

# 2017 Trading Secrets

An Annual Compilation of Seyfarth Shaw's Trade Secrets Law, Non-Competes, and Computer Fraud Blog Posts from 2017.



JAN

FEB

MAR

APR

MAY

JUN

JUL

AUG

SEP

OCT

NOV

DEC



# Trading Secrets



Dear Clients and Friends,

2017 was another great year for our blog and our dedicated Trade Secrets, Non-Compete, and Computer Fraud group. 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, and Corporate Counsel. We are pleased to provide you with the 2017 Year in Review, which compiles our significant blog posts from 2017 and highlights our blog's authors. For a general overview of 2017, we direct you to our Top 2017 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2017 Trade Secrets Webinar Series—Year in Review blog entry, which together provide a summary of key cases and legislative developments in 2017, 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, and access to our well-received Trade Secret Webinar Series, archived from 2011 to the present. In 2017, we offered audio podcasts, guest authors, and provided an additional enhanced Resources page on the blog. We also continued our special feature tracking federal trade secret legislation. In 2018, we will offer content on recent developments in Defend Trade Secrets Act decisions, non-compete, computer fraud, data breach 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 2017, we hosted six webinars, which are listed in this Review. For those who missed any of the programs in the 2017 webinar series, the webinars are available on the blog or CD upon request.

We kicked off the 2018 webinar series with a program entitled, "2017 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 2018 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 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

2017 Trade Secrets Webinar Series..... 3

2018 Trade Secrets Webinar Lineup ..... 4

Our Authors..... 5

2017 Summary Posts ..... 22

Trade Secrets Legislation..... 34

Trade Secrets..... 37

Computer Fraud and Abuse Act ..... 116

Non-Competes & Restrictive Covenants ..... 119

Legislation ..... 135

International ..... 140

Social Media and Privacy ..... 144



# Trading Secrets



## 2017 Trade Secrets Webinar Series

- [2016 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law](#)  
*February 2, 2017*
- [Simple Measures for Protecting Intellectual Property and Trade Secrets](#)  
*April 20, 2017*
- [Protecting Confidential Information and Client Relationships in the Financial Services Industry](#)  
*April 27, 2017*
- [Protecting Your Trade Secrets in the Pharmaceutical Industry](#)  
*June 28, 2017*
- [Trade Secret Protection: What Every Employer Needs to Know](#)  
*July 18, 2017*
- [Protecting Trade Secrets in the Social Media Age](#)  
*September 28, 2017*



## 2018 Trade Secrets Webinar Lineup

- 2017 National Year in Review: What You Need to Know About the Recent Cases/ Developments in Trade Secrets, Non-Compete, and Computer Fraud
- Protecting Confidential Information and Client Relationships in the Financial Services Industry
- The Anatomy of a Trade Secret Audit
- Protecting Trade Secrets from Cyber and Other Threats
- Protecting Trade Secrets Abroad and Enforcing Rights Abroad and in the U.S.
- Criminal Trade Secret Theft Updates

# Trading Secrets



## 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 a partner 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 senior 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 senior 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.



**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.



**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.

# Trading Secrets



**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.



**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.



**Anne Dunne** is a litigation associate in Seyfarth Shaw LLP's Boston office, and is a member of the firm's Commercial Litigation, Construction, Securities and Financial Litigation, Consumer Financial Services Litigation and Distribution & Franchise Litigation and Counseling practice groups. Ms. Dunne is also a member of the White Collar, Internal Investigations and False Claims Team. Her clients include banking institutions, manufacturers, supermarkets, contractors and various other business ventures.



# Trading Secrets



**Dean Fanelli, Ph.D.**, is a partner in the Intellectual Property Department of Seyfarth Shaw LLP's Washington D.C. office. Dr. Fanelli's practice focuses on the chemical, pharmaceutical, and biotechnology industries and his expertise lies in patent portfolio creation and management, counseling, technology transactions, due diligence, opinion work, including drafting novelty, freedom-to-operate, and invalidity opinions, and inter partes review and post grant review proceedings. Dr. Fanelli also focuses his practice on Paragraph IV litigation strategies, Hatch-Waxman litigation, and biosimilar market assessment and litigation strategy.



**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.



**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.

# Trading Secrets



**Thomas Haag, Ph.D.**, is a partner in the Intellectual Property Department of Seyfarth Shaw LLP's Washington D.C. office where he co-chairs the firm's chemical & life science patent team. His practice focuses on pharmaceutical and biotechnology patent counseling, due diligence and licensing/transactional matters; as well as Hatch-Waxman litigation and patent opinion work.



**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.



**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.



**Cassie Howman-Giles** is a senior associate in Seyfarth Shaw Australia's International Labor & 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.

# Trading Secrets



**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.



**Emily Kesler** is an associate in the Commercial Litigation Department of the Seyfarth Shaw LLP's Chicago office. Her practice includes a variety of complex commercial litigation disputes, including those which involve business torts, non-compete and non-solicitation agreements, trade secrets, requests for injunctive relief, unfair competition, product liability, and alleged violations of state and federal consumer protection statutes.



**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.



**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.

# Trading Secrets



**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.



**Robyn Marsh** is an associate for the Litigation Department in the Chicago office of Seyfarth Shaw LLP. Prior to joining Seyfarth Shaw, Ms. Marsh worked as a litigation associate at a boutique Chicago law firm specializing in products liability and professional liability defense. In that capacity, she represented and defended Fortune 500 domestic and foreign automobile manufacturers, appearing in both state and federal courts on behalf of her clients.



**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.



**Alex Meier** is an associate in Seyfarth's Labor and Employment Group. His practice includes the full array of federal remedial rights, non-compete and trade secret litigation, Fair Credit Reporting Act class actions, and workplace safety and health disputes. Mr. Meier has spearheaded multiple initiatives to promote conscious improvements to case management tools and client-facing resources, including document automation tools, operational summaries, and existing resource identification.

# Trading Secrets



**Dawn Mertineit** is a partner 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.



**Patrick Muffo** is a partner in the firm's Chicago office, where he focuses his practice on intellectual property litigation and prosecution. Mr. Muffo represents clients in a wide range of complex litigation matters, particularly in the patent, trade secret, copyright, DMCA, and trademark areas. He represents clients in all phases of litigation, from pre-suit investigation through trial. His litigation experience involves technology such as 3D printing, Internet-connected speakers, e-commerce and software technology, data encryption techniques, and HVAC motors.



