on them. Of course, other than the additional consideration piece (in many states continued employment is sufficient), these are all things that we recommend to our clients, and on which most non-compete agreements are generally based in any event (at least those that are enforceable in most states).

Takeaways

The study only addresses the effects of non-compete agreements, not other types of restrictive covenants, such as customer and employee non-solicitation or confidentiality agreements. It is unclear what, if any, effect this Treasury Department study will have on policy makers, but we will certainly report on anything that comes of it.

Despite Evidence That Ex-Employee Violated Customer Non-Solicitation Covenant, Injunction Denied Because No "Irreparable" Harm

By Paul E. Freehling (May 6th, 2016)

Touzot was an employee of ROM, a seller of products used in making balsa wood model planes and boats. His employment agreement included a post-termination customer non-solicitation covenant. After he left ROM, he became a competitor. The company sued him and his Ecuadorian supplier of balsa wood, which previously had been ROM's supplier, alleging that they were colluding to steal ROM's customers. Although ROM was found to have satisfied most of the other requirements for injunctive relief, the court held that a monetary award would provide adequate compensation for any damages. *Touzot v. ROM Dev. Corp.*, Civ. Ac. No. 15-6289 (D.N.J., Apr. 26, 2016) (Linares, J.) (not for publication).

Status of the Case

Touzot initiated litigation in a New Jersey state court against ROM. The company is based in Rhode Island. ROM removed the case to federal court and moved to dismiss for lack of personal jurisdiction. While the motion was pending, ROM filed its own lawsuit in Rhode Island federal court, charging breach of contract, misappropriation of trade secrets, tortious interference, etc. ROM sought and obtained from the judge in Rhode Island a temporary restraining order, but it was stayed pending a determination of which court should adjudicate the dispute.

After ROM's motion to dismiss the New Jersey case was denied, the Rhode Island suit was transferred to New Jersey for consolidation with the case there. A few days ago, Judge Linares issued his opinion denying ROM's application for a preliminary injunction and granting the motion filed by Touzot and his balsa wood supplier to dissolve the TRO.

Background

By 2011, ROM had sustained a sharp decline in the volume of its quite profitable sales of balsa wood products, partly because of a shortage of balsa wood. Hoping to improve its sales, ROM hired Touzot who introduced the company to a supplier in Ecuador which had abundant quantities of balsa wood and became ROM's principal source. Touzot was ROM's contact person with the supplier as well as ROM's sales representative for its model wood customers (according to ROM, the customers, unlike the supplier, previously were unknown to Touzot).

Once ROM had an adequate supply of balsa wood, its model products sales took off. Nevertheless, after four years the company fired Touzot who then formed his own company to sell balsa wood model products. ROM's supplier announced dramatically increased prices for sales of balsa wood to ROM, which would have eliminated its profits for wood model products. However, the supplier sold balsa wood to Touzot at the old, lower prices. Other suppliers of balsa wood did not raise their prices but, as

before, they did not have the capacity to satisfy ROM's needs. Consequently, the company could not compete effectively with Touzot, and many of its former customers became his customers.

The Restrictive Covenants

Touzot's employment agreement with ROM contained multiple restrictive provisions (non-compete, non-solicitation, trade secret confidentiality, etc.). The only covenant ROM sought to enforce with an injunction was Touzot's promise that for two years after termination he would not solicit anyone in "the Americas" who was a ROM customer during his employment for orders with respect to products similar to those sold by ROM.

Injunction Standards

In his opinion, Judge Linares stated that, whether New Jersey or Rhode Island law applied, ROM was required to show that (1) it was likely to succeed on the merits, (2) the balance of equities favored ROM, (3) an injunction was in the public interest, and (4) ROM would suffer irreparable harm if the injunction were not issued. He wrote that ROM was likely to be able to prove that Touzot solicited its customers, and that he sold products substantially similar to those it sold. The time and geographical restrictions were found to be reasonable. Touzot was said to have admitted that he could obtain employment without violating the non-solicit restriction and simply chose not to do so. However, regarding the fourth prong, the judge ruled that if ROM could prove lost sales as a result of Touzot's covenant violations, a monetary award would provide adequate relief.

Takeaways

The same evidence admitted at an injunction hearing frequently is offered at a subsequent trial on the merits, and the ruling on a motion for entry of a preliminary injunction often is a good predictor of the likely judgment at trial. For these reasons, many cases settle after an injunction hearing and ruling. Of course, Judge Linares stressed that his decision applied solely to the motion for preliminary injunctive relief and was not dispositive with respect to the merits of (a) the parties' differing interpretations as to the meaning of the non-solicitation covenant, much less (b) ROM'S allegation that Touzot breached it.

The court did not really address the public interest prong of the injunction standards. Yet, if Touzot is enjoined from selling to model wood customers for two years, they might be unable to locate an alternative source for the product during that period. On the other hand, there is a public interest in holding contracting parties, especially relatively sophisticated parties, to the contractual commitments they make.

In his opinion, Judge Linares pointed out that monetary relief is rarely adequate for breach of a confidentiality covenant which puts another's trade secrets into the public domain. On the other hand, many courts recently have denied motions for injunctions with respect to violations of various covenants, holding that compensatory damages can be an adequate remedy when the injury consists of provable lost sales and profits.

White House Issues A Call To Arms With Respect To Non-Competes

By Erik Weibust and Andrew Stark (May 6th, 2016)

On May 5, 2016, the White House issued a report largely piggybacking on a recent U.S. Treasury Department study, on which we previously posted, with a primary focus on the purported misuse and negative impacts of non-compete agreements. The White House report reiterated much of what the Treasury Department covered its March 31, 2016 study, and focused on how the White House will apparently begin to "facilitate discussion on non-compete agreements and their consequences."

Indeed, on the same day that the White House issued its report, Vice President Joe Biden posted a lengthy message on his Facebook page, linking to a White House survey that encourages employees to share with the administration "how non-competes agreements or wage collusion are holding you down." The Vice President expressed concern in his post about "the improper use of non-compete agreements, where companies make workers promise when they are hired that if they leave the company, they can't work for another company in the same industry," and noted that "these agreements can create unnecessary roadblocks for any worker trying to get a raise, looking to move up the ladder by joining another employer, or even start their own company." He concluded by promising that "the President and I will continue to fight for the dignity and respect of hardworking Americans," including "put[ting] forward a set of best practices and call to action for state legislators to make progress on reforms to address the misuse of non-competes."

Like the U.S. Treasury Department, the authors of the White House report briefly acknowledge that, in some cases, non-compete agreements can play an important role in protecting businesses, promoting innovation, and encouraging greater employer investment in their workers. They ultimately conclude, however, that the potential harm of misuse by employers, and effects on wages, labor market dynamism, innovation, entrepreneurship, and regional economic growth outweighs those benefits. The authors further noted the "growing movement in states to take action to limit the misuse of non-compete agreements," specifically highlighting that several states have taken steps to limit the scope and duration of non-compete agreements, noting for example Hawaii's ban on non-compete agreements for technology jobs and New Mexico's recent ban on non-compete agreements for health care jobs.

The authors go on to list seven areas in which they believe that workers may be disadvantaged by non-competes, and gives examples of how state legislatures are attempting to address the issues. The issues include (1) compelling workers who are unlikely to possess trade secrets to sign non-competes, (2) having new employees sign a non-compete only after accepting a job offer, (3) not explaining the implications and enforceability of such agreements to employees, (4) drafting overly broad or unenforceable agreements,(5) requiring non-competes without consideration beyond continued employment, (6) restricting employees after they are fired without cause, and (7) the purported detrimental health and well-being effects by restricting consumer choice.

The authors note that in the ensuing months, the White House, the Treasury Department, and Department of Labor will convene a group of experts in labor law, economics, government and business to facilitate discussion on this matter. "The goal will be to identify key areas where implementation and enforcement of non-competes may present issues, to examine promising practices in states, and put forward a set of best practices and call to action for state reform." They also stress that research must continue to assess and identify policy reforms and how such reforms will impact the non-compete world. Lastly, the authors emphasize that ultimately the power of reform is in the hands of state legislators and policymakers to adopt institutional reforms that strike a balance between the appropriate use of non-competes and the protection of the workers subjected to them.

No Microscope Needed to See Why This Noncompete Is Unenforceable

By James D. McNairy and Michael Cross (May 10th, 2016)

When is a microscope not needed? When the problem one is looking at is big as an elephant, not small as an amoeba.

Nion, an electron microscope manufacturer, contracted with Gatan, a spectrometer manufacturer, to use Gatan's spectrometers in Nion's microscopes. The contract contained both confidentiality and non-compete clauses. When Gatan learned that Nion had sold other parties microscopes that used Nion's own spectrometer, Gatan sued, claiming that Nion had breached the non-compete (but not the confidentiality) provision of the contract. In ruling on Nion's motion to dismiss, the court found that the non-competition provision was void and that Gatan's claim that the provision was necessary to protect its trade secrets was without merit. *Gatan, Inc. v. Nion Company*, 2016 WL 1243477 (N.D. Cal. Mar. 30, 2016).

Gatan proffered some interesting arguments in opposition to Nion's motion (kind of like your mother said it was "interesting" when you cut your own hair at the age of 5 using some rusty scissors that you found in the neighbor's yard). Though Gatan's complaint captioned a trade secret claim, it never used the word "misappropriate" anywhere in its complaint. Gatan also asserted that the covenant not to compete in its contract with Nion protected Gatan's trade secrets. But the non-compete covenant said nothing whatsoever about trade secrets.

In making its arguments, it appears that Gatan was shooting for the so-called "trade secrets exception" to California Business and Professions Code 16600 (prohibiting covenants not to compete), but unfortunately had somewhat of a misfire. Still, the court's order contains some notable analysis.

First, the court acknowledges that there is a trade secret exception to California's prohibition on covenants not to compete. As we have discussed in earlier blogs, here and here, California courts are split on whether there is a trade secret exception to BPC 16600. Some, like those cited in the *Gatan* order, believe that an exception exists. Others, like *Ret. Grp. v. Galante*, 176 Cal. App. 4th 1226 (2009), deny (in dicta) that such an exception does or even needs to exist. Unfortunately, the *Gatan* court did not advance this discussion.

So lesson #1 from *Gatan*: If one is going to invoke the "trade secrets exception" to BPC 16600, then the covenant not to compete better expressly make reference to the alleged "trade secrets." Companies cannot, as Gatan did, simply point to a theoretical exception to the rule as a way to enforce what some would argue is a facially void clause. As the court wrote, "under any reading of the Agreement …, [the non-compete clause] cannot be considered 'necessary' to protect Gatan's trade secrets"—the court found that the agreement's separate confidential information provision sufficiently did this.

Second, *Gatan* cites to *Golden v. California Emergency Physicians Med. Grp*., 782 F.3d 1083 (9th Cir. 2015), for the proposition that BPC 16600 applies in the business-to-business context as much as in the employer-to-employee context, on the ground that the section "does not specifically target covenants not to compete between employees and their employers." (See our blog on *Golden* here.) Other courts have held similarly. *See, e.g*., *Jan Marini Skin Research, Inc. v. Allure Cosmetic USA, Inc*., 2007 WL 1508686, at *13 (Cal. Ct. App. May 24, 2007), as modified on denial of reh'g (June 25, 2007) (unpublished) ("While many cases applying section 16600 arise in the context of an employer-employee relationship, the statute also applies to other contracts, such as manufacture or distributorship agreements between businesses or individuals."); *Richmond Techs., Inc. v. Aumtech Bus. Sols*., 2011 WL 2607158, at *17 (N.D. Cal. July 1, 2011).

Perhaps time will tell if *Golden* and *Gatan* accurately predict the breadth of BPC 16600. In the meantime, one thing appears clear: if one seeks to enforce a covenant not to compete on the basis that the covenant is needed to protect trade secrets, the covenant better at least mention the term "trade secrets" at least before Judge Hamilton in the Northern District of California.

Georgia's Restrictive Covenants Act Turns Five Years Old: Assessing the Impact of Georgia's Law Five Years On

By Daniel P. Hart, Bob Stevens, and Alex Meier (May 12th, 2016)

While the federal Defend Trade Secrets Act is garnering a great deal of attention, it's worthwhile to remember that state law remains critically important in drafting restrictive covenants. This week, May 11, 2016, marks the fifth anniversary of Georgia's revised trade secrets act, which fundamentally recast how courts view and enforce restrictive covenants.

Prior to enactment of the new law, Georgia was one of the most difficult states in which to enforce restrictive covenants against employees. As a result, before the revised act, employees sometimes moved to Georgia to take advantage of Georgia's extremely pro-employee public policy. (In fact, some lawyers commented — only half -jokingly — that their clients should go to Las Vegas to get out of their marriage and go to Atlanta to get out of their non-compete.)

The new act implemented a sea change in Georgia's public policy towards restrictive covenants. The new act substantially liberalizes drafting requirements for restrictive covenants in Georgia (which, before the new act, were governed by a series of arcane court decisions that imposed a variety of highly technical drafting requirements). Perhaps most notably, the new act permits Georgia courts to "blue pencil" or partially enforce overbroad restrictive covenants (though the Georgia courts have had few opportunities to exercise that new power). As a result, with enactment of the new law, Georgia is one of the more favorable jurisdictions for enforcement of restrictive covenants in employment agreements.

In our one-year anniversary post on the act's passage, we made three predictions: (1) Georgia courts would be considerably more likely to enforce restrictive covenants under the new act than they had under prior Georgia law, (2) Georgia courts would "blue pencil" overbroad restrictive covenants, and (3) Georgia courts would continue to apply prior Georgia law to agreements that predate the new act. Five years later, the jury is still out. Few published or appellate decisions have examined the revised act. Although some trial courts have grappled with the act in recent years, there has not been enough time for agreements signed after May 11, 2011 to make their way into more than a handful of published or electronically-available decisions.

Nevertheless, one decision over the past few years, *Cellairis v. Duarte*, is particularly notable. That case (which we previously examined here as an illustration of the difficulties in drafting effective carveouts from arbitration provisions) suggests that courts are more likely to enforce restrictive covenants under the new law, just as we predicted four years ago.

In *Cellairis*, a franchisor sued a former employee who, at various times, worked as an officer, employee, and independent contractor. A 2014 franchise agreement between the franchisor and

employee obligated the employee to refrain from owning or operating a competing business within 10 miles of any franchise operating as of the termination date. The franchise agreement also contained a two-year non-solicitation provision prohibiting the employee from soliciting any customer who the franchisee *or* the employee did business with in the two years preceding the agreement's termination.

The franchisor moved for and obtained a preliminary injunction. The court sidestepped the employee's multifaceted career with the franchisee by analyzing the restrictive covenants as if the employee worked only as an employee.

The court quickly found that a two-year restriction was "presumptively reasonable" under Georgia's new act and brushed aside the employee's attempts to argue that it was still unreasonable. The court also honored the new act's position on geographic limitations; it held that a 10-mile radius from *any* franchise, even those that did not exist when the agreement was signed, was reasonable.

Unlike previous restrictive covenant decisions, the court *did not* limit the non-compete and non-solicitation to customers that the employee managed. This is a clear departure from pre-amendment Georgia law, which routinely struck down restrictive covenant agreements that were untethered from customers managed by the former employee.

Finally, the court found that the public interest now *favored* the entry of a preliminary injunction because "reasonable restrictive covenants . . . serve the legitimate purpose of protecting business interests and creating an environment favorable to attracting commercial enterprise to Georgia and keeping existing businesses within the state." Formerly, the public interest element always weighed against imposing a preliminary injunction. This decision suggests a party moving for a preliminary injunction can always cite to public interest as a factor favoring preliminary injunctive relief because even overly broad restrictive covenants can be "blue penciled" to reasonable limitations on competition.

Takeaways

The *Cellaris* decision illustrates the profound impact that the new act has on restrictive covenants signed on or after May 11, 2011. Restrictive covenant agreements governed by pre-act law remain vulnerable. Employers with restrictive covenants signed before May 11, 2011 should sign new agreements to erase any doubts about which law governs. (Some decisions have found that pre-act restrictive covenants amended after May 11, 2011 are still governed by pre-act law.)

Employers should also feel more comfortable about seeking preliminary injunctive relief if they can present evidence that a former employee is violating a restrictive covenant. With the public interest on its side and a blue pencil in hand, courts seem less hesitant to impose preliminary injunctive relief — even though the federally governed standard for preliminary injunctive relief has not changed.

Finally, practitioners should look to federal Alabama and Florida decisions until Georgia state courts have established Georgia's position on post-act restrictive covenants. The *Cellaris* court looked to Florida law to guide its analysis. Without any binding authority, these out-of-state decisions should serve as a rough proxy for how much evidence a district court wants to see before it grants preliminary injunctive relief.

If you have any questions about how the May 2011 revisions to Georgia's law on restrictive covenants affects your restrictive covenants portfolio, or if you would like assistance drafting compliant agreements for your workforce, please contact a Seyfarth Shaw Trade Secrets Group attorney.

Webinar Recap! Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?

By Gary Glaser and James D. McNairy (May 13th, 2016)

We are pleased to announce the webinar "Trade Secrets, Restrictive Covenants and the NLRB: Can They Peacefully Coexist?" is now available as a podcast and webinar recording.

In Seyfarth's fifth installment of its 2016 Trade Secrets Webinar series, attorneys Gary Glaser, Jim McNairy and Marc Jacobs conveyed strategies and best practices to help you, as in-house counsel and HR professionals, to ensure that your company and internal clients are protected.

As a conclusion to this well-received webinar, we compiled a list of brief summaries of the more significant cases that were discussed during the webinar:

- The National Labor Relations Act applies to all private sector workplaces — not just unionized facilities. Among other things, the Act protects an employee's right to engage in protected concerted activities, which in general are group action (usually by two or more employees) acting together in a lawful manner, for a common, legal, work-related purpose (e.g., wages, hours and other terms and conditions of employment). Limits on these rights and retaliation against an employee for engaging in protected concerted activity violates the Act. The National Labor Relations Board is aggressively protecting employees' rights to engage in protected concerted activity. As part of this effort, the NLRB will find unlawful workplace rules, policies, practices and agreements that explicitly restrict Section 7 activities (such as a rule requiring employees to keep their wage rate confidential) or that employees would reasonably believe restricts their Section 7 rights (e.g., a confidentiality agreement or policy that generally includes in the definition of confidential information "personnel information").

- In the 2015 *Browning-Ferris Industries* decision, the NLRB substantially broadened the definition of "joint employer". Under this new expanded definition, an entity can be found to be a joint employer if it has the authority, even if unexercised, to control essential terms and condition of employment. As a result, if one entity has agreements with other entities to provide labor or services, that entity may be a joint employer of the other entities' employees based on the level of control it has over the terms and conditions of employment of the other entities/ employees. One indicia of that control would be requirements for hiring or employment, such as requirements to sign agreements or adopt policies for the protection of confidential information and similar restrictions.

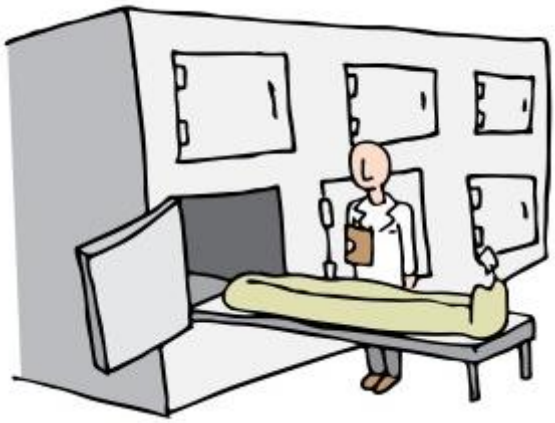
- As a result, and also because of the signing of the federal Defend Trade Secrets Act, now is a critical time for all employers to review their policies, practices, procedures and agreements (1) regarding the protection of confidential information; and (2) with third-party service and labor providers. In reviewing confidential information policies and agreements, the focus should be

on narrow tailoring using specifics and examples to protect information that lawfully may be protected in a lawful manner. For agreements with parties, the review should include an analysis of the factors that may show joint employer status so that you can balance the risk of a joint employer finding with the needs to protect your organization.

Bring Out the Body Bags: Seller's Covenant, In Asset Sales Agreement, Not To Compete Within 150 Miles For 10 Years Unenforceable

By Paul E. Freehling (May 20th, 2016)

Palmetto bought the assets of Knight Systems' mortuary transport business. The agreement of purchase and sale included (a) Palmetto's commitment to buy body bags, at specified discounted prices, exclusively from Knight Systems for 10 years, and (b) Knight Systems' promise not to provide mortuary transport services within 150 miles of Palmetto's offices for the same period. Notwithstanding the non-compete covenant, a few years later Knight Systems submitted a timely proposal — and was selected — to provide those services to a Palmetto customer within the 150-mile territory. Palmetto sued Knight Systems for breach of contract, won below, but lost in the South Carolina Court of Appeals.



Status of the Case

By consent, Palmetto's complaint and Knight Systems' counterclaim were tried before a court-appointed referee. Concluding that the geographic restriction in the non-compete was reasonable, he ruled in favor of Palmetto and awarded $373,000. The Court of Appeals reversed and remanded. *Palmetto Mortuary Transport, Inc. v. Knight Systems, Inc.*, No. 2014-001819 (S.C. Court of Appeals, May 4, 2016).

Background

Four years after the purchase and sale transaction, Palmetto customer Richland County published a RFP with regard to providing mortuary transport services to the county for five years. The day before the deadline for responding, Knight Systems accused Palmetto of purchasing body bags from others in violation of its commitment to buy those products exclusively from Knight Systems. Palmetto replied that it had spent a minimal amount, less than $450 (1% of the aggregate amount it had paid Knight Systems), for products covered by the contract's exclusivity provision.

Knight Systems was the only source for the odor-proof body bags required by the RFP. Shortly before the contract was awarded, it informed Richland County that it (Knight Systems) intended to take those products off the market. This would leave Palmetto unable to satisfy a contractual condition. Whether for this reason or otherwise, and despite Palmetto's contention that it had submitted the most favorable proposal, Knight Systems was awarded the contract.

Reversal of the Referee's Decision

The only issue addressed on appeal was the reasonableness of the geographic limitation in the assets sale agreement. According to the court, the referee cited two bases for his conclusion that the limitation was reasonable.

- Palmetto's owner testified that it wanted the 150-mile restriction included in the purchase and sale agreement because, although Knight Systems did mortuary transport business in only two South Carolina counties, Palmetto was considering an expansion of the territory. The appellate tribunal held that this testimony did not justify a restriction encompassing parts of three states, especially since there was insufficient "evidence of definitive planning, acquisitions, or other overt acts" in support of possibly enlarging the service area.

- A Knight Systems owner testified that the company did not object to including the restriction in the agreement because, at that time, Knight Systems had not intended to get back into the business after the sale to Palmetto. The court said Knight Systems' "intention of not returning to the mortuary transport business is [not] a relevant factor for analyzing whether a territorial restriction is reasonable."

Lastly, the Court of Appeals addressed the possibility of "blue penciling" the 150-mile restriction. That would be permissible under South Carolina law, the judges said, only if the agreement authorized redrawing the provision. The Palmetto-Knight Systems contract did not so authorize. Accordingly, blue penciling would mean inserting "an arbitrary term" as to which the parties neither negotiated nor agreed.

Takeaways

Many judicial opinions state that restrictive clauses in a non-compete contained in an *employment agreement* must be reasonable or they are subject to being invalidated. *Palmetto* makes the same point regarding restrictions in an *assets sale contract*.

Palmetto also teaches that when drafting a non-competition and/or a non-solicitation clause for an employment or sales agreement, consider authorizing a decision-maker to modify unreasonable geographic and duration provisions. However, trade secret confidentiality clauses — not involved in the *Palmetto* case — rarely are invalidated because of allegedly unreasonable territorial or time restrictions (such clauses are subject to being stricken in their entirety by a court holding that there is no substantial risk of disclosure).

Court Upholds Non-Compete Giving Former Employer Discretion To Determine Whether Ex-Employee Is Working For A Competitor

By Paul E. Freehling (June 15th, 2016)

A severance agreement executed in connection with a Stark Truss employee's resignation included a one-year non-competition clause. It allowed the company unfettered discretion to decide if his new employer was a competitor and, if so, to terminate his severance. The ex-employee took another job and sued Stark Truss in an Ohio court, seeking a declaration that he was entitled to 100% of his severance. The trial court's judgment for Stark Truss was affirmed on appeal. *Saunier v. Stark Truss Co.*, Case No. 2015CA00202 (Ohio App., May 23, 2016).

The Parties

Stark Truss is an Ohio manufacturer and distributor of wood and steel components used in building construction. Saunier, a 35-year employee, was the company's asset manager. Immediately after his separation from Stark Truss, Saunier accepted a similar position, nearby, with Carter Lumber.

Stark Truss' "Sole Discretion"

Under the severance agreement, Start Truss had "sole discretion" to denominate Saunier's subsequent employer a "Competitor." The definition of "Competitor" was a business located within 100 miles of Stark Truss and "substantially similar" to that company. Saunier was required to provide the company with detailed information concerning his new employment. If Saunier affiliated with a "Competitor" within one year from his separation date, he forfeited further severance payments. Stark Truss determined that Carter Lumber was a "Competitor."

Ruling on Appeal

The Court of Appeals noted that both parties were represented by counsel in negotiating the Severance Agreement. Consistent with several Ohio judicial decisions involving a "sole discretion" contract provision in other contexts, the appellate tribunal determined that the clause was unambiguous and was valid.

The court did not address the issue of whether Stark Truss' "sole discretion" was without limitations. Perhaps the judges concluded that the company's determination was within the bounds of sound judgment and, therefore, it was reasonable. Nor did the judges say whether the same ruling would have been issued to a "sole discretion" provision in a traditional employment contract non-compete rather than a severance agreement.

Takeaways

The *Saunier* appellate court held that, under the circumstances there, an employer may reserve to itself the unilateral right to decide whether an employee has violated a non-compete. Is such "sole discretion" unqualified? Probably not.

There are very few reported decisions mentioning, much less adjudicating, the limits of a "sole discretion" contract provision in a non-compete context.

- One opinion that refers to a "sole discretion" provision within a non-compete agreement is *SkyHawke Technologies LLC v. Unemployment Commission*, 27 A.3d 1050, 1052-53 (Pa. Commonwealth Court 2011). However, the court did not address the provision's validity. There, an individual had a contract to provide services to a company. He was permitted to furnish similar services to others, but he could be fired if the company determined, in its "sole discretion," that his performance of those similar services was not in its best interests. The company apparently made such a determination and terminated the contract. The litigation concerned (a) the individual's claim that he had been an employee and was entitled to unemployment compensation, and (b) the company's counter that he had been an independent contractor to whom no such compensation was owed. The court ruled in favor of the company but without significant discussion of the "sole discretion" provision.