**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.



**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.



# Trading Secrets



**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.



**Craig Simonsen** is a senior litigation paralegal in the Seyfarth Shaw LLP's Labor & Employment, Workplace Safety and Health (OSHA/MSHA), Environmental Compliance, Enforcement & Permitting, and Commercial Litigation Practice Groups. Mr. Simonsen is an author and managing editor of several books, including the Pearson Prentice Hall Legal Series titles *Essentials of Environmental Law*, 3rd ed. (2007), and *Computer-Aided Legal Research (CALR) on The Internet* (2006). Mr. Simonsen has spoken on occupational safety and health law, environmental law, and internet legal resource topics at the American Industrial Hygiene Conference and Expo and other professional conferences and webinars.



**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





# Trading Secrets



## 2017 Summary Posts

- [Top Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2017](#)  
*By Robert B. Milligan and Daniel Joshua Salinas (February 16, 2018)*
- [2017 Trade Secrets Webinar Series Year In Review Released](#)  
*By Robert B. Milligan (December 7, 2017)*

## Trade Secrets Legislation

- [Texas Legislature Clarifies and Expands the Texas Uniform Trade Secrets Act](#)  
*By Andrew P. del Junco & Jesse M. Coleman (June 20, 2017)*

## Trade Secrets

- [2016 Trade Secrets Webinar Series Year in Review Released](#)  
*By Robert B. Milligan (January 5, 2017)*
- [Save the Date: Seyfarth Attorneys to Speak at AIPLA Trade Secret Law Summit in Atlanta](#)  
*By Erik Weibust & Eric Barton (January 10, 2017)*
- [Seyfarth Shaw Attorneys Contribute to ABA's Annual Trade Secret Law Report](#)  
*By Robert B. Milligan (January 24, 2017)*
- [Texas Court of Appeals Rules That Mere Suspicions of Trade Secret Misappropriation Are Insufficient to Trigger the Discovery Rule](#)  
*By Andrew P. del Junco & Jesse M. Coleman (January 25, 2017)*
- [Top Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2016](#)  
*By Robert B. Milligan & Daniel Joshua Salinas (January 27, 2017)*
- [Seyfarth Litigation Partners to Present on Trade Secrets Law at Pharmaceutical and Biotechnology Roundtable](#)  
*By Robert B. Milligan (March 3, 2017)*
- [Texas Court Holds Mere Possession and Opportunity to Use Trade Secrets is Sufficient for Misappropriation](#)  
*By Jesse M. Coleman & Andrew P. del Junco (March 22, 2017)*
- [Seyfarth Attorneys Published in Bloomberg's White Collar Crime Report](#)  
*By Seyfarth Shaw LLP (March 23, 2017)*

# Trading Secrets



- [Second Shot at Anti-SLAPP Motion Fails in Trade Secrets Dispute Involving Former Beer Worker](#)  
*By Daniel Joshua Salinas & Robert B. Milligan (March 30, 2017)*
- [Introducing Seyfarth's BioLoquitur Blog](#)  
*By Seyfarth Shaw LLP (April 7, 2017)*
- [Seyfarth IP, International, Trade Secrets, and Corporate Attorneys to Participate in ITechLaw 2017 World Technology Conference in Chicago](#)  
*By Seyfarth Shaw LLP (April 12, 2017)*
- [Seyfarth Shaw, AlixPartners, and Directors Roundtable to Present Cyber Risk Management Program in San Francisco](#)  
*By Seyfarth Shaw LLP (April 13, 2017)*
- [Trade Secret Protection: What Every California Employer Needs to Know](#)  
*By Seyfarth Shaw LLP (April 14, 2017)*
- [Are My Customer Lists a Trade Secret?](#)  
*By Alex Meier & Eric Barton (April 17, 2017)*
- [Don't Forget to Establish Personal Jurisdiction in Defend Trade Secrets Act Cases](#)  
*By Eric Barton (April 19, 2017)*
- [Webinar Recap! Simple Measures for Protecting Intellectual Property and Trade Secrets](#)  
*By Patrick Muffo & Kevin Mahoney (April 26, 2017)*
- [Enlisting Government Help to Protect Your Trade Secrets](#)  
*By Wayne Bond (April 27, 2017)*
- [Webinar Recap! Protecting Confidential Information and Client Relationships in the Financial Services Industry](#)  
*By J. Scott Humphrey, Dawn Mertineit & Robyn Marsh (May 4, 2017)*
- [Joshua Salinas a Panelist for "Trade Secrets in 2017: Recent Legal Trends and Developments LIVE Webcast"](#)  
*By Seyfarth Shaw LLP (May 19, 2017)*
- [Seyfarth Attorneys to Speak at the Management Association's 2017 Employment Law Conference](#)  
*By Seyfarth Shaw LLP (May 22, 2017)*
- [Great Employee or Insider Threat?](#)  
*By Guest Author for TradeSecretsLaw.com (May 25, 2017)*
- [Robert Milligan to Present "Trade Secret Mediations in 2017: What You Need to Know" Webinar](#)  
*By Seyfarth Shaw LLP (May 26, 2017)*

# Trading Secrets



- [Seyfarth's Trade Secrets Group Earns Top Tier Ranking from Legal 500 Second Year in Row](#)  
*By Seyfarth Shaw LLP (June 8, 2017)*
- [Trade Secrets May Retain Protections Despite Disclosure to Single Competitor](#)  
*By Daniel Joshua Salinas & Sierra J. Chinn-Liu (June 9, 2017)*
- [Court Allows Plaintiff to Amend Complaint to Add Defend Trade Secrets Act Claim After Discovery Reveals Alleged Continued Misappropriation](#)  
*By Daniel Joshua Salinas & Lauren Leibovitch (June 12, 2017)*
- [Briefing Recap! Trade Secret Protection: What Every California Employer Needs to Know](#)  
*By Daniel Joshua Salinas, Scott E. Atkinson & Robert B. Milligan (June 14, 2017)*
- [Emerging Issues In the Defend Trade Secrets Act's Second Year](#)  
*By Robert B. Milligan & Daniel Joshua Salinas (June 14, 2017)*
- [Illinois Federal Court Allows Inevitable Disclosure Theory in Defend Trade Secrets Act Case](#)  
*By Kyla Vick & J. Scott Humphrey (June 28, 2017)*
- [Webinar Recap! Protecting Your Trade Secrets in the Pharmaceutical Industry](#)  
*By Justin K. Beyer, Marcus Mintz, Dean L. Fanelli, Ph.D. & Thomas A. Haag, Ph.D. (July 5, 2017)*
- [California Federal Court Finds CUTSA Preemption on Unfair Competition Claim in Uber Row](#)  
*By Robert B. Milligan & Sierra J. Chinn-Liu (July 7, 2017)*
- [The Third Circuit Addresses the Defend Trade Secrets Act and Appears to Have Applied the Inevitable Disclosure Doctrine](#)  
*By Erik Weibust & Andrew Stark (July 11, 2017)*
- [The Smartphone: A Treasure Trove of Evidence in Trade Secret Cases](#)  
*By Guest Author for TradeSecretsLaw.com (July 13, 2017)*
- [The Neutral Corner: Using Forensic Neutrals in Trade Secret Disputes](#)  
*By Guest Author for TradeSecretsLaw.com (July 20, 2017)*
- [Robert Milligan to Speak on the "Injunctive Relief" Panel at the Sedona Conference on Developing Best Practices for Trade Secret Issues](#)  
*By Seyfarth Shaw LLP (July 21, 2017)*
- [How to Catch Trade Secret Thieves Who Try to Cover Their Tracks: A Forensic Perspective](#)  
*By Guest Author for TradeSecretsLaw.com (July 24, 2017)*
- [How To Address Wipers in Trade Secret Cases](#)  
*By Guest Author for TradeSecretsLaw.com (August 2, 2017)*
- [Webinar Recap! Trade Secret Protection: What Every Employer Needs to Know](#)  
*By Robert B. Milligan & Daniel Joshua Salinas (August 11, 2017)*



# Trading Secrets



- [Key Employee Departures and Trade Secret Risk Assessment](#)  
*By Guest Author for TradeSecretsLaw.com (August 24, 2017)*
- [File Share Platforms and Business Risk](#)  
*By Corey Bieber (September 5, 2017)*
- [Wisconsin High Court Affirms High Summary Judgment Bar to Trade Secret Misappropriation Claims](#)  
*By Kevin Mahoney (September 6, 2017)*
- [Locating Digital Breadcrumbs: Programs Can Run, But They Can't Hide](#)  
*By Guest Author for TradeSecretsLaw.com (October 4, 2017)*
- [Big Brown v. PowerPoint Pilferers in Trade Secret Spat](#)  
*By Eric Barton (October 10, 2017)*
- [Webinar Recap! The Defend Trade Secrets Act—The Biglaw Partner and Forensic Technologist Perspective](#)  
*By Robert B. Milligan (November 20, 2017)*

## Computer Fraud and Abuse Act

- [Supreme Court Refuses to Hear Password-Sharing Case, Leaving Scope of Criminal Liability Under Computer Fraud and Abuse Act Unclear](#)  
*By Scott E. Atkinson (October 16, 2017)*

## Non-Competes & Restrictive Covenants

- [Webinar Recap! 2016 National Year In Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law](#)  
*By Robert B. Milligan, Michael Wexler & Daniel Joshua Salinas (February 7, 2017)*
- [In Georgia, the Blue-Pencil Only Strikes Overly Broad Non-Competes and Does Not Rewrite Them](#)  
*By Stephanie Stewart (February 27, 2017)*
- [Can You Say P-e-c-u-l-i-a-r-i-t-i-e-s? Seyfarth's Cal-Peculiarities Guide Is Here Highlighting Quirks in California Restrictive Covenant and Trade Secret Law](#)  
*By James D. McNairy & Robert B. Milligan (May 9, 2017)*
- [The Latest East Coast/West Coast Conflict: Massachusetts Courts Consider the Application of California Law in Non-Compete Litigation](#)  
*By Erik Weibust & Dallin Wilson (June 21, 2017)*
- [Nevada Enacts New Non-Compete Law](#)  
*By Robert B. Milligan & Lauren Leibovitch (July 6, 2017)*

# Trading Secrets



- [Robert Milligan to Present “Growing Importance of Trade Secrets in Protecting Emerging Technology” Webinar](#)  
*By Seyfarth Shaw LLP (July 6, 2017)*
- [Illinois Employers Should Not Depend on Blue Penciling to Enforce Restrictive Covenants](#)  
*By Marcus Mintz & Emily Kesler (July 31, 2017)*
- [Now Available! 2017-2018 Edition of the Trade Secrets and Non-Competes 50 State Desktop Reference](#)  
*By Seyfarth Shaw LLP (August 4, 2017)*
- [Robert Milligan to Present “Understanding and Exploring the DTSA” CLE Webinar](#)  
*By Seyfarth Shaw LLP (August 23, 2017)*
- [Robert Milligan to Present Defend Trade Secrets Act Webinar](#)  
*By Seyfarth Shaw LLP (October 24, 2017)*
- [Federal Court Rules Against Calzone Franchisor in Meaty Lawsuit Against Former Franchisee](#)  
*By Erik Weibust & Anne Dunne (December 14, 2017)*

## Legislation

- [Will the Massachusetts Legislature Finally be Able to Keep Its New Year’s Resolution to Pass Non-Compete Reform?](#)  
*By Katherine Perrelli, Erik Weibust, Dawn Mertineit & Andrew Stark (January 25, 2017)*
- [Missouri Legislator Introduces Bill to Ban Restrictive Covenants](#)  
*By J. Scott Humphrey (April 3, 2017)*
- [Massachusetts Legislature Schedules Hearing on Non-Compete Reform](#)  
*By Katherine Perrelli, Erik Weibust & Andrew Stark (October 3, 2017)*

## International

- [\\$1.2 Million Dispute Between West Mountain Environmental and the Shanghai Hehui Environmental Technology](#)  
*By Wan Li, Robert B. Milligan & Craig B. Simonsen (April 5, 2017)*
- [Robert Milligan to Present “Effective Use of Non-Compete Agreements by International Employers” Webinar](#)  
*By Seyfarth Shaw LLP (July 10, 2017)*

## Social Media and Privacy

- [WannaCry Ransomware Attack: What Happened and How to Address](#)  
*By Richard Lutkus, EnCE, EnCEP, CEH (May 15, 2017)*

# Trading Secrets



- [ABA Encourages Encryption of Emails When Transmitting Confidential Client Information](#)  
*By Erik Weibust & Andrew Stark (May 22, 2017)*
- [Technically Speaking, Cybersecurity Isn't About Speaking Technically](#)  
*By Guest Author for TradeSecretsLaw.com (July 6, 2017)*
- [Webinar Recap! Protecting Trade Secrets in the Social Media Age](#)  
*By Justin K. Beyer, Dawn Mertineit & Ryan Behndleman (October 20, 2017)*
- [Now Available! Seyfarth Shaw's 2017-2018 Edition of the Social Media Privacy Legislation Desktop Reference](#)  
*By Seyfarth Shaw LLP (November 20, 2017)*



## 2017 Summary Posts

# Trading Secrets



## Top Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2017

By Robert B. Milligan & Daniel Joshua Salinas (February 16, 2018)

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

### 1. Notable Defend Trade Secrets Act Developments

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



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

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

While the language of the DTSA appears to bar or significantly limit the inevitable disclosure doctrine, some federal district courts have nonetheless used the doctrine as grounds for injunctions. See, e.g., *Fres-co Systems USA, Inc. v. Hawkins*, 2017 WL 2376568 (3rd Cir. June 1, 2017) (“Given the substantial overlap (if not identity) between Hawkins’s work for Fres-co and his intended work for Transcontinental—same role, same industry, and same geographic region—the District Court was well within its discretion to conclude Hawkins would likely use his confidential knowledge to Fres-co’s detriment.”); *Molon Motor and Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545 (N.D. Ill. May 11, 2017) (“allegations on the direct competition between the parties, as well as the allegations on the





# Trading Secrets



employment breadth and similarity of Desai's quality control work at the two companies, are enough to trigger the circumstantial inference that the trade secrets inevitably would be disclosed by Desai to Nidec.")