- A case holding that "sole discretion" sometimes is unlimited is *Sunshine Gas. Distributors, Inc. v. Biscayne Enterprises, Inc.*, 39 So.3d 978 (Fla. App. 2014). Each party to a lease had "sole discretion" to decide whether or not to renew. The jurists stated that imposing a duty of "good faith and fair dealing" with respect to a contract containing what they called a "binary choice" would frustrate, rather than protect, the parties' interests. 39 So.3d at 980 n.1.

- However, an older Florida Appellate Court decision, *Cox v. CSX Intermodal, Inc.*, 732 So.2d 1092, 1097-98 (1979), explained when a "good faith and fair dealing" requirement should be imputed with respect to an exercise of "sole discretion." In the jurists' view, if a "broad range of authority is reposed in one party" to a contract, "the reasonable expectations" of the parties may need to be protected from an arbitrary discretionary decision. So, if the parties seem to have anticipated that community standards of honesty, decency and reasonableness would be applied, "good faith and fair dealing" is required. Although the *Cox* lawsuit did not involve a non-compete, the same principles might well be applied to an employer exercising "sole discretion" to decide whether an ex- employee is engaging in prohibited competition.

Webinar Recap! Enforcing Trade Secret and Non-Compete Provisions in Franchise Agreements

By John Skelton, Dawn Mertineit, and James Yu (July 1st, 2016)

As a thank you to our valued readers, we are pleased to announce the webinar "Enforcing Non-Compete Provisions in Franchise Agreements" is now available as a podcast and webinar recording.

In Seyfarth's seventh installment in its series of Trade Secrets Webinars, Seyfarth attorneys John Skelton, James Yu and Dawn Mertineit focused on the importance of State specific non-compete laws and legislation and recent Federal and State efforts to regulate the use of non-compete agreements; enforcement considerations for the Franchisee when on-boarding and terminating employees; and lessons learned from recent decision regarding enforcing non-compete provisions upon termination and non-renewal.

As a conclusion to this well-received webinar, here are three key takeaway points:

- As reflected by the May 5, 2016, White House report (*Non-Compete Agreements: Analysis of the Usage, Potential Issues, and State Responses*), state and federal non-compete legislative proposals and recent enforcement action by the Illinois Attorney General challenging the use of non-compete agreements for lower level employees, Franchisors and Franchisees need to anticipate more regulation and scrutiny.

- With respect to their own employees, Franchisors and Franchisees need to develop and implement on-Boarding, termination and other procedures designed to ensure that both departing and prospective employees understand their ongoing obligations with respect to the company's confidential and proprietary information and trade secrets and that such information is protected throughout the employment relationship.

- The enforceability of non-compete provisions are most often litigated in the context of a request for a preliminary injunction and several recent decisions confirm that to enforce a non-compete against a departing franchisee the franchisor (1) should be able to show harm to actual competition; (2) needs to act promptly and that enforcement delays likely means that any alleged harm is not irreparable; and (3) should develop and implement a post-termination plan beyond simply sending a notice of termination as the franchisor will need to present evidence of actual harm.

All or Nothing: Nevada Supreme Court Refuses to Adopt "Blue Pencil" Doctrine for Non-Compete Agreements

By Salomon Laguerre (August 4th, 2016)

In a recent opinion, the Supreme Court of Nevada refused to adopt the "blue pencil" doctrine when it ruled that an unreasonable provision in a non-compete agreement rendered the entire agreement unenforceable. "Blue penciling" refers to a court's willingness to strike unreasonable clauses from a non-compete agreement, leaving the rest of the agreement to be enforced; or to modify the agreement to reflect terms that are reasonable under the law. Many jurisdictions permit "blue penciling" while others have refused to adopt the doctrine.

Traditionally, Nevada courts have followed the latter approach by refraining from reforming or "blue penciling" parties' private contracts, including non-compete agreements. The case of *Golden Road Motor Inn, Inc. v. Islam*, presented the Supreme Court of Nevada with an opportunity to join the number of jurisdictions that have embraced the doctrine. For various reasons, the Court refused to do so.

The *Islam* case involved a dispute between a casino worker and his former employer. The worker, who worked as a casino host for the former employer, entered into an agreement with the former employer to refrain from working for any other gaming establishment within 150 miles of the former employer for one (1) year following the end of his employment with the former employer. After resigning from his employment with the former employer, the worker began working as a casino host for a new employer within the prohibited 150-mile radius. The former employer sued the worker to prevent his employment with the new employer.

The Court found the non-compete agreement's prohibition of all types of employment with a gaming establishment within 150 miles of the former employer was overbroad, as such a prohibition extended beyond what was necessary to protect the former employer's interests. The Court also found such a prohibition severely restricted the worker's ability to be gainfully employed. Finding this provision unreasonable, the Court declared the entire agreement unenforceable.

The former employer asked the Court to modify the overbroad provisions of the non-compete agreement to render the agreement enforceable. Rejecting the former employer's argument, the Court stated that it was not its role to rewrite the parties' contract and that courts are not empowered to make private agreements. The Court explained that its restraint from "the urge to pick up the pencil" to modify the non-compete agreement avoids trampling the parties' contractual intent, preserves judicial resources, and holds the employer, as the drafter of the agreement, to a higher standard. The Court explained that under a "blue pencil doctrine," the employer receives what amounts to a "free ride" on the unreasonable provision, perhaps knowing that the provision would never be enforced. Consequently, the Court stated, the practice of "blue-penciling" encourages employers with superior bargaining power to "insist upon unreasonable and excessive restrictions, secure in the knowledge that

the promise will be upheld in part, if not in full." This, the Court maintained, forces the employee to bear the burden as employers "carelessly, or intentionally overreach."

In light of this opinion, employers conducting business in Nevada should ensure that non-compete agreements with their employees are reasonably necessary to protect the employers' interests. This means that the scope of activities prohibited, the time limits, and geographic limitations contained in the non-compete agreements should all be reasonable. If an agreement contains even one overbroad or unreasonable provision, the employer risks having the entire agreement invalidated and being left without any recourse against an employee who violates the agreement. Employers should consult with an attorney if they have any concerns about the enforceability of their non-compete agreements with their employees.

D.C. Circuit Upholds NLRB Finding that Employment Agreement's Confidentiality and Non-Disparagement Provisions Violated the NLRA

By Ashley Laken (August 9th, 2016)

Cross Posted from Employer Labor Relations Blog.

Seyfarth Synopsis: *The U.S. Court of Appeals for the D.C. Circuit recently denied Quicken Loans, Inc.'s petition for review of an NLRB decision finding that confidentiality and non-disparagement provisions in the company's Mortgage Banker Employment Agreement unreasonably burdened employees' rights under Section 7 of the NLRA.*

Back in 2013, an NLRB administrative law judge found that certain confidentiality and non-disparagement provisions contained in Quicken's Mortgage Banker Employment Agreement violated the NLRA (see our earlier blog post here). The Board agreed with the ALJ, and the Company petitioned the D.C. Circuit for review. Recently a three-judge panel of the D.C. Circuit denied the Company's petition for review and granted the NLRB's cross-application for enforcement, finding that there was nothing arbitrary or capricious about the Board's decision and there was no abuse of discretion in the Board's hearing process (Case No. 14-1231).

Facts

As a condition of employment, mortgage bankers were required to sign a Mortgage Banker Employment Agreement that included a confidentiality provision and a non-disparagement provision. The confidentiality provision prohibited employees from disclosing nonpublic information regarding the company's personnel, including personnel lists, handbooks, personnel files, and personnel information of coworkers such as phone numbers, addresses, and email addresses. The non-disparagement provision prohibited employees from publicly criticizing, ridiculing, disparaging or defaming the company or its products, services, policies, directors, officers, shareholders or employees.

Court's Reasoning

The D.C. Circuit noted that its review of the Board's decision was limited, as Congress has entrusted the Board with implementing Sections 7 and 8(a)(1) of the Act and determining when an employer's workplace rules run afoul of those provisions. The three-judge panel noted that the Board's determinations are therefore entitled to considerable deference and will be sustained as long as the Board "faithfully applies" the legal standards and its textual analysis of a challenged rule is "reasonably defensible" and adequately explained.

In finding that the Board properly determined that the confidentiality provision violated employees' Section 7 rights, the court noted that the very information the provision forbids employees from sharing (i.e., personnel lists and employee rosters) has long been recognized as information that employees must be permitted to gather and share among themselves and with union organizers. With respect to the non-disparagement provision, the court found that the Board "quite reasonably found that such a sweeping gag order would significantly impede mortgage bankers' exercise of their Section 7 rights because it directly forbids them to express negative opinions about the company, its policies, and its leadership in almost any public forum."

In reaching its conclusions, the appeals court noted that the validity of a workplace rule turns not on subjective employee understandings or actual enforcement patterns, but on an objective inquiry into how a reasonable employee would understand the rule's disputed language. The court observed that this approach serves "an important prophylactic function: it allows the Board to block rules that might chill the exercise of employees' rights by cowing the employees into inaction," rather than forcing the Board to wait until that chill is manifest and then try to undertake the difficult task of dispelling it. The court also noted that the absence of enforcement "could just as readily show that employees had buckled under the Employment Agreement's threat of enforcement."

Employer Takeaway

In recent years, the Board has issued numerous decisions in which workplace rules were found to unlawfully restrict employees' Section 7 rights, and the D.C. Circuit's decision demonstrates that employer petitions for review of such decisions may not be successful. The decision also highlights the need to not just draft and review employee handbooks and policies for possible non-compliance with the NLRA, but employment agreements as well.

Federal Court Rejects Foreign Employee's Attempt to Avoid Forum Selection Clause on Grounds He Signed Under Duress Upon Arriving in U.S.

By Andrew Stark and Erik Weibust (October 24th, 2016)

Earlier this fall, the U.S. District Court in Massachusetts transferred an employee's declaratory judgment action to the Eastern District of Michigan pursuant to a forum-selection clause in a non-compete agreement over the employee's argument that he had signed the agreement under duress because he was not told he would need to sign it until he had already spent the money and traveled all the way from India to the United States. The court also used the value of the employee's annual salary, not just the damages the former employee was seeking to recover, to determine whether the minimum threshold for diversity jurisdiction had been satisfied, because his former employer was seeking to enforce his non-compete and keep him out of work. The case is *Kurra v. Synergy Computer Solutions, Inc.*, No. 15-cv-13952-ADB (D. Mass.).

Summary of the Case

In January 2014, Rishi Vas Kurra entered into an agreement with an affiliate of Synergy Computer Solutions ("Synergy"), an IT staffing firm, while living in India, under which Synergy agreed to employ him in the United States for 18 months and to apply for an H-1B visa on his behalf. As part of the agreement, the Kurra agreed to start working for Synergy within 18 months, and if he were to leave Synergy within that time period, he would reimburse the company for his visa processing fees and travel expenses. Kurra alleged that when he arrived to the United States, Synergy required him to sign a non-compete agreement, despite never disclosing this agreement to him when he had agreed to move. Kurra signed the non-compete and was placed at a technology company (although he remained an employee of Synergy).

A few months later, the technology company offered Kurra a position as a full-time employee and to renew his H-1B visa, which he accepted. When Kurra told Synergy that he was going to work directly for the technology company, Synergy demanded that Kurra repay the $9,500 in visa and travel expenses it had paid to him under his agreement, and reminded him of his non-compete obligations.

In reaction to Synergy's demand, Kurra filed a declaratory judgment action in the Massachusetts Superior Court, seeking to void the non-compete agreement, contending that he signed it under duress when he arrived to the U.S. after moving from India. Synergy removed the case to the U.S. District Court for the District of Massachusetts, and then requested a transfer of the case to the Eastern District of Michigan pursuant to a forum-selection clause in the agreement. In addition to opposing the transfer on the grounds of duress, Kurra sought a remand of the case back to state court, arguing that it did not meet the $75,000 amount in controversy requirement.

In determining whether to transfer the action to the Eastern District of Michigan, the court noted that while Kurra presented an affidavit in which he asserted that Synergy had forced him to sign the non-compete agreement once he landed in the United States, at which point he had no choice but to sign it,

Synergy presented evidence showing that it had presented Kurra with the agreement while he still resided in India, and that he had in fact signed an earlier version of it prior to traveling to the United States. The court thus rejected Kurra's argument that he entered into the non-compete agreement under duress and granted Synergy's motion to transfer the case to Michigan.

Regarding the amount in controversy, the court reasoned that notwithstanding the fact that Kurra only sought to avoid paying $9,500 and void the non-compete agreement, he stood to lose his $110,000 salary should the non-compete be deemed enforceable. Therefore, the court held that the aggregate value of Kurra's claims exceeded the minimum statutory threshold of $75,000.

HR Professionals Take Note: DOJ and FTC Issue Guidance Regarding Antitrust Laws in the Employment Context

By Ashley Laken and Timothy F. Haley (October 26th, 2016)

Cross Posted from Employment Law Lookout.

Seyfarth Synopsis: *On October 20, the DOJ and the FTC jointly issued their Antitrust Guidance for HR Professionals, stating that DOJ intends to pursue employers criminally for alleged wage fixing and no-poaching agreements.*

On October 20, 2016, the DOJ and FTC jointly issued their "Antitrust Guidance for Human Resource Professionals." The Guidance explains how antitrust law applies to employee hiring and compensation practices. The agencies also issued a "quick reference card" that lists a number of "antitrust red flags for employment practices."

In a nutshell, agreements (whether formal or informal) among employers to limit or fix the compensation paid to employees or to refrain from soliciting or hiring each other's employees are per se violations of the antitrust laws. Also, even if competitors don't explicitly agree to limit or suppress compensation, the mere exchange of compensation information among employers may violate the antitrust laws if it has the effect of suppressing compensation.