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

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

## 2. Other Notable Trade Secret Cases

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

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

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

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

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



# Trading Secrets



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

### 3. Notable Restrictive Covenant and Forum Selection Clause Cases

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

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

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

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

The 3rd Circuit Court of Appeals in *In re: Howmedica Osteonics Corp.*, 867 F.3d 390 (3d Cir. 2017), held that, as a matter of impression, the court would apply a four-step framework (in sequence) to evaluate a transfer motion involving a forum-selection clause applicable to some, but not all, parties: (1) the forum-selection clauses; (2) the private and public interests relevant to non-contracting parties; (3)



# Trading Secrets



threshold issues related to severance; and (4) which transfer decision most promotes efficiency while minimizing prejudice to non-contracting parties' private interests. Under this analysis, the 3rd Circuit denied sales representatives' motion to transfer a District of New Jersey case to the Northern District of California, severed the former employers' claims against the sales representatives from its claims against the sales representatives' new employer, and transferred claims against the new employer to Northern District of California.

## 4. New State Legislation Regarding Restrictive Covenants

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

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

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

## 5. Vermont's New Social Media Legislation

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

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

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

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



# Trading Secrets



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

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

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

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

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

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

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

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

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

The Opinion makes clear that lawyers must have an open exchange of communication with their clients about the securities measures their firms are taking to safeguard the clients’ confidential information. They must recognize that the determination of whether they are making reasonable efforts in



# Trading Secrets



enhancing their cybersecurity is a fact-based analysis to be made on a case-by-case basis and may not be uniformly employed.

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.

# Trading Secrets



## 2017 Trade Secrets Webinar Series Year in Review

*By Robert B. Milligan (December 7, 2017)*

Throughout 2017, 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 six webinars:

1. 2016 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Simple Measures for Protecting Intellectual Property and Trade Secrets
3. Protecting Confidential Information and Client Relationships in the Financial Services Industry
4. Protecting Your Trade Secrets in the Pharmaceutical Industry
5. Trade Secret Protection: What Every Employer Needs to Know
6. Protecting Trade Secrets in the Social Media Age



As a conclusion to this well-received 2017 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 [DVD 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 2018, and we will release the 2018 trade secrets webinar series topics in the coming weeks.

### [2016 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, Michael Wexler, and Joshua Salinas, reviewed noteworthy cases and other legal developments from across the nation over the last year 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 2017.

- The DTSA can be a powerful tool to protect intellectual capital. However, in order to take full advantage of the DTSA, businesses should carefully check their agreements with employees, handbooks and equity awards to make sure they contain language mandated by the Defend Trade Secrets Act.



# Trading Secrets



- 2016 was a record year for data and information security breaches. Organizations should alert and train employees on following company policies, 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.
- Several states enacted laws to limit the scope and duration of non-competes in 2016. There were also some significant decisions limiting their scope and enforceability in 2016 as well. Companies should have their non-disclosure and non-compete agreements reviewed to ensure that they comply with the latest state and federal laws, including the new Defend Trade Secrets Act.

## Simple Measures for Protecting Intellectual Property and Trade Secrets

Every day, companies unknowingly give up intellectual property and trade secrets, which they could have otherwise protected with simple processes. Poor R&D policies may not capture patent rights on a company invention, or a faulty or simply outdated employment agreement may not protect a customer list used by an employee who leaves for a competitor. These pitfalls are easily avoidable by implementing measures on the front end and educating employees on the basics of intangible property and how to protect it.

In this webinar, Seyfarth attorneys Patrick Muffo and Kevin Mahoney provided a basic overview of what types of intellectual property and trade secrets are protectable, how to protect them, and helpful tips to ensure that a company is doing everything they can to avoid common issues associated with intangible property.

- Businesses routinely miss out on opportunities to protect their valuable intellectual property simply because they do not realize that their inventions or developments qualified as intellectual property in the first place. Particularly in light of changes in patent law that reward the first party to file for a patent—regardless of whether they invented something first or not—it is important to be proactive about applying for patent protection as early as possible. If a business believes that an invention may qualify for either a design or utility patent, it should take steps to start the patent application process as soon as possible.
- Copyright and trademark protection are also an important, and often overlooked, component of intellectual property protection. Trademarks are routinely granted for patterns, brands, logos, trade dress, and other identifying images which businesses may have thought were too generic to qualify for such protection. Copyrights are also becoming an increasingly important tool in protecting computer code.
- Trade secrets are also intellectual property, but are governed by an entirely different set of laws and are protected in different ways, often through litigation. Because the recently-enacted Defend Trade Secrets Act of 2016 requires the owner of trade secrets to have taken reasonable steps to protect that information, businesses should identify their processes for identifying what information qualifies as a trade secret and what steps they have taken to protect that information, including the implementation of employee confidentiality agreements. Confidentiality agreements drafted before 2016 need to be updated to include certain whistleblower language as a result of the passage of the Defend Trade Secrets Act.



# Trading Secrets



## Protecting Confidential Information and Client Relationships in the Financial Services Industry

In Seyfarth's third installment of its 2017 Trade Secrets Webinar series, Seyfarth attorneys Scott Humphrey, Robyn Marsh, and Dawn Mertineit focused on trade secret and client relationship considerations in the banking and financial services industry, with a particular focus on a firm's relationship with its FINRA members. This webinar also included practical steps financial institutions can implement to protect trade secrets and client relationships; tips on what to do if your trade secrets are improperly removed or disclosed or if a former employee is violating his/her restrictive covenant agreements; how to prosecute a case against a former employee who is a FINRA member; and the impact of the Protocol for Broker Recruiting on trade secrets and client relationships.