The seriousness of this issue is underscored by the agencies' statements in their press releases that the guidance is aimed at putting companies on notice that DOJ will proceed criminally against wage fixing and no-poaching agreements. There also has been a significant uptick in recent years in class action litigation and enforcement activity challenging antitrust violations in the employment context. In one exchange of wage information case in Detroit, a group of hospitals paid a total of $90 million to settle the case, and in one consolidated case involving allegations of agreements among employers not to poach each other's employees, the defendants settled for a total of $435 million.

The evidence in many of these cases demonstrates that many HR professionals and other managers and executives do not realize that the antitrust laws apply in the employment marketplace just as they do in the commercial marketplace. It is important that those HR professionals and other managers and executives who are involved in recruiting, hiring or the compensation process have a clear understanding of antitrust requirements as applied to those practices.

For more information on this topic, please contact the authors, your Seyfarth Attorney or a member of the Firm's Antitrust/Trade Regulation Team or the Workplace Policies and Handbooks Team.

The White House's Call to Action: A Step in the Right Direction or a Bridge Too Far?

By Katherine Perrelli, Erik Weibust, and Dallin Wilson (October 28th, 2016)

Fresh off of signing the Defend Trade Secrets Act, the White House released a report yesterday entitled "Non-Compete Reform: A Policymaker's Guide to State Policies," which contains information on state policies related to the enforcement of non-compete agreements. Additionally, the White House issued a "Call to Action" that encourages state legislators to adopt policies to reduce the misuse of non-compete agreements and recommends certain reforms to state law books.

The "Non-Compete Reform: A Policymaker's Guide to State Policies," which relied heavily on Seyfarth Shaw's "50 State Desktop Reference: What Employers Need to Know About Non-Compete and Trade Secrets Law," suggests that non-compete clauses have recently become more widespread, impacting 18% of all workers and 15% of employees without a college degree. The report analyzes the various states that have enacted statutes governing the enforcement of non-compete agreements and the ways in which those statutes address aspects of non-compete enforceability, including durational limitations; occupation-specific exemptions; wage thresholds; "garden leave;" enforcement doctrines; and prior notice requirements.

With those issues in mind, the Call to Action encourages state policymakers to pursue three "best-practice policy objectives:"

1. **Ban non-competes for categories of workers**, including workers under a certain wage threshold; workers in occupations that promote public health and safety; workers who are unlikely to possess trade secrets; or workers who may suffer adverse impacts from non-competes, such as workers terminated without cause.
2. **Improve transparency and fairness of non-competes** by, for example, disallowing non-competes unless they are proposed before a job offer or significant promotion has been accepted; providing consideration over and above continued employment; or encouraging employers to better inform workers about the law in their state and the existence on non-competes in contracts and how they work.
3. **Incentivize employers to write enforceable contracts**, and encourage the elimination of unenforceable provisions by, for example, promotion of the use of the "red pencil doctrine," which renders contracts with unenforceable provisions void in their entirety.

While some large employers have already publicly embraced the Call to Action, even reform-minded employers are likely to be wary of some of these proposals. For example, broad prohibitions against non-competes for workers under a certain wage threshold could threaten the many small start-ups where employee salaries tend to be lower than established businesses, but where those employees have access to highly confidential information and trade secrets. Start-ups need room to innovate at

lower cost, but they still need to protect their R&D and IP from competitors, and non-competes can be an effective tool in accomplishing that goal.

Moreover, a ban on non-competes for all workers that are laid off loses sight of the purpose of the non-compete: to prevent employees with valuable competitive information from joining a competitor and using that information to compete against their former employers. Instead of using a broad brush to exempt all laid off employees from non-competes, many employers would prefer to see legislative reform focused instead on whether the employee has information worthy of protection and the appropriate duration of the non-compete to protect against disclosure of the information.

Lastly, while incentivizing narrowly tailored (and thus, enforceable) non-competes should be a goal of all employers, promoting the use of the "red pencil doctrine" may be a bridge too far. Many employers embed non-compete provisions in broader agreements that contain otherwise enforceable non-disclosure or non-solicitation agreements. Striking the entire agreement in these instances would unnecessarily harm business interests and the innovation economy. Instead, many employers would rather see state legislators leave these issues up to the courts by allowing judges to use gentler options such as the "blue pencil doctrine," which allows the court to strike only the overbroad provisions while keeping the rest of the agreement intact. Another option is the reformation doctrine, which empowers judges to narrow overbroad restrictions while maintain the agreement's enforceability.

It remains to be seen whether state legislatures will answer the White House's call for action on non-compete reform. In the meantime, we will keep our readers up-to-date on any developments.

Texas Court of Appeals Finds Noncompete Agreement Inapplicable to Former President's Post-Termination Activities Due to the Inexact Language of the Noncompete Period

By Andrew P. del Junco and Jesse M. Coleman (December 1st, 2016)

On October 27, 2016, the Fort Worth Court of Appeals affirmed a lower court's order denying an application for temporary injunction seeking to enjoin Thomas Musgrave, the former president of Henry F. Coffeen III Management, Inc., d/b/a Coffeen Management Company ("CMC"), from competing with and soliciting its business. By doing so, the court emphasized the importance of carefully drafting noncompete and nonsolicitation provisions in employment agreements to ensure that an employee's post-termination activities remain subject to the restrictive covenants.

CMC is an insurance agency that sells insurance products to car dealerships. Musgrave began working for CMC in 2011 as an independent contractor and, as its president, was responsible for managing CMC's day-to-day operations. Musgrave signed a "Non-Compete Agreement" barring him from competing with CMC or soliciting its customers for a specified term. In August 2015, Musgrave began travelling to New Mexico to visit Tate Branch Automotive ("TBA"), a CMC client that owns several car dealerships. A short time later, Musgrave started assisting TBA with acquiring car dealerships. In December 2015, Musgrave resigned from CMC, but he continued to advise TBA on the acquisition of car dealerships.

On the heels of Musgrave's resignation, CMC filed a lawsuit against him in Texas state court for, among other things, breach of contract based on the noncompete and nonsolicitation provisions he signed, and sought a temporary restraining order and temporary and permanent injunctions. The trial court granted CMC ***a temporary restraining order***, blocking Musgrave from soliciting or marketing any products or services that comprise part of CMC's business to specified clients of CMC, including TBA. Shortly thereafter, the trial court, following a hearing, denied CMC's application for ***a temporary injunction***, finding, *inter alia*, that the Non-Compete Agreement was unsupported by consideration and lacked geographical boundaries.

On interlocutory appeal, CMC maintained that the term of the restrictive covenants applied for two years from the date of Musgrave's resignation in December 2015; therefore, it established a likelihood of success on the merits of its breach-of-contract claim. The court of appeals began its analysis by reciting the text of the Non-Compete Agreement, which provided that Musgrave would remain subject to the restrictive covenants "[d]uring the Term of this Agreement and for a period of two (2) years after the 'CMC Account Development Sub Agent Agreement' is terminated." Despite being capitalized, the word "Term" from the Non-Compete Agreement was undefined. The court reasoned that because the covenants specify the restrictions expire two years after the termination of the "CMC Account Development Sub Agent Agreement," and it was undisputed that Musgrave, as an independent

contractor and president of CMC, was not a subagent or sales representative, the noncompete period was inapplicable, so the provisions at issue never restricted Musgrave's post-termination conduct. Accordingly, CMC did not show a probable right to recovery on its contract claim, and thus, the trial court did not abuse its discretion in denying CMC's application for temporary injunction.

The court reached this result even though the findings of fact supporting the trial court's order did not rest on the ground that the noncompete period was inapplicable. According to the court, it was unconstrained by the lower court's findings because "[t]he trial court's stated reasons for denying CMC's application for temporary injunction do not meet the requirements of civil procedure rule 299a [which requires that findings of fact be separately filed from the judgment or order] and do not control the outcome of this case." Thus, the court effectively reviewed the trial court's order based on the legal fiction that no findings of fact were made, such that it was free to uphold the trial court's decision on any legal theory supported by the record—even one not embraced by the lower court's findings.

This opinion underscores the importance of the requirement that findings be filed separate and apart from the judgment or order they support. Otherwise, as CMC learned, litigants will face an uphill battle obtaining reversal on appeal. Ist-termination activities, and to properly define their terms.

Henry F. Coffeen III Mgmt., Inc. v. Musgrave, 02-16-00070-CV, 2016 WL 6277375 (Tex. App.—Fort Worth Oct. 27, 2016, no. pet. h.)

Texas Appellate Court Holds Condition Subsequent in Noncompete Agreement Excused Former Employee's Competitive Activities

By Jesse M. Coleman and Andrew P. del Junco (December 27th, 2016)

A Texas Court of Appeals affirmed a summary judgment last month in favor of an ex-employee declaring that a noncompete clause in an asset purchase agreement and separate noncompete agreement did not bar him from competing with his former employer after he had resigned his position. The court's opinion serves as a reminder that conditions subsequent in noncompete clauses must be drafted with special care in order to avoid the risk that former employees may ignore such clauses with impunity.

Jason Player, a former IT manager for East Texas Copy Systems, Inc. ("Copy Systems") sold his business to Copy Systems and, in the process, signed an asset purchase agreement ("APA"), as well as a separate noncompete agreement ("NCA"), that contained clauses precluding him from competing with Copy Systems for a certain period of time. Both the APA and the NCA also included nearly identical provisions which provided that "[i]f . . . Player's employment with [Copy Systems] is terminated prior to two years from the date of this Agreement [July 1, 2013] for any reason other than a for cause termination, this non-compete Agreement will no longer be binding." Player resigned his position with Copy Systems effective June 30, 2015—one day shy of the two-year period—and immediately began engaging in IT-related business for a competitor. Copy Systems then sent a cease-and-desist letter to Player demanding that, pursuant to its interpretation of the noncompete clauses, he refrain from engaging in any activities that are competitive with Copy Systems.

Player then filed suit in Texas state court against Copy Systems, requesting a declaration that the NCA and noncompete clause in the APA no longer forbid him from competing with Copy Systems. Copy Systems, in turn, filed a counterclaim seeking (1) a declaration that the noncompete provisions at issue remained effective, and (2) damages for breach of contract. As the facts were undisputed, both parties filed motions for summary judgment. After a hearing, the trial court granted Player's motion and denied Copy Systems'.

On appeal, Copy Systems challenged the trial court's construction of the parties' noncompete agreement as reflected in the NCA and APA. Both parties focused on the interpretation of "*[i]f . . . Player's employment with [Copy Systems] is terminated* prior to two years from the date of this Agreement for any reason other than a for cause termination, *this non-compete Agreement will no longer be binding*." Copy Systems argued that this clause should be interpreted so that the noncompete would remain effective post-termination in the event Player resigned. This is, the noncompete would cease to apply only if the Player was fired without cause. Player, on the other hand, maintained that the clause was effective if either party terminated his employment, including if he resigned.

Siding with Player, the court of appeals construed this clause, like the trial court had before it, to be a condition subsequent clause, i.e., a clause where the fulfillment of a condition excuses performance of an otherwise binding agreement. The court reasoned that, adhering to the plain and ordinary meaning of the agreements' terms, the clause at issue was effective if *either party* terminated Player's employment, since that clause did not identify which party must terminate the employment relationship. According to the court of appeals, what triggers the condition subsequent clause is "the termination of Player's employment, not which party initiates the termination." Copy Systems' argument to the contrary was, in effect, asking the court to rewrite the agreement to insert the following underlined language: "[i]f . . . Player's employment with [Copy Systems] is terminated [***by Copy Systems***] prior to two years from the date of this Agreement for any reason other than a for cause termination, this non-compete Agreement will no longer be binding." This the court refused to do. Because Player resigned on June 30, 2015, and nothing in the parties' agreement indicated that the inclusion of this clause was intended to restrict the party initiating the triggering termination to only Copy Systems, the court held that Player was excused from the performance of any obligations prescribed by the APA and NCA.

The takeaway from this case appears to be that employers should be cautious when inserting conditions subsequent in noncompete agreements, especially if the language triggering the condition subsequent does not specify which party terminates the employment relationship. If employers intend for noncompetes to continue to bind an employee post-resignation, they must specifically include language in any condition subsequent clause that the termination was at the instance of the employer. If no such language is included, the courts may decline to reform imprecise agreements and redistribute the contractually allocated risks and benefits. Accordingly, employers may wish to protect themselves by ensuring that an employee's voluntary resignation is not a triggering event, thereby guaranteeing that the noncompete does not become ineffective upon the employee's resignation.

E. Texas Copy Sys., Inc. v. Player, 06-16-00035-CV, 2016 WL 6638865 (Tex. App.—Texarkana Nov. 10, 2016, no. pet. h.).

Legislation

Massachusetts Legislature Takes Up Noncompete Reform . . . Again

By Erik Weibust (March 3rd, 2016)

Another year, another attempt at noncompete reform in Massachusetts. According to the *Boston Globe*, Massachusetts House Speaker Robert DeLeo announced that lawmakers would unveil a bill limiting the use of noncompete agreements in the Commonwealth. As we have previously reported, legislators have been attempting to enact noncompete reforms in Massachusetts for years (since at least 2008), to no avail, including a last minute push by outgoing Governor Deval Patrick at the end of his term in 2014. Thus far, nothing has been accomplished, but the forthcoming bill appears to propose less dramatic restrictions than in the past, so perhaps 2016 is finally the year.

Specifically, Speaker DeLeo's bill is expected to contain the following restrictions:

- Noncompete agreements would be limited to 12 months in duration;
- Employers would be required to notify incoming employees about noncompetes before they accept a job offer; and
- Noncompetes would be prohibited for low-wage workers like restaurant and retail workers.

More specifics will no doubt be forthcoming, such as whether the restrictions will be retroactive, whether tolling provisions will be permitted beyond the 12 month restriction, the definition of low wage workers, and what, if any, effects this will have on other post-employment restrictive covenants such as nonsolicitation agreements. We will keep you informed as the bill progresses through the Massachusetts Legislature, and we encourage you to check out our friend Russell Beck's blog as well for further insights and updates.

Umpteenth Time's the Charm? Massachusetts Has Another Go At Non-Compete Reform

By Katherine Perrelli, Erik Weibust, and Dawn Mertineit (May 20th, 2016)

The Massachusetts legislature is back at it again — as the Boston Globe reports, the Joint Committee on Labor & Workforce Development has sponsored a compromise bill with the goal of limiting non-competes in the Commonwealth.

As our readers may recall, for nearly a decade, Massachusetts legislators have attempted to pass legislation regarding non-competes, to no avail. In fact, in recent years, there have been unsuccessful attempts to join California in banning non-compete agreements outright (including a failed proposal by former Governor Deval Patrick himself).

Now, with still over 2 months to go before the formal legislative session ends, legislators are once more taking a crack at it, although unlike the attempts to ban non-competes 2 years ago, the current bill may not be nearly as concerning to proponents of non-competes.

That said, the proposed legislation is not controversy-free. In fact, the inclusion of a provision requiring "garden leave," which would force employers to pay former employees bound by non-compete agreements 50% of their highest annualized salary over the last 2 years of employment for the restricted period, has prompted many in the business community to express their concern. Some, such as executive vice president of the Associated Industries of Massachusetts, Chris Geehern, have noted that employees who are bound by non-competes are often highly-paid employees to begin with, who may receive the benefit of inflated compensation in their base salary to reflect the fact that they are so bound. Likewise, the Greater Boston Chamber of Commerce's president and CEO, Jim Rooney, told the Boston Globe that the inclusion of the garden leave provision was "unexpected," and likely "would be a problem for [the Chamber]." Notably, we are unaware of any other jurisdiction in the United States that requires — statutorily or otherwise — "garden leave" payments as a prerequisite for the enforcement of non-competes.

Other provisions of the proposed legislation may cause some consternation for businesses, or at the very least, may require those businesses to change their practices. For example:

- The proposed legislation prohibits judicial reform of non-competes in contrast to current Massachusetts common law. This provision could have disastrous results for employers who have a good-faith belief that their agreement is reasonable and enforceable, but whose agreements are nonetheless found to be over-reaching by a reviewing court. Without the ability to reform the agreement, the proposed legislation could be read to require the court to strike the entire agreement. The proposed legislation does not indicate whether it merely prohibits reformation in the sense that a court could not replace a nationwide restriction with a 10 miles restriction, for example, or if a court could not even "blue pencil" the agreement to strike only offending portions of the non-compete and leave the remainder.

- As is the case in certain other states, the bill would do away with "continued employment" as sufficient consideration for the non-compete agreement. This could be potentially costly for employers seeking to enter into non-compete agreements with existing employees as they will need to provide some other form of consideration.

- With certain exceptions (addressed below), the proposed legislation limits the length of non-competes to 1 year. While this is certainly an improvement from a prior bill that would have rendered agreements lasting longer than 6 months "presumptively unreasonable," some Massachusetts employers may find a one-year period insufficient to protect their legitimate business interests, particularly given that courts in the Commonwealth have historically found that longer restrictions are warranted in some cases.

- Notwithstanding the one-year limit noted above, the bill allows a longer restricted period if "the employee has breached his or her fiduciary duty to the employer or the employee has unlawfully taken, physically or electronically, property belonging to the employer, in which case the duration may not exceed 2 years from the date of cessation of employment." It is unclear whether this provision merely suggests that the restricted period will be tolled in the event the employee has acted improperly.

- The bill prohibits non-competes for employees "classified" as non-exempt under the Fair Labor Standards Act ("FLSA") (although the bill does not clarify by whom the employee would be classified — the employer, or the Department of Labor?), student interns or grad/undergrad students engaged in short-term employment while enrolled in school, employees who have been terminated without cause or laid off, or employees aged 18 or under. While most of these categories will likely be accepted by the business community as common-sense, some may find the prohibition on non-competes for any and all non-exempt employees to be overly simplistic. Some businesses will likely seek for the legislature to carve out non-exempt employees who have unique access to the employee's confidential and/or trade secrets in order to perform the functions of their jobs.

Additionally, as we have observed in many posts on our Wage and Hour Litigation Blog, the FLSA's overtime exemptions are not always a model of clarity and can be a moving target. Accordingly, if an employee is exempt (and otherwise can legally be bound by a non-compete agreement under the proposed legislation) at the time of execution, but later becomes non-exempt due to changing FLSA regulations or caselaw, it is unclear whether a court would enforce a non-compete against the employee. Given that the bill provides that a "noncompetition agreement shall not be enforceable against . . . an employee who *is* classified as nonexempt" (emphasis added), as opposed to "*was* classified as nonexempt at the time of execution," it appears likely that changes in the FLSA regulations could instantaneously prohibit an employer from enforcing certain non-compete agreements that were enforceable the day prior, without *any* change in an employee's roles or responsibilities.

- The proposed legislation also prohibits choice-of-law provisions that would avoid the effects of the bill where the employee, for the 30 days preceding the cessation of employment, is a Massachusetts resident or was employed in the Commonwealth. This provision could prove difficult for multi-state employers, who will need separate agreements for Massachusetts employees (and would need to rigorously and regularly review where its employees reside or work, in case an employee relocates). It also means an employee could move to Massachusetts specifically to avoid enforcement of his or her non-compete.

- The bill also purports to grant exclusive jurisdiction for any disputes relating to non-compete agreements in the Massachusetts superior courts or the Business Litigation Session of the Suffolk County superior court. This suggests that parties may be prohibited from bringing claims related to non-compete agreements in federal court (which may be unconstitutional), potentially leading to claim-splitting (such as where an employer wishes to also assert a Defend Trade Secrets Act claim or other claims in federal court), and may unnecessarily tax the already burdened superior courts of the Commonwealth.

- The bill also defines "employee" to include independent contractors, notwithstanding the many fundamental differences between employees and independent contractors under Massachusetts law. It's unclear why the committee chose to define "employee" in this way, given that its definition as drafted seems to have no rational tie to "employee" as that term is used in other laws.

Not all provisions of the bill will be concerning to employers. For example, the legislation will not be retroactive — a major improvement over previous attempts to limit non-competes. Nor would the bill affect non-solicit provisions, non-disclosure agreements, non-competes made in connection with the sale of a business (or otherwise made outside of employment relationships), forfeiture agreements, or agreements not to reapply for employment. Other uncontroversial provisions include requirements that the agreement be signed, in writing, state that the employee has the right to consult with counsel, and must be provided to the employee by the earlier of a formal offer of employment or 10 business days before the commencement of the employee's employment (which are already considered best practices for enforcement of non-competes in Massachusetts). Finally, the bill also would adopt the Uniform Trade Secret Act, which would leave New York as the lone hold-out.

At this point, the bill may move straight to a vote, or may be further discussed in the Ways & Means committee. In any event, given the apparent appetite in the Commonwealth both in the legislature and in the business community to come to some form of compromise, it appears that there is a fair chance we will see some non-compete legislation passed this year, or early in the next session.

Update: Massachusetts House of Representatives Edits and Unanimously Approves Non-Compete Bill in an Attempt to Make Progress Before End of Legislative Session

By Dawn Mertineit, Katherine Perrelli, and Erik Weibust (June 30th, 2016)

As we previously reported, Massachusetts is making yet another go at non-compete reform, as the Joint Committee on Labor & Workforce Development introduced a compromise bill at the end of May that has many in the Commonwealth talking. As we noted, there were several provisions that gave some commentators pause, including most notably a garden leave provision that would require employers to pay former employees bound by non-compete agreements 50% of their highest annualized salary over the last 2 years of employment for the restricted period.

House leaders have recently made edits to the bill that might provide some comfort to employers who rely on non-compete agreements and were wary of the bill's provisions. First, the revised bill would allow an employer to agree to "other mutually-agreed upon consideration" as an alternative to garden leave, provided such consideration is specified in the agreement. This change has already made some in the business community more comfortable with the bill; for example, the Greater Boston Chamber of Commerce's CEO, Jim Rooney, acknowledged that "it's better than what we were working with."

The revised bill would also maintain the status quo by allowing judges in the Commonwealth to reform non-competes that they deem overbroad (for example, by replacing a 100-mile geographic scope with a 50-mile one), which is a significant departure from the bill's original text, which would have forced judges to invalidate such agreements even if they were largely enforceable, but only slightly overreaching. The original "red pencil" text, like the garden leave provision, was quite concerning to many in the business community, so this change will likely comfort many employers.

Additionally, an amendment revised the jurisdictional provision of the bill, and now provides that all civil actions relating to employee non-compete agreements be brought in either the county where the employee resides, or Suffolk county (where such actions would be brought in the Business Litigation Session) — although this still leaves some confusion as to whether a claim relating to a non-compete agreement could be brought in federal court. If not, the bill might lead to claim-splitting where an employer seeks to assert a Defend Trade Secrets Act claim. Finally, the revised bill would only apply to agreements entered into on or after October 1, 2016, allowing employers with additional time to revamp their agreements.

Yesterday, the House voted unanimously to approve the revised bill, sending it to the Senate, which will consider the legislation after July 4th. That said, despite the improvements noted above, there are still many provisions in the bill that might give employers heartburn; as we mentioned in our last post,

among other things, the bill eliminates “continued employment” as sufficient consideration for such agreements, and prohibits non-competes across-the-board for certain categories of employees, including most notably those classified as non-exempt under the Fair Labor Standards Act.

It remains to be seen whether legislators will continue to revise the bill to address these (and other) concerns. However, given that the Senate voted unanimously to ban non-competes outright fairly recently, we anticipate that the bill will meet with considerable success in the Senate.

Finally, even assuming the bill passes, it’s still unclear whether Governor Baker will sign or veto it, given that his administration has not strongly signaled one way or the other how he views the pending legislation. That said, in the face of the unanimous vote in the House (and potential for a unanimous vote in the Senate), Governor Baker may be hard-pressed to justify a veto.

Massachusetts Governor Supports Noncompete Reform, But Not Abolition

By Dawn Mertineit, Katherine Perrelli, and Erik Weibust (July 26th, 2016)

According to *The Boston Globe*, Massachusetts Governor Charlie Baker has publicly voiced his support for some restrictions on noncompete agreements, but he does not want to abolish them entirely. Specifically, Governor Baker supports the bill passed by the Massachusetts House of Representatives (discussed previously here), but not the far more restrictive bill passed by the Massachusetts Senate (discussed here). According to Governor Baker's spokesman:

The Governor favors the House version of the noncompete legislation because he believes it better balances workers' abilities to seek new employment while ensuring cutting edge businesses can protect essential intellectual property. . . . Finding the right compromise on this issue is essential to ensuring innovative businesses want to stay and grow in the Commonwealth.

A conference committee, being led by House Ways and Means Chairman Brian Dempsey and Senator Daniel Wolf, with Representatives John Scibak and Jay Barrows and Senators William Brownsberger and Ryan Fattman, will attempt to resolve the differences between the competing bills by the end of the formal legislative session, which wraps up for the year on July 31.

In Like A Lion, Out Like A Lamb: Following Much Fanfare, Massachusetts Noncompete Reform Again Fails

By Erik Weibust, Dawn Mertineit, and Katherine Perrelli (August 1st, 2016)

In what has become a highly anticipated annual game of "Will They/Won't They," the Massachusetts legislature again failed to pass comprehensive noncompete reform legislation this year, despite much fanfare and high hopes from certain quarters. This should come as no surprise to our loyal readers, who have seen this happen virtually every year over the past decade, but it actually seemed as though something might be different this year, with the House and Senate both passing bills, and the Governor signaling his support for the House version. Alas, the wheels of state government have again come to a screeching halt with no movement as the 2016 legislative session ended late last night with no compromise. No controversial matters can now be advanced until the next legislative session, which begins in January 2017. As we seem to say every summer, maybe next year . . .

Two New England States Pass Legislation Restricting Physician Non-Competes

By Erik Weibust and Andrew Stark (August 22nd, 2016)

We've written a lot this summer about the Massachusetts legislature's latest failed attempt at non-compete reform. Two other states in New England, however, are able to claim accomplishments in that regard. Specifically, Connecticut and Rhode Island each enacted statutes this summer imposing significant restrictions on the use of non-compete provisions in any agreement that establishes employment or any other form of professional relationship with physicians. While Connecticut's simply law limits the duration and geographic scope of physician non-competes, Rhode Island completely banned such provisions in almost all agreements entered into with physicians.

Connecticut

Effective July 1, 2016, any covenants not-to-compete entered into, amended, or renewed in Connecticut can no longer restrict a physician's competitive activities (i) for longer than one year and (ii) in a geographic region beyond 15 miles from the "primary site" where the physician practices. Primary site refers to "the office, facility or location where a majority of the revenue derived from such physician's services is generated" or "any other office, facility or location where such physician practices and mutually agreed to by the parties and identified in the covenant not to compete." The law also renders such provisions enforceable only if (i) the provision is made in anticipation of a partnership or ownership agreement or (ii) the employment or contractual relationship is terminated by the employer for cause.

Rhode Island

Effective July 12, 2016, it is now unlawful in Rhode Island to restrict in any way "the right to practice medicine in any geographic area for any period of time after the termination" of any partnership, employment, or professional relationship with a physician. The law also prohibits any restrictions on the right of physicians "to solicit or seek to establish a physician/patient relationship with any current patient of the employer." It does not, however, apply in connection with the purchase and sale of a physician practice, provided the restrictive covenant is less than five years in duration.