- Remember that you can seek court injunctive relief (Temporary Restraining Order and, possibly, Preliminary Injunction) before proceeding in FINRA.
- The definition of a trade secret varies by company, but you must take adequate steps to protect them as a company, and the information cannot be publicly available or easily discovered, to merit enforcement under the law.
- Employers can take steps at all stages to protect their confidential information—don't forget to implement on-boarding and off-boarding procedures, as well as policies and procedures that will be in effect during an employee's tenure, to protect your information before a problem arises.

## Protecting Your Trade Secrets in the Pharmaceutical Industry

Seyfarth's fourth installment, presented by Justin Beyer, Marcus Mintz, Dean Fanelli, and Thomas Haag, focused on how to define and protect trade secrets in the pharmaceutical industry, including a review of significant civil and criminal cases in the industry, a discussion on how federal and state trade secret statutes and decisions may impact the protection of trade secrets, and best practices for protecting trade secrets from invention through sale.

- Trade secret laws cover any information which is confidential, kept confidential, and from which the owner derives economic benefit. In order to maintain such protections, owners must be vigilant and proactive about maintaining the secrecy of their trade secret information. One of the ways in which employers should do so is to update their employment agreements to comply with the immunity notice provisions of the Defend Trade Secrets Act, without which the employer may lose the ability to recover attorney's fees or double damage awards.
- In the pharmaceutical and biotechnology space, companies should also take active steps to develop internal guidelines and protocols for the identification and protections of information that may be the subject of trade secret protection, whether that information is related to research and development, strategic business plans, or future opportunities and trends. These steps include, but are not limited to: (i) advising all employees of the confidential and proprietary nature of their work; (ii) limiting access to proprietary and confidential information to only those employees requiring such information; (iii) actively monitoring how information is distributed both internally and externally; and (iv) regularly updating employees of the necessity to maintain confidentiality of all information.
- Trade secrets are particularly valuable with respect to the development of biologics. Given long clinical development timelines, composition patents covering reference biologics may be about





# Trading Secrets



to expire or will have already expired, at time of marketing approval. Confidential and proprietary details relating to reference protein drug production, isolation, storage and delivery; as well as its post-transnational modifications, are at least as important to know as the identity of the reference protein's amino acid sequence, when creating a biosimilar. Thus these trade secrets represent potentially enormous barriers to market entry for third party developers of biosimilar versions. They should, therefore, be kept in the strictest confidence.

- If a company does, however, find itself in a situation in which it fears that an employee has or may misappropriate its trade secret information, it should take certain immediate steps, including: (a) reminding the employee of his/her obligations; (b) forensically imaging and reviewing the employee's email communications, downloading history, and/or internet activity; (c) cutting off the employee's access to company confidential information, as soon as notice is provided that the employee is taking a position with a competitor; and (d) if necessary, filing suit to recover and protect the secrecy of the trade secrets. Once trade secrets are disclosed in public, whether properly or improperly, it becomes exceedingly difficult to prove the ongoing secrecy of the information and even harder to put the secret back in its box.

## Trade Secret Protection: What Every Employer Needs to Know

In Seyfarth's fifth installment, attorneys Robert Milligan and Daniel Joshua Salinas were joined by Jim Vaughn, one of California's leading forensics experts. The panel focused on how to help employers navigate the tricky trade secrets waters and provided best practices for trade secret protection.

- Employers should review their non-disclosure and non-compete agreements to determine whether they have accurately defined the scope of categories of their confidential information, as well included the whistleblower immunity language required under the Defend Trade Secrets Act. Additionally, they should ensure their agreement complies with recent changes in non-compete law, including legislative changes in Nevada, Oregon, Idaho, and Alabama.
- Employers should consider how they treat employee-owned devices for work, as well as corporate-issued mobile devices. Getting access to those devices may prove to be challenging upon an employee's departure. Having technology and a policy in place to allow the employer to gain access to their data is critical.
- Effectively protecting trade secrets includes not only creating an internal culture of confidentiality with employees but also limiting information made available to vendors and subcontractors and having appropriate trade secret protection agreements with third parties.

## Protecting Trade Secrets in the Social Media Age

There is no denying that social media has transformed the way companies conduct business, but social media and related issues in the workplace can be a headache for employers. In light of the rapid evolution of social media, companies today face significant legal challenges on a variety of issues, ranging from employee privacy and protected activity to data practices, identity theft, cybersecurity, and protection of intellectual property.

- In Seyfarth's sixth installment, attorneys Justin Beyer, Dawn Mertineit, and Ryan Behndleman discussed the relationship between trade secrets and social media, including the interplay between social media privacy laws and workplace investigations and how developing internal





## Trade Secrets Legislation

# Trading Secrets



## Texas Legislature Clarifies and Expands the Texas Uniform Trade Secrets Act

*By Andrew P. del Junco & Jesse M. Coleman (June 20, 2017)*

On May 19, 2017, Texas Governor Greg Abbott signed into law several amendments to the Texas Uniform Trade Secrets Act (“TUTSA”), located in Chapter 134A of the Texas Civil Practice & Remedies Code. The amendments go into effect on September 1, 2017. In doing so, Texas has aligned its statute more closely with federal law and codified recent judicial interpretations of the law.



Two events precipitated the amendments, one legislative, one judicial. In the first, Congress passed the Defend Trade Secrets Act (“DTSA”) in May 2016, which provides a federal cause of action for trade-secret misappropriation. In the second, the Texas Supreme Court announced in *In re M-I L.L.C.*, 505 S.W.3d 569 (Tex. 2016) that a presumption exists that a party is authorized to participate and assist in the defense of a trade-secret misappropriation claim under TUTSA, which presumption cannot be surmounted unless the trial court considers a seven-factor balancing test. These events resulted in the following key changes to the TUTSA:

### Trade Secret

The amended TUTSA expands the definition of “trade secret” to more closely harmonize Texas law with the DTSA’s definition. Specifically, the Texas Legislature added to the definition “all forms and types of information” including, by way of example, “business, scientific, technical, economic, or engineering information,” design, prototype, plan, program device, code, or procedure, “whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.” There remain, however, several important differences between the amended TUTSA and the DTSA. First, the revised TUTSA definition of trade secrets lists illustrative examples of the form or type of information that can constitute a trade secret, whereas § 1839(3) of the DTSA confines a trade secret as “financial, business, scientific, technical, economic, or engineering information.” Second, in contrast to the DTSA, TUTSA includes a “list of actual or potential customers or suppliers” as an example of trade-secret information. Third, a trade secret under TUTSA, unlike the DTSA, need not be “related to a product or service used in, or intended for use in, interstate or foreign commerce.”

### Injunctive Relief

TUTSA generally allows for injunctive relief from actual or threatened misappropriation. The amendment, however, preserves and clarifies the common-law rule that an employee cannot be enjoined “from using the general knowledge, skill, and experience acquired during employment.” *Sharma v. Vinmar Int’l, Ltd.*, 231 S.W.3d 405, 424 (Tex. App.—Houston [14th Dist.] 2007, pet. dism’d).

### Willful and Malicious Misappropriation

Under the pre-amendment TUTSA, a trade-secret owner must establish “willful and malicious” misappropriation as a precondition to an award of exemplary damages and attorney’s fees. The

# Trading Secrets



amendments clarifies that “willful and malicious misappropriation,” means “intentional misappropriation resulting from the conscious disregard of the rights of the owner of the trade secret,” which definition is derived from the Seventh Circuit’s definition in *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 730 (7th Cir. 2003) (applying the Illinois Uniform Trade Secret Act). The amended TUTSA also defines the phrase, previously undefined by TUTSA, that triggers an award of exemplary damages—“clear and convincing evidence”—by using the definition in section 41.001(2) of the Texas Civil Practice and Remedies Code.

## **Trade Secret “Owner”**

The amendment, which relies on the modified definition of “owner” found in the DTSA, provides that an “owner” of a trade secret is a “person or entity in whom or in which rightful, legal, or equitable title to, or the right to enforce rights in, the trade secret is reposed.” Thus, the amendment clarifies that certain nonowners, such as licensees, may be entitled to file a claim for trade-secret misappropriation under TUTSA.

## **Seven-Factor Balancing Test**

The amendment codifies the Texas Supreme Court’s holding in *In re M-I L.L.C.*, which sets out a seven-factor balancing test that courts must consider before excluding a party or a party’s representative at any stage of the proceedings, including discovery, pretrial, or trial. The revised TUTSA presumes that parties are allowed to participate and be present during proceedings and may not be excluded until after a court considers the following seven factors:

- (1) the value of an owner’s alleged trade secret;
- (2) the degree of competitive harm an owner would suffer from the dissemination of the owner’s alleged trade secret to the other party;
- (3) whether the owner is alleging that the other party is already in possession of the alleged trade secret;
- (4) whether a party’s representative acts as a competitive decision maker;
- (5) the degree to which a party’s defense would be impaired by limiting that party’s access to the alleged trade secret;
- (6) whether a party or a party’s representative possesses specialized expertise that would not be available to a party’s outside expert; and
- (7) the stage of the action.

TUTSA, as amended, is now one of the most modern and comprehensive laws governing trade secrets in the United States.



# Trading Secrets



## Trade Secrets



## 2016 Trade Secrets Webinar Series Year in Review Released

*By Robert B. Milligan (January 5, 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.





# Trading Secrets



## 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.



# Trading Secrets



- 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



# Trading Secrets



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 confidentiality 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

# Trading Secrets



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



# Trading Secrets



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 damages 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

# Trading Secrets



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 as well as 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 one's 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



# Trading Secrets



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).

# Trading Secrets



## Save the Date: Seyfarth Attorneys to Speak at AIPLA Trade Secret Law Summit in Atlanta

*By Erik Weibust & Eric Barton (January 10, 2017)*

Seyfarth attorneys Erik Weibust and Eric Barton will be presenting on trade secret and noncompete legislative updates at the American Intellectual Property Law Association's 2017 Trade Secret Summit, being held on March 2-3, 2017 at Emory University in Atlanta, Georgia. The theme of

the Summit is "Emerging Standards During Tumultuous Times," and it will include panels of leading practitioners and members of the judiciary and law enforcement on topics ranging from the Defend Trade Secrets Act to cybersecurity, to competitive intelligence, as well as roundtable discussions and networking opportunities. CLE credits will be available.





# Trading Secrets



## Seyfarth Shaw Attorneys Contribute to ABA's Annual Trade Secret Law Report

*By Robert B. Milligan (January 24, 2017)*

Seyfarth attorneys Robert Milligan, Joshua Salinas, Amy Abeloff, and Michael Cross contributed to this year's ABA Section of Intellectual Property Law, Trade Secrets and Interferences with Contracts Committee Annual Trade Secret Law Report.

The Annual Report, found [here](#), covers the significant trade secrets cases from around the country that were decided in 2016. The Report is a good resource for staying current in trade secrets developments and trends.



# Trading Secrets



## Texas Court of Appeals Rules That Mere Suspicions of Trade Secret Misappropriation Are Insufficient to Trigger the Discovery Rule

*By Andrew P. del Junco & Jesse M. Coleman (January 25, 2017)*

Applying new Texas Supreme Court precedent, a Texas Court of Appeals recently held that a six-year-old cease-and-desist letter alleging trade-secret misappropriation did not constitute proof of knowledge for purposes of the discovery rule. By allowing for the accrual date of this claim to be deferred, the court appears to have made it easier for trade-secret plaintiffs to overcome the statute-of-limitations defense in the future.



According to the opinion issued by the First Court of Appeals in Houston, Garner Environmental Services, Inc. (“Garner”) provides disaster-response training and related services. In 2008, Garner’s then-vice president quit, formed a competing company called First in Rescue, Safety and Training, LLC (“FIRST”), and hired several Garner employees. In January 2009, Garner sent FIRST a letter accusing it of wrongfully using Garner’s customer lists, contacts, and other trade secrets to solicit Garner’s customers. Garner based these allegations solely on the fact that, shortly before sending this letter, Garner had learned that a client scheduled to attend one of Garner’s training classes switched at the last minute to attend a class held by FIRST instead. Later that month, FIRST responded that it had not stolen Garner’s trade secrets because Garner’s customer lists and contacts were readily available to the general public, could be replicated from memory, and were therefore not confidential information in the first instance. FIRST’s letter also pointed out that none of the former Garner employees had entered into non-compete or non-solicitation agreements while employed by Garner, so they were not prohibited from contacting Garner’s customers. Apparently, this mollified Garner because it did not file suit against FIRST at this time.

Fast-forward nearly five years: In late 2013, FIRST filed suit against a former employee that had gone to work for another competitor. At an unspecified time in 2014, after reviewing documents the employee had filed in that suit, Garner determined that FIRST had unlawfully used Garner’s confidential information. So, in July 2015—more than six years after sending the initial cease-and-desist letter in January 2009—Garner filed suit against FIRST asserting, *inter alia*, a claim for misappropriation of trade secrets. FIRST filed for summary judgment, arguing that all of Garner’s claims were barred by the statute of limitations because it discovered or should have discovered the nature of its injury in January 2009. Garner argued in response that the discovery rule applied and, as such, limitations did not begin to run until it discovered the injury in 2014 when it reviewed the documents filed in connection with the lawsuit FIRST’s former employee had asserted against a third party. The trial court granted FIRST’s motion and dismissed Garner’s claims with prejudice.