Takeaway

Entities that employ physicians in Connecticut and Rhode Island should take note of these recent changes to the law and thoroughly review their existing physician non-compete and non-solicitation agreements. These agreements may need significant modifications to be in compliance with the new standards discussed above.

New California Law May Preclude Use of Forum-Selection Clauses to Enforce Non-Compete Agreements in Employment Contracts

By James D. McNairy and Michael Cross (October 10th, 2016)

On September 25, California Governor Jerry Brown signed into law Senate Bill 1241. SB 1241, effective **January 1, 2017**, adds Section 925 to the Labor Code to restrain the ability of employers to require employees to litigate or arbitrate employment disputes (1) outside of California or (2) under the laws of another state. The only exception is where the employee was individually represented by a lawyer in negotiating an employment contract.

For companies with headquarters outside of California and employees who work and reside in California, this assault on the freedom of contract is not welcome news. Particularly affected are companies that include forum-selection clauses in contracts with California employees that include non-competition or customer non-solicit provisions. Once SB 1241 becomes effective, it may foreclose—in all but the most unusual circumstances—the sometimes successful strategy of enforcing a non-competition agreement against a California resident through litigation in another state.

The Genesis of SB 1241—The Recent Rise of Forum Selection and Choice-of-Law Clauses

Companies have long used forum-selection clauses and choice-of-law provisions in an effort to avoid California courts applying California law to employment disputes, especially those concerning attempts to enforce non-competition provisions. There often are legitimate reasons to have employment disputes decided where the company primarily does its business. Companies often prefer a court in their own state to decide which law (California's or some other state's) will govern a dispute. SB 1241 generally invalidates these provisions.

Courts have long held that the freedom to contract favors the enforcement of forum-selection clauses. The U.S. Supreme Court in 2013 reinforced this rule in *Atlantic Marine Constr. Co*. Although not an employment case, *Atlantic Marine* broadly endorsed forum-selection clauses, stating that "courts should not unnecessarily disrupt the parties' settled expectations" and that usually " 'the interest of justice' is served by holding parties to their bargain." Since that time, federal district courts in California have increasingly given more weight to forum-selection clause, including those in employment contracts, leaving the decision on which law to apply to the dispute—that of California or the foreign state—to a court outside of California.

What SB 1241 Provides

SB 1241 was among a bevy of employment-related bills that were sent to Governor Brown at the end of August 2016. SB 1241, the full text of which appears here, will be enacted as Labor Code section 925. It applies to employment contracts entered into, modified, or extended **on or after January 1, 2017.**

The key provision of Section 925 is its first section:

(a) An employer shall not require an employee who primarily resides and works in California, as a condition of employment, to agree to a provision that would do either of the following:

(1) Require the employee to adjudicate outside of California a claim arising in California.

(2) Deprive the employee of the substantive protection of California law with respect to a controversy arising in California.

A key exception to the application of Section 925 appears in subdivision (e):

(e) This section shall not apply to a contract with an employee who is in fact individually represented by legal counsel in negotiating the terms of an agreement to designate either the venue or forum in which a controversy arising from the employment contract may be adjudicated or the choice of law to be applied.

Thus, Section 925 generally forbids employers to require California employees to adjudicate claims outside of California or to submit to the laws of another state. An employee who successfully sues to void such offending provisions can recover reasonable attorney's fees. (Lab. Code § 925(e).)

A Shift in Codified Public Policy that Will Likely Impact How Federal Courts in California Analyze Forum Selection Clauses in Employment Agreements

Under California state law, a party seeking to enforce a forum-selection clause in an employment agreement already faced an uphill battle: it had to "prove that enforcement of the forum-selection clause would not result in a significant diminution of rights." What is more, even though the party seeking to avoid a forum-selection clause generally bears the burden of showing it is unreasonable or unfair, that burden is reversed when, like in the employment context, the claims at issue are based on unwaivable rights. It is therefore unsurprising that California Courts of Appeal regularly refuse to enforce an employer's forum-selection clause and related choice-of-law provision when they violate California public policy. For cases brought in California state court, then, some might say that Section 925 changes the employer's battle from difficult to hopeless: clauses that once were simply presumptively unenforceable may now be categorically unenforceable, except for clauses negotiated with an employee "individually represented by legal counsel."

But Section 925 will almost certainly change the analysis of forum-selection enforceability in federal courts, too. Federal Courts apply federal law when determining the enforceability of forum-selection clauses. And the Supreme Court has held that forum-selection clauses are "prima facie valid and should be enforced unless enforcement is shown by the resisting party to be 'unreasonable' under the circumstances." Federal courts' generally find forum-selections clauses unreasonable only if they are (1) the product of fraud or overreaching, (2) would serve to deprive a party of its day in court, or (3) contravene public policy.

Employees whose employment agreements contained non-competition clauses have tried to avoid enforcement of their forum-selection clauses by arguing that their enforcement would contravene Business and Professions Code section 16600. However, some federal courts have rejected such attempts to conflate forum-selection clauses with choice-of-law provisions, stating that the problem with such an argument "is that it does not challenge the reasonableness of the forum-selection clause itself, only the reasonableness of its effect."

Section 925 may make such a distinction less tenable. It serves to make the reasonableness of a forum-selection clause itself a contravention of public policy. To this extent, it brings employment agreements into line with franchise agreements. As the Ninth Circuit has held when evaluating forum-selection clauses in franchise agreements, Business and Professions Code section 20040.5 establishes a public policy "to protect California franchisees from the expense, inconvenience, and possible prejudice of litigating in a non-California venue." Because that provision itself, rather than its effect, contravenes California public policy, the Court affirmed the district court's order denying the motion to transfer venue from California to Pennsylvania.

Labor Code section 925 may serve the same function in federal courts' analyses of forum-selection provisions in employment agreements as Business and Professions Code section 20040.5 serves now in the context of franchise agreements.

It remains to be seen how Labor Code section 925 and Business and Professions Code section 16600 may operate where an California employee individually represented by legal counsel in negotiating the terms of her employment contract agrees to forum selection and choice-of-law provisions that are later used to enforce a non-compete against such an employee.

Employer Takeaways

- Employers with California employees should continue to use caution when using forum-selection clauses to provide the potential option of enforcing non-compete agreements. After January 1, 2017, attempting to enforce such provisions may not only result in litigation, but now may also result in the employer being on the hook for the employee's attorneys' fees.
- Use of forum-selection provisions may also increase litigation over questions such as what "primarily resides and works" in Section 925 actually means and whether attempts to enforce non-competition provisions in this context may be argued to be unfair competition in violation of Business and Professions Code section 17200.

- Although the law takes effect January 1, 2017, it only applies prospectively to employment contracts "entered into, modified, or extended on or after January 1, 2017." The law will not apply retroactively (which would violate the Contract Clause) to employment contracts effective before the new year.

A Holiday Miracle? Massachusetts Legislature Discussing Late-Session Non-Compete Deal

By Erik Weibust (November 22nd, 2016)

Apparently there may be some life left yet in the Massachusetts Legislature's attempt to pass non-compete reform this year. As we previously reported, the House and the Senate were unable to bridge their differences and agree on a compromise bill before the formal session wrapped up on July 31.

According to the Boston Business Journal, however, "House and Senate leaders involved in the negotiations that came up just short at the close of formal sessions in July have continued talking, with a White House summit on non-competes serving as a spark plug to rekindle some hope that a compromise could still be brokered." Among other differences, the Senate bill would have limited non-compete agreements to three months, whereas the House version had a one year limit. Both versions also provided for garden leave clauses, wherein an employee is paid during the restricted period, but the House set the compensation during the garden leave at 50% and the Senate recommended 100%. The major disagreement, however, was over language that would have allowed both the employer and the employee to substitute garden leave pay for a different, mutually agreed upon, arrangement negotiated at the commencement of employment. Even if a compromise deal is reached by the House and the Senate before the end of the year, it may be difficult to get passed in the full Legislature, as a single lawmaker can defeat any bill during an informal session by simply objecting to it.

The Associated Industries of Massachusetts and the Massachusetts High Technology Counsel have both said that they are in favor of something more akin to the House bill.

We will continue to monitor these developments and report back with any updates. It may be that 2016 is the finally year for non-compete reform in Massachusetts after all . . . But we have said that before.

International

EU Publishes Text of Compromise Trade Secrets Directive for Approval by European Parliament

By Daniel P. Hart (January 26th, 2016)

As we reported last month in this blog, in December the European Council and representatives of the European Parliament reached a "provisional agreement" on the European Commission's proposed Directive to protect trade secrets. With this provisional agreement, the Council and representatives of the European Parliament agreed on compromise language to be submitted to the Parliament for approval, thus clearing the way for adoption of the proposed directive in the next few months.

At the time that we reported on this development, the compromise text was not yet available. However, now that the Parliament and Council have completed a legal-linguistic review of the text, the full English-language version of the compromise text is now available. With the benefit of the full text, we can now answer one final open question that we reported last month — i.e., what is the scope of the protections that will be available to trade secrets during litigation under the compromise text?

As we previously noted, the European Commission's original text contemplated that courts in Member States may issue "Attorneys' Eyes Only" protective orders like those that are typically used in trade secrets cases in the U.S. Specifically, the Commission's original text provided that:

Member States shall also ensure that the competent judicial authorities may, on a duly reasoned application by a party, take specific measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of the legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret. The measures referred to . . . shall at least include the possibility: (a) to restrict access to any document containing trade secrets submitted by the parties or third parties, in whole or in part; (b) to restrict access to hearings, when trade secrets may be disclosed, and their corresponding records or transcript. In exceptional circumstances, and subject to appropriate justification, the competent judicial authorities may restrict the parties' access to those hearings and order them to be carried out only in the presence of the legal representatives of the parties and authorised experts . . .

In contrast, in its draft Legislative Resolution, the European Parliament's Legal Affairs Committee watered down this language with the following proposed language that would appear to eliminate true "Attorneys' Eyes Only" protective orders:

The measures referred to . . . shall at least include the possibility: (a) to restrict access to any document containing trade secrets or alleged trade secrets submitted by the parties or third parties to a limited number of persons, in whole or in part ***provided that at least one person from each of the parties***, and, where appropriate in view of the proceedings, their respective lawyers and/or legal representatives, are given access to the document in full; (b) to restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed, and their corresponding records or transcript to a

limited number of persons, ***provided that it includes at least one person from each of the parties***, and, where appropriate in view of the proceedings, their lawyers and/or legal representatives . . .

Based on the compromise text, the Council and representatives of the Parliament appear to have adopted the Legal Affair's Committee's approach, albeit with different language. The relevant portion of the compromise text now reads as follows:

Member States shall also ensure that the competent judicial authorities may, on a duly reasoned application by a party, take specific measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of the legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret. Member States may also allow competent judicial authorities to take such measures on their own initiative.

The measures referred to in the first subparagraph shall at least include the possibility:

(a) to restrict access to any document containing trade secrets or alleged trade secrets submitted by the parties or third parties, in whole or in part, to a limited number of persons;

(b) to restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed, and their corresponding records or transcript to a limited number of persons;

(c) to make available to any person other than those comprised in the limited number of persons referred to in points (a) and (b) a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed or redacted.

The number of persons referred to in points (a) and (b) of the second subparagraph shall be no greater than what is necessary in order to ensure compliance with the right to an effective remedy and to a fair trial of the parties to the proceedings and shall include, ***at least, one natural person from each party*** and the respective lawyers or other representatives of those parties to the proceedings.

Proposed Directive, Article 8, ¶ 2.

Assuming that this compromise text is approved by the European Parliament, legislatures and courts in Member States will no doubt take different approaches to effectuate this language. Although the final compromise text is somewhat weaker than the protections that U.S. practitioners typically see in trade secrets litigation, on balance the compromise language provides a reasonable baseline for protection of trade secrets during litigation that is probably more than sufficient for most disputes.

The compromise text is expected to be submitted to the full European Parliament for approval in the next few months. If the Parliament approves the text on a first reading, the European Council will approve the European Parliament's position and the Directive will be adopted. Member States then will be required to enact national law consistent with the Directive within two years. We will continue to track progress of the proposed Directive as it crosses the final hurdle necessary for adoption.

Hidden Details: Thoughts on Trade Secrets From the UK

By Guest Author for TradeSecretsLaw.com: Jeremy Morton (April 12th, 2016)

As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Jeremy Morton, an English solicitor who advises in the areas of intellectual property and data protection law.

As reported recently by Seyfarth Shaw's lawyers in this very blog, on 13 April the European Parliament will vote on the EU Commission's proposed trade secrets directive. Many English legal practitioners, more or less familiar with our non-statutory protections for confidential information, will assume that nothing will change when the directive is implemented. We already protect trade secrets pretty well, unlike other EU countries for whom reform is seen as essential in order to fill legislative voids. But if we look more closely at the EU proposals, we find plenty of uncertainties that could arise under the EU proposals.

For starters, the English law of breach of confidence is not limited to 'trade secrets'.

Why Does it Matter?

This is important not only to provide certainty for business that confidential information will be protected, but to provide comfort that businesses won't be hit with a rush of unmeritorious claims. The draft directive tackles that, in Article 6(2), providing that defendants should be able to ask the court for appropriate relief where a claim is "*manifestly unfounded and the applicant is found to have initiated the legal proceedings abusively or in bad faith*". We currently deal with abuse of process through sanctions such as striking-out or adverse costs awards. But the draft directive provides that such measures may include an award of damages. Like the current sanctions for unjustified threats in connection with intellectual property rights in the UK, this will be a trap for the unwary.

Perhaps the biggest uncertainty arises from the role of the European Court of Justice (CJEU). When the Directive is in force, the CJEU will have jurisdiction to determine the outcome of cases where the correct interpretation of the Directive is unclear. That will mean that the English courts will have to apply CJEU decisions, as well as themselves referring issues to the CJEU. Our law will change. And trade mark practitioners know how difficult things can become when one has to follow CJEU jurisprudence.

What is a Trade Secret?

Let's look briefly at the current position in English law. Information will be protected where it has the necessary quality of confidence and provided it has been communicated in circumstances importing an obligation of confidence. It does not have to be a 'trade secret'. This equitable protection for confidentiality is separate from other measures such as contract law, the Data Protection Act, the Computer Misuse Act, database right and copyright. It has also developed into the relatively new area of privacy protection.

Trading Secrets

Employees are under an implied duty of good faith which imports contractual obligations of confidentiality under English law. But after their employment ends they need only preserve 'trade secrets', and may use information having a lesser degree of confidentiality, subject to their restrictive covenants. For example, customer details might be protected during employment but not after. What is a 'trade secret'? We may feel that we would know it when we see it. Confidential chemical formulae sound like 'trade secrets', for example. The well-known *Faccenda Chicken* case provides guidance here: for example, we should look at the nature of the employment, and whether the information can be easily isolated from other, non-confidential information.

Recital 1 of the draft directive gives several examples of potential trade secrets: technology; customers/suppliers (in contrast with *Faccenda Chicken* where customer details were not 'trade secrets' after employment ended); business plans; market research. More interesting is the following cumulative definition of a "Trade Secret" in Article 2(1):

"…secret in the sense that it is not … generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question…

…has commercial value because it is secret…

…has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

Alarm bells are gently tinkling. Not only is this very different from the *Faccenda Chicken* guidelines, but it introduces the Euro-speak notion of "*circles that normally deal with the kind of information*" (how do we establish who they are?), and requires a direct link between secrecy and commercial value. Would this cover information to which employees have access because of their employment, during the term of that employment, even if not a 'trade secret' in the English sense? What about a famous author, who publishes a new book under a pseudonym for artistic reasons, but whose true identity is then revealed by a trusted intermediary against their wishes? That information arguably has *more* commercial value once in the public domain (although less *personal* value).

Also, since this directive will be concerned with "trade secrets", does it permit the English courts to continue to protect 'lesser' confidential information that does not meet the "trade secret" threshold, or does it do away with such protections? That would be surprising. It does say (in Article 1(2a)(a) and (b)) that "*in relation to the exercise of mobility of employees*", nothing in the directive offers any ground for limiting employees' use of information not constituting a trade secret as defined in the directive, or limiting their use of experience and skills honestly acquired in the normal course of their employment. This seems to preserve the protections for employees under *Faccenda Chicken*.

Springboard Relief

The other aspect of the new legislation that will be fascinating to see unfold is its take on springboard relief. This is where a defendant has gained a head-start by using confidential information, even if they are no longer using it as such or it is no longer confidential. It's a tricky area, which the English courts have discretion to tackle via the terms of any injunctive relief granted.

Article 11 of the draft directive sets out the available measures that a court may order against a defendant. These include "*the prohibition to produce, offer, place on the market or use infringing goods*". "Infringing goods" has a special meaning here, as defined in Article 2, namely: "*goods whose design, characteristics, functioning, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed*". What remains unspoken here is, first, the extent

to which (if any) those goods must continue to embody any aspect of the trade secrets in question; secondly, whether the information must still be a trade secret at the time relief is granted; and thirdly whether "unlawfully" means only in breach of the trade secrets laws implementing the directive, or could include other unlawful steps under national laws. There is plenty of room for argument on this.

Summing up, many details are far from clear (unsurprisingly), and astute English lawyers will have plenty to get their teeth into with this new legislation. Judges in other countries may be less eager to grapple forcefully with protection of trade secrets, potentially leading to forum shopping in favour of the English courts. And let's not even talk about Brexit…

Jeremy Morton is an English solicitor who advises in the areas of intellectual property and data protection law. www.harbottle.com/jeremy-morton

European Parliament Debates Proposed Trade Secrets Directive

By Daniel P. Hart (April 13th, 2016)

As we have previously reported in this blog, this week marks a milestone in ongoing attempts in the European Union to overhaul the existing regulatory framework for the protection of trade secrets. Earlier today, members of the European Parliament debated the compromise text of the proposed Directive to protect trade secrets. A full recording of the debate can be found here.

Today's debate came on the heels of a press conference earlier in the day by MEP Constance Le Grip (European People's Party — France), the rapporteur who has shepherded the proposed directive in the European Parliament for the past 18 months. For those who have been following the proposed Directive, Ms. Le Grip's comments provide an interesting explanation of the varying political considerations that produced the compromise text, including balancing the concerns of businesses and the rights of workers.

Questions posed by journalists at the press conference are perhaps more interesting. If the questions posed by journalists (as well as the comments by many MEPs during the debate) are any indication, considerable opposition exists to the proposed directive. While business groups and many MEPs have largely welcomed the proposed directive, other MEPs and some interest groups have expressed concern that the proposed directive will be used by companies to stifle whistleblowers and journalists. Notably, the compromise text already includes language that expressly guarantees protection of whistleblowers, freedom of the press, and other fundamental rights, as follows:

Member States shall ensure that the application for the measures, procedures and remedies provided for in this Directive is dismissed when the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

(a) for exercising the right to freedom of expression and information as set out in the Charter of Fundamental Rights of the European Union, including respect for freedom and pluralism of the media;

(b) for revealing a misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;

(c) the trade secret was disclosed by workers to their representatives as part of the legitimate exercise of their representative functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise;

(e) [*sic*] for the purpose of protecting a legitimate interest recognised by Union or national law.

See Proposed Directive [compromise text], Art. IV. Yet despite this language, opponents of the proposed directive have argued that the directive does not go far enough in protecting

whistleblowers. Whether such concerns are wide enough to scuttle the proposed directive remains to be seen.

Breaking News: European Parliament Approves Trade Secrets Directive

By Daniel P. Hart (April 14th, 2016)

Earlier today (by a vote of 503 to 131 with 18 abstentions), the European Parliament approved the text of a proposed Directive for the protection of trade secrets in the European Union. Once approved by the European Council (which is typically a formality), the Directive will be binding on all EU member states and will require member states to enact national legislation that meets certain minimum requirements for the protection of trade secrets.

Up to this point, no legal framework has existed for the protection of trade secrets throughout the EU. In 2013, the European Commission commissioned a study on trade secrets protections in EU member states by comparison to legal protections for trade secrets in the United States, Switzerland, and Japan. Following that study, which highlighted the lack of uniformity in the laws of EU member states, the European Commission proposed an initial draft of the directive to remedy perceived inadequacies in the existing legal framework. With adoption of the new directive, EU member states now have a period of 24 months to adopt national legislation that meets certain minimum standards of protection for trade secrets.

Several key provisions of the Directive are notable.

First, the directive **provides a uniform definition of a "trade secret**" as "information which meets all the following requirements: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is a secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret." (Directive, Art. 2 ¶ 1.)

Second, the directive **defines the following conduct as unlawful**:

- "Acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful, whenever carried out by . . . unauthorised access to, appropriation of, or copy of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced; [and] any other conduct which, under the circumstances, is considered contrary to honest commercial practices." (Directive, Art. 3 ¶ 2.)

- "The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions: (a) have [*sic*] acquired the trade secret unlawfully; (b) be in breach of a legally valid confidentiality agreement or any other duty to maintain secrecy of the trade secret; [or] (c) be in breach of a legally valid contractual or any other duty to limit the use of the trade secret." (Directive, Art. 3 ¶3.)

- "The acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of acquisition, use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of [Art. 3 ¶3]." (Directive, Art. 3 ¶4.)

- "The production, offering or placing on the market of infringing goods, or import, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret when the person carrying out such activities knew, or should, under the circumstances, have known that the trade secret was used unlawfully within the meaning of [Art. 3 ¶3]." (Directive, Art. 3 ¶5.)

Third, the Directive establishes exceptions that essentially **creates a whistleblower defense to trade secrets misappropriation claims**, similar to language in the U.S. Senate's version of the proposed Defend Trade Secrets Act pending in the U.S. Congress. The relevant portion of the text provides as follows:

"Member States shall ensure that the application for the measures, procedures and remedies provided for in this Directive is dismissed when the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases: (a) for exercising the right to freedom of expression and information as set out in the Charter of Fundamental Rights of the European Union, including respect for freedom and pluralism of the media; (b) for revealing a misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest; (c) the trade secret was disclosed by workers to their representatives as part of the legitimate exercise of their representative functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise; (e) for the purpose of protecting a legitimate interest recognised by Union or national law."

(Directive, Art. 4.)

Fourth, the Directive **requires member states to establish limitations periods for trade secrets claims**, as follows: "Member States shall, in accordance with this article, lay down rules on the limitation periods applicable to the substantive claims and actions for the application of the measures, procedures and remedies pursuant to this Directive. . . . The duration of this limitation period shall not exceed six years." (Directive, Art. 7.)

Fifth, the Directive requires member states to establish **minimum rules for protection and preservation of trade secrets during litigation**, including measures that "shall at least include the possibility (a) to restrict access to any document containing trade secrets or alleged trade secrets submitted by the parties or third parties, in whole or in part, to a limited number of persons; (b) to restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed, and their corresponding records or transcript to a limited number of persons; (c) to make available to any person other than those comprised in the limited number of persons referred to in points (a) and (b) a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed or redacted."

To take full advantage of the protections provided by the new Directive, as well as the protections that will be afforded by the Defend Trade Secrets Act in the U.S., employers on both sides of the Atlantic would be wise to review their existing practices and procedures to ensure that they are taking "reasonable steps under the circumstances" to protect their trade secrets, including:

- Reviewing IT policies and procedures for protecting sensitive information;
- Reviewing existing employment agreements, including restrictive covenant agreements in jurisdictions where they are permitted, to ensure that they provide appropriate levels of protection permitted under applicable law;
- Reviewing existing employment policies regarding protection of confidential information and ensuring that employees are adequately trained on the policies; and
- Reviewing employee exiting policies and procedures to ensure that sensitive information is returned upon the end of employment.

In addition, in light of the new whistleblower protections afforded by both the EU Directive and the Defend Trade Secrets Act, employers should ensure that their policies and practices are in compliance with all applicable anti-retaliation laws and that management employees are properly trained on best practices to reduce the risks of whistleblower retaliation claims.

For more on these practical tips and background to the Directive and the Defend Trade Secrets Act, please check out our recent webinar on these topics.

Webinar Recap! International Non-Compete Law Update

By Dominic Hodson (July 31, 2016)

In this installment in Seyfarth's 2016 Trade Secrets Webinar Series, International attorney Dominic Hodson focused on non-compete considerations from an international perspective. Dominic discussed general principals and recent international developments in non-compete issues around the globe. Companies who compete in the global economy should keep in mind these key points:

- Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. However, there are some common requirements and issues regarding enforceability based on the region, particularly in common law jurisdictions such as the UK, Canada (excluding Quebec), Australia/New Zealand, and Singapore/Hong Kong. A restrictive covenant is void unless it is reasonable to protect a legitimate interest of the employer; simply wanting to stop competition post-termination is not a legitimate interest.

- Outside of common law countries, there is no uniformity in rules, and every country must be taken separately. There are often detailed statutory rules that the clause must fulfill, but nevertheless there are repeating themes: There must be reasonableness to the non-compete agreement, and you must require proportionality between the clause and the interest sought to be protected.

- With respect to non-common law countries, liquidated damaged are often allowed. Civil law countries tend to be much more forgiving of liquidated damages and don't have the same rules regarding "penalty clauses."

Social Media and Privacy

Q&A Concerning IP Protection and Social Media Issues in the Workplace

By Robert B. Milligan (January 14th, 2016)

The explosion of digital and social media enables companies to work more efficiently and to easily and creatively promote their products and services to large audiences across the globe. Modern technological developments in the workplace, however, come with modern issues – one such challenge for companies is protecting intellectual property (IP) and confidential information in today's dynamic, digital and mobile environment.

On January 19, the State Bar of California is bringing together leading IP and employment attorneys from private industry, public agencies, private law firms and law schools for a conference in San Francisco on these issues: "Intellectual Property Protection and Social Media Issues in the Workplace." Seyfarth Shaw is a proud sponsor of the conference and I have the honor of serving as the conference chair.

In this Q&A, I was interviewed by CREATe.org President and CEO Pamela Passman about the conference and these important issues.

1) The issue of social media and IP protection is a daunting one for companies. As you were putting together topic areas for the conference, how did you decide what to focus on?

Indeed, companies are challenged today with a broad range of issues related to IP protection in today's digital and social media environment. For this conference, we considered the top areas of concern and information that would be most practical for participants.

For example, the session "Ownership of IP in the Workplace," looks at the types of agreements you should and can have employees sign. The "IP Issues You Didn't Know you Had" panel takes a look at emerging challenges stemming from hackers, third-party hosted sites, open source software, unscrupulous partners who claim your IP as their own, and users of torrents and the Darknet, to name a few. The luncheon program – "Testimonials and Endorsements: How to Properly Involve Employees" – will provide an overview of the restrictions on the use of testimonials and endorsements and will offer general and specific approaches to staying out of trouble when navigating new advertising media. Closing the day is the session featuring Ms. Passman – "IP Theft in the Workplace." It looks at insider threats – both malicious and unintentional – to confidential information and provides practical steps for improving the protection of IP, including trade secrets.