# Trading Secrets



On appeal, the sole issue before the Court of Appeals was when Garner discovered, or in the exercise of reasonable diligence should have discovered, the nature of its injury. Under the discovery rule, the accrual of a claim is deferred until the injured party learned of, or in the exercise of reasonable diligence should have learned of, the wrongful act causing the injury. Garner argued that the court of appeals was bound by the Texas Supreme Court's recent decision in *Southwestern Energy Production Co. v. Berry-Helfand*, 491 S.W.3d 699 (Tex. 2016), which involved the discovery rule in the context of trade-secret misappropriation. In that case, the court held that surmise, suspicion, and accusation, even if sufficient to make one aware of a potential for misuse of trade secrets, are not facts that in the exercise of reasonable diligence would lead to the discovery of theft of trade secrets. Furthermore, the *Southwestern* court held that the defendant asserting the limitations defense "ha[d] not identified any evidence revealing what [the plaintiff] would have discovered had she made further inquiry."

Finding "no meaningful differences between *Southwestern* and this case," the Garner court noted that although Garner alleged in its January 2009 letter that FIRST had stolen its trade secrets, it had no facts to support these allegations other than mere suspicion that FIRST was competing with Garner's clients. As in *Southwestern*, accusations were insufficient to establish knowledge of injury, the discovery rule applied. The Court of Appeals further noted that FIRST did not explain why it is entitled to have Garner's statements of accusation construed as proof of knowledge while having its own statements of denial construed as "lawyer posturing" upon which Garner could not reasonably rely. The court thus rejected FIRST's attempt to have its cake and eat it too.

FIRST also argued that Garner could have discovered the injury had it conducted presuit depositions under Texas Rule of Civil Procedure 202, which it did not do. In order to take a presuit deposition under Rule 202, the petitioner must show that there is a reason that the deposition must occur before the anticipated lawsuit is filed, and not after. The Court of Appeals, however, reiterated that Garner lacked any proof of its suspicions and thus had no basis to establish that FIRST had any information in its possession that could justify a Rule 202 deposition. A petitioner is also entitled to conduct a Rule 202 deposition if it demonstrates that the likely benefit of the requested deposition to investigate a potential claim outweighs the procedure's burden or expense. The Court of Appeals stated: "To allow a rule 202 deposition in th[is] situation would require the other party to reveal the confidential information in their possession," which the court concluded was too heavy a burden on FIRST. Thus, FIRST failed to establish a date (prior to Garner's stated discovery date in 2014) by which Garner knew or, with reasonable diligence, could have discovered the nature of its injury. Accordingly, the Court of Appeals reversed the judgment of the trial court, and remanded for further proceedings.

The take-away from this case is that potential plaintiffs who, although suspicious, lack concrete proof that a potential defendant has misappropriated its trade secrets, will, on account of the *Southwestern* and *Garner* decisions, likely find it easier to assert the discovery rule to defer the accrual date of its misappropriation claim. Moreover, according to Garner, such potential plaintiffs will find it difficult, if not impossible, to meet their burden to establish the necessity of the information to be entitled to conduct a Rule 202 presuit deposition. It remains to be seen, however, if this case might decrease the use of Rule 202 depositions in trade-secret cases. Still, the boot-and-suspenders approach of attempting a Rule 202 deposition may be the better course to preserve the legal rights of a potential misappropriation plaintiff.

*Garner Envtl. Services, Inc. v. First In Rescue, Safety & Training, LLC*, 01-16-00388-CV, 2016 WL 7671377 (Tex. App.—Houston [1st Dist.] Dec. 22, 2016, no. pet. h.)



# Trading Secrets



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

*By Robert B. Milligan & Daniel Joshua Salinas*

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

# Trading Secrets



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





# Trading Secrets



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.).



# Trading Secrets



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





# Trading Secrets



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 (Zhangjiang) 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.

# Trading Secrets



## Seyfarth Litigation Partners to Present on Trade Secrets Law at Pharmaceutical and Biotechnology Roundtable

*By Robert B. Milligan (March 3, 2017)*

On Wednesday, March 15, 2017, as part of Seyfarth Shaw's Pharmaceutical and Biotechnology Roundtable at Seyfarth's Boston office, Litigation Department Chair Katherine Perrelli and Partner Erik Weibust will be presenting with Carmine Nigro, the FBI's Counterintelligence Strategic Partnership Coordinator in Boston, on civil vs. criminal trade secret protection, including a discussion of the Defend Trade Secrets Act of 2016.

The pharmaceutical and biotechnology industries face unique legal challenges and media misperceptions, and they continue to ride a wave of uncertainty as the Trump administration takes control. In preparation of changes to come, Seyfarth attorneys have developed a comprehensive afternoon for in-house attorneys to get insight and get practical takeaways in this critical time of change.



# Trading Secrets



## Texas Court Holds Mere Possession and Opportunity to Use Trade Secrets is Sufficient for Misappropriation

*By Jesse M. Coleman & Andrew P. del Junco (March 22, 2017)*

The San Antonio Court of Appeals recently held that an applicant for a temporary injunction in a trade-secret-misappropriation case under the Texas Uniform Trade Secrets Act is not required to show the defendant is actually using trade-secret information. Instead, the applicant need only show that the defendant possesses trade secrets and is in a position to use them.

Age Industries, Ltd. (“AI”) is a manufacturer of packaging materials for whom Christopher Michael Hughes worked for nearly 20 years as a general manager. In late June 2016, Hughes resigned his employment with AI. Hughes never signed an agreement restricting him from competing with AI. Prior to resigning, Hughes had discussed creating a business to compete with AI. In early June, Diamondback Corrugated Container, LLC (“Diamondback”) was created and, shortly after his resignation, Hughes was hired to be its operations manager.



Two months later, AI sued Hughes and Diamondback for, inter alia, misappropriation of trade secrets under the Texas Uniform Trade Secrets Act, and obtained a temporary restraining order. Following the hearing on AI’s application for a temporary injunction, the trial court granted a temporary injunction against Hughes that (1) required Hughes to account for all documents in his possession belonging to AI, and (2) enjoined Hughes from disclosing AI’s proprietary or trade-secret information, including AI’s sales journals, customer lists, or pricing information.

Hughes appealed the trial court’s temporary injunction against him, contending, among other things, that AI failed to produce sufficient evidence of a probable, imminent, and irreparable injury, because AI only established a fear of possible misappropriation of trade secrets. The court of appeals noted that “the very purpose of an injunction is to prevent disclosure of trade secrets pending trial, [so AI] is not required to show [Hughes] is actually using the information.” Relying on authority from the Dallas, Austin, and Fort Worth Courts of Appeals, the San Antonio Court of Appeals required AI to instead show only that Hughes possesses the trade secrets and is in a position to use them.