2) Why should companies be more proactive when it comes to social media in the workplace?

First, companies need to be aware of the legal risks related to the use of social media in the workplace. These include:

- Document retention and electronic discovery issues

- Exposure of confidential information and trade secrets and cybersecurity concerns
- Securities law concerns, including insider trading
- Vicarious liability for discrimination, retaliation, defamation, invasion of privacy, trademark & copyright infringement, obscene material and otherwise illegal content

A 2013 Ponemon study, while a bit dated, illustrates some of the scenarios that can get companies in trouble. They interviewed 3317 individuals in six countries (United States, United Kingdom, Brazil, France, China, and Korea) and found that of those surveyed:

- Over half e-mail business documents from their workplace to their personal e-mail accounts (41 percent say they do it at least once a week);
- 41 percent download intellectual property to their personally owned smart phones or tablets; and
- 37 percent use file-sharing applications (e.g., Dropbox™ or Google Docs™) without company permission.

3) Where should companies start? Is it necessary for your company to have a social media policy in place and, if so, what should your policy include?

Social media platforms attract large audiences worldwide: Facebook has over 1.4 billion account holders and over 936 million daily active users. LinkedIn has over 364 million members in over 200 countries in territories. Given these statistics, it is more than likely that some of your employees are active social media users. It is absolutely necessary for your company to have a social media policy in place, one which should address:

- Proper Use: acknowledging your company provides its employees internet access, that it is a useful business tool and that employees must use it properly
- Use During Work Hours While Using Company Provided Equipment/Systems**:** no or limited use of social media by your employees unless directly related or necessary to perform the job
- Limitations on Social Media Activity to Those Impacting The Company: acknowledging that social media may be a personal activity and that your company will only seek to impose limitations on its use when it impacts your company, co-workers, clients or third parties who deal with your company

4) Are there any legal issues for your company to consider regarding employee social media activity?

If your company decides to implement a social media policy or agreement, there are legal implications to take into consideration. Most states have limits on what you can ask an employee regarding social media accounts. Other implications include (but are not limited to):

- First Amendment: protects free speech
- Fourth Amendment: protects against unreasonable searches and seizures
- National Labor Relations Act (NLRA): An employee is protected under the National Labor Relations Act (NLRA) when engaging in a discussion of work conditions with other co-workers on social media, including sharing information about wages, complaining about policies or managers and expressing union support. Section 7 of the NLRA prohibits employers from enacting policies that stifle or prevent employees from engaging in “concerted activity” for “mutual aid and protection”

You should always consult with your company's legal department to determine the limitations you can impose on employee social media activity.

5) You have mentioned trade secrets as one type of IP that is particularly vulnerable. What are trade secrets and how can employees access company trade secrets in the workplace?

Because trade secrets can be central to your company's competitive edge, these company 'crown jewels' must be properly protected in the workplace. There are six factors to determine whether information constitutes a trade secret:

- Extent known outside company
- Extent known by employees and others inside company
- Measures taken by company to protect secrecy
- Value of trade secret to company and competitors
- Time, effort and money expended in development
- Ease of difficulty which it can be properly acquired or duplicated by others

Examples of trade secrets include: product launches and designs, formulas, processes, business plans and customer lists. Rogue employees and business partners account for 90% of trade secret misappropriation, the vast majority of this misappropriation occurring by electronic means.

The Legality of Tracking Employees By GPS

By Karla Grossenbacher (February 16th, 2016)

Over the past several years, technology has dramatically increased employee accountability in the workplace. For example, in an office environment, employees are expected to respond to emails immediately because they are either sitting in front of their computers or carrying a mobile device on which they can access their email. As for employees who work outside the office, the availability of employer-issued phones and, alternatively, the proliferation of BYOD policies, has resulted in off-site employees being generally just a phone call away. In specific industries in which employees drive motor vehicles while conducting business for the employer, yet another method of accountability exists: Global Positioning Systems (GPS).

For businesses that provide transportation or delivery services, it is not surprising to find that such employers have installed GPS devices in the vehicles used by their employees. The use of such devices can benefit both the employer and the employee in situations in which delivery status needs to be checked or a vehicle breaks down. In all likelihood, the employee in these situations is aware that a GPS device has been installed on the company vehicle he or she is driving and that the employee's movements are being tracked while on duty. Privacy issues tend to arise, however, when employers use GPS data in connection with investigating alleged misconduct in the workplace.

There cases in which courts have addressed the legal parameters of an employer's use of GPS devices to track workers in order to investigate potential misconduct are few but nonetheless instructive.

In *Elgin v. Coca-Cola Bottling Co.* (E.D.Mo. 2005), the employer attached a GPS device to a company-owned vehicle used by the employee to service vending machines after a cash shortage was reported on a number of machines. Although the employee was cleared of any wrongdoing in the investigation, when he found out that a GPS device had been installed on the company vehicle he drove during the investigation, he filed a claim for intrusion upon seclusion under state law. The court rejected this claim, noting that the vehicle was owned by the employer and the only information potentially revealed by the alleged "intrusion" was the whereabouts of the company vehicle. In another case, *Tubbs v. Wynne Transport* (S.D. Texas 2007), the court dismissed an invasion of privacy claim against an employer who had used information gathered by a GPS device that had been installed as a matter of course on a company-owned vehicle driven by the employee to perform his duties as a truck driver. The court did not, however, provide any substantive analysis regarding its decision to dismiss the claim.

Elgin and *Tubbs* both involved employers attaching GPS devices to company-owned vehicles. The balance between the employer's interest in rooting out misconduct and the employee's individual privacy rights shifts, however, when an employee's personal vehicle is at issue — even if it is used for work purposes. In *Cunningham v. New York Department of Labor* (NY Ct. App. 2013), a state employee was under investigation for falsifying time records and voucher information related to work travel and had used his personal vehicle during work hours in connection with some of the suspected

misconduct. As part of its investigation into the alleged misconduct, the employer had a GPS device installed on the employee's personal vehicle to gather information about his movements during periods in which he was suspected of misconduct. The employee was ultimately discharged and filed suit to exclude the GPS data from evidence at his disciplinary hearing based on federal and state constitutional grounds.

The New York Court of Appeals held that installation of the GPS device on the employee's personal vehicle was an unreasonable search under constitutional law principles. Although the Court held the search was reasonable at its inception because the employer had a reasonable suspicion that the employee was engaging in workplace misconduct, the search was unreasonable in its scope because it had not been designed to obtain only the information the employer needed to determine if workplace misconduct had occurred. Rather, the employer had monitored the employee's personal vehicle 24/7, as opposed to only during working hours, and made no attempt to remove the device prior to the employee's scheduled vacation. The Court concluded that "[w]here an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable."

However, the extent to which a personal vehicle is used for work purposes can alter the analysis. In two cases involving the revocation of a New York City taxi cab driver's license for over-charging passengers, two New York city state courts held that taxi drivers had no legitimate expectation of privacy in GPS data gathered from the Taxi Technology System (TTS) installed on the cabs. The court also held that, even if the drivers had a legitimate expectation of privacy in the data, the city had a legitimate interest in determining whether or not the driver was overcharging passengers and had narrowly tailored its search to obtain information from the TTS only during the driver's work hours. In these two cases, even though the cabs were personally owned by the drivers, the court found that the cab drivers had limited privacy rights with respect to the vehicles because they were open to public use and subject to regulation by the state. The regulatory authority required that all city cabs have the TTS equipment installed and drivers were required to use the system to transmit information regarding location, trip and fare information to the regulatory authority.

The takeaway from these cases is that, although an employer appears to be on solid ground attaching a GPS device to a company-owned vehicle and using data gathered by the device in an investigation of workplace misconduct, especially where the employee is aware the device is on the vehicle and the information is only being gathered while the employee is on duty, caution should be taken in attaching a GPS device to a personal vehicle used by the employee for work purposes. Employers also need to be mindful of complying with state laws regarding electronic surveillance. California, Connecticut, Delaware and Texas all have laws requiring either notice or consent prior to placing a GPS on another person's motor vehicle.

As the foothold of technology sinks deeper into the terrain of the workplace, the privacy issues confronted by employers will only grow in complexity. However, courts have been reticent about making broad pronouncements about the intersection of law and technology in the workplace. As the Supreme Court stated in *United States v. Kwon*, a case involving a state employer's review of an employee's text messages on a state-issued pager, "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role society has become clear." This restraint, while understandable, can leave employers with unanswered questions about how to balance the competing interests of legitimate business needs and individual privacy concerns in the workplace, particularly where technology is involved. Perhaps in 2016, the courts will offer more guidance in this area.

Monitoring Employee Communications: A Brave New World

By Karla Grossenbacher (April 29th, 2016)

Over the last decade, communication via email and text has become a vital part of how many of us communicate in the workplace. In fact, most employees could not fathom the idea of performing their jobs without the use of email. For convenience, employees often use one device for both personal and work-related communications, whether that device is employee-owned or employer-provided. Some employees even combine their personal and work email accounts into one inbox (which sometimes results in work emails being accidentally sent from a personal account). This blurring of the lines between personal and work-related communications creates novel legal issues when it comes to determining whether an employer has the right to access and review all work-related communications made by its employees.

Employers have legitimate business reasons for monitoring employee communications. Take, for example, the scenario in which an employee leaves her employment, and the employer is concerned that she has taken proprietary information or solicited clients in violation of her duty of loyalty or a contractual agreement. Another common scenario that gives rise to the need for employers to review all of an employee's work-related emails is when the employer is in litigation that requires production of employee communications.

Most employers are comfortable with the notion that, with a properly worded policy that provides notice to employees of the ability and intent to monitor email, an employer can access emails on an email server provided by the employer. However, what about cases in which the employer does not provide the email service? With employees using web-based emails, like Gmail and Hotmail, and texts to communicate in the workplace, the relevant communications may be elsewhere. In these situations, what are an employer's rights to access and review such communications?

An employer's ability to review electronic communications is governed by the Electronic Communication Privacy Act (ECPA) and the Stored Communications Act (SCA). The ECPA prohibits the interception of electronic communications, and the term "interception" as used in the ECPA has been interpreted so narrowly that this title of the ECPA rarely comes into play in cases involving an employer's review of employee email or texts. The SCA makes it illegal to access without authorization a facility through which electronic communication service is provided and thereby obtain access to communications in electronic storage.

With regard to an employer's review of employee emails sent through web-based email accounts like Gmail or Hotmail, the most frequent scenario confronted by courts is one in which a former employer accesses the web-based email of a former employee, looking for evidence of malfeasance. In these cases, the former employer is typically able to access the former employee's web-based email account because the employee has saved her username and password on a device provided by the employer, which was returned at termination, or failed to delink an account from such a device. In these cases,

courts have been reluctant to punish the former employee for failing to take appropriate steps to secure their own personal, and allegedly private, communications.

For example, a district court in New York considered an employee's claim that his former employer's review of emails in his Hotmail account after his termination violated the SCA because it was unauthorized. The defendant argued that its review of the emails did not violate the SCA because the employee had implicitly authorized its review of the emails on his Hotmail account because the employee had stored his username and password on the employer's computer system or forgot to remove such an account from an employer-provided phone before returning it.

The court rejected this argument, holding that it was tantamount to arguing that, if the employee had left his house keys on the reception desk at the office, he would have been implicitly authorizing his employer to enter his home without his knowledge. The court also noted that the employer's computer usage policy did not provide the necessary authorization because it only referred to communications sent over the employer's systems.

Likewise, a district court in Ohio confronted with similar facts, refused to hold the plaintiff responsible for his own failure to safeguard his information. In this case, the employee had turned in a company-issued blackberry upon termination without first deleting the Gmail account he had added to the phone. The former employer reviewed the emails in the former employee's Gmail account, and the former employee alleged that this violated the SCA. The former employer argued that the former employee had negligently or implicitly consented to their review of the emails in her Gmail account by returning the blackberry to the company without deleting the account. However, the court held that the employee's "negligence" in leaving the Gmail account on her phone when she turned it in was not tantamount to her authorizing the defendant to review the emails on her Gmail account.

However, a federal district court in California reached a different result in a case involving text messages. In this case, a company had sued its former employee for misappropriating trade secrets when it discovered, upon his termination, a number of text messages on the former employee's company-issued iPhone that documented his misappropriation. The former employee had forgotten to delink his Apple account from the company phone he returned, and thus, his text messages continued to go to the phone — and his former employer. The court granted the company's motion to dismiss the former employee's counter claim that the company's review of his text messages violated the SCA. The court held that text messages stored on phones are not in "electronic storage" within the meaning of the SCA, citing a Fifth Circuit case that reached the same conclusion about text messages. Of course, a violation of the SCA is not the only issue in these cases.

For example, in this case, the employee also alleged that his employer had invaded his privacy. However, the court held that the employee had no reasonable expectation of privacy in a company-owned phone that was no longer in his possession. In contrast to the two cases above, the court found that the employee's failure to undertake precautions to maintain the privacy of his text messages showed he had no right to exclude others from accessing them.

The main lesson from these cases is that, if an employer wants to have the ability to review all employee communications that take place in the workplace, the employer needs to have, at a minimum, a policy that specifically provides for the right to monitor and review, for legitimate business reasons, any work-related communications made by the employee on a device provided by the company or a personal device used for work purposes. (Although the SCA does not require any showing about the employer's motives in accessing the emails, a traditional invasion of privacy analysis would take this into account.) As a practical matter, the employer may not have the ability to access such accounts, but where access is available, this policy language is critical.

Acknowledgments:

Special thanks to Karthik Raman, Colleen Vest, and Bridget Rabb for their work in putting together this year in review.