Drawing all legitimate inference in favor of the trial court’s order granting the temporary injunction, the court of appeals concluded that AI made the proper showing under this standard. AI presented evidence during the temporary-injunction hearing that shortly before he resigned, Hughes downloaded a large quantity of data from his AI computer onto a USB storage device. Additionally, AI offered evidence that certain financial information Hughes maintained while working for AI could not be located after his resignation, and that Hughes had some of AI’s confidential information on his home computer.



# Trading Secrets



Moreover, at the temporary-injunction hearing, Hughes could not testify that emails he sent to a co-worker at Diamondback did not contain AI's proprietary information.

This evidence—combined with the fact that Hughes left AI to become the operations manager of a company that was formed to compete with AI—established that Hughes was in a position to use AI's trade secrets to gain an unfair market advantage. Therefore, the appellate court held the trial court did not abuse its discretion in concluding that AI established a probable, imminent, irreparable injury.

This case demonstrates that it is not necessary to present evidence of trade-secret use; mere possession and an opportunity to use is sufficient at the temporary injunction stage.

[Hughes v. Age Industries, Ltd.](#), 04-16-00693-CV, 2017 WL 943423 (Tex. App.—San Antonio Mar. 8, 2017, no. pet. h.)

# Trading Secrets



## Seyfarth Attorneys Published in Bloomberg's White Collar Crime Report

*By Seyfarth Shaw LLP (March 23, 2017)*

Seyfarth continues to be at the forefront of issues involving the Defend Trade Secrets Act ("DTSA"). On March 17, 2017, two Seyfarth attorneys, Andrew Boutros and Alex Meier, published the first-ever in-depth analysis of the intersection between the DTSA and the Racketeer Influenced and Corrupt Organizations Act ("RICO") in Bloomberg's White Collar Crime Report.



The article, "[An Endangered Claim Reemerges: The Defend Trade Secrets Act Breathes New Life Into Trade-Secrets-Based RICO Claims](#)," examines how the DTSA, in certain circumstances, may create liability under RICO for the misappropriation of trade secrets. Pre-DTSA, courts were hesitant to impose RICO liability based on trade-secrets misappropriation, because even fraudulent acts with the end goal of misappropriating trade secrets did not present a threat of ongoing criminal activity ("continuity," in RICO parlance). With the DTSA's passage, however, the misappropriation, copying, disclosure, and use of trade secrets constitute "predicate acts" that may satisfy RICO's continuity requirement. The article analyzes two scenarios that may create civil RICO liability: First, a coordinated departure involving multiple employees defecting to join the same competitor; and, second, when a company repeatedly hires key employees in an attempt to acquire its competitors trade secrets.

"[An Endangered Claim Reemerges: The Defend Trade Secrets Act Breathes New Life Into Trade-Secrets-Based RICO Claims](#)" is reproduced with permission from *White Collar Crime Report*, 12 WCR 243, 03/17/2017. Copyright 2017 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>.

# Trading Secrets



## Second Shot at Anti-SLAPP Motion Fails in Trade Secrets Dispute Involving Former Beer Worker

*By Daniel Joshua Salinas & Robert B. Milligan (March 30, 2017)*

A California federal district court has recently given employers a small victory against former employees who misappropriate trade secrets and assert whistleblower immunity or the litigation privilege as after-the-fact defenses. The federal district court for the Eastern District of California recently [rejected](#), for a second time, a defendant's anti-SLAPP motion to strike a trade secret lawsuit brought against him by his former employer. Notably, the court rejected the defendant former employee's whistleblower and litigation privilege defenses as inapplicable, thereby allowing the beer company's trade secret action to proceed.



On March 1, 2013, the beer company sued the former employee for, among other things, trade secret misappropriation and breach of nondisclosure agreements. The former employee subsequently filed a motion to dismiss and strike the Complaint under California's anti-SLAPP statute. Specifically, the former employee argued that the Complaint was an attempt to punish him for purportedly exercising his constitutional rights of petition and free speech in connection with a consumer class action litigation that he filed against the company exactly one week before.

The federal district court denied the former employee's anti-SLAPP motion and concluded that the company's claims did not arise out of the former employees protected litigation activity. The former employee appealed.

The Court of Appeals for the Ninth Circuit reversed the district court and remanded back so the district court could consider the next prong of the anti-SLAPP analysis, the plaintiff's probability of prevailing on its claims.

Upon its second review of the former employee's anti-SLAPP motion, the federal district court concluded that the company had demonstrated a likelihood of prevailing on its trade secret misappropriation and breach of contract claims. The court then turned to and rejected the former employee's substantive legal defenses of public policy, whistleblower immunity, and the litigation privilege.

First, the court rejected the former employee's argument that confidentiality agreements are unenforceable as a matter of public policy. The court refused to adopt such a sweeping rule that would render confidentiality agreements unenforceable that would allow former employees to disclose trade secret or confidential information.

Second, the court acknowledged that California provides protection to whistleblowers but only when the employee discloses reasonably based suspicious of illegal activity to a **governmental agency**. The court concluded that such protections did not apply to employees who disclose information to their attorneys in order to further a class action against an employer.





# Trading Secrets



Lastly, the court rejected the former employee's argument that the misappropriation of documents in furtherance of anticipated litigation was protected under the litigation privilege. The court reasoned that the litigation privilege does not protect against illegal activity that causes damage and to protect such threats is inconsistent with the purposes of the anti-SLAPP statute.

It would be interesting to see the court's analysis and decision, however, had the alleged misappropriation occurred after the enactment of the new Defendant Trade Secrets Act ("DTSA"), which appears to provide broader whistleblower protections. The court in this case highlighted that California's whistleblower statute protected only disclosures to government agencies and not a defendant's attorneys. The DTSA, however, protects individuals from criminal and civil liability under any federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding. (For additional information on the DTSA and its implications regarding whistleblowers, please [see our DTSA Guide](#).)

Nonetheless, this case confirms that employees do not have an unfettered right to surreptitiously take documents from the workplace for their own use in litigation or otherwise. Indeed, the Ninth Circuit has rejected the concept of "blanket" protection for whistleblowers for violation of confidentiality agreements and misappropriation of confidential documents. See *Cafasso v. General Dynamics C4 Systems, Inc.*, 637 F.3d 1047 (9th Cir. 2011).

With the likely broader whistleblower protections under the recently enacted DTSA, however, employers that utilize agreements and policies to protect trade secrets and other confidential information should ensure such documents have been updated to comply with the DTSA and its **important employee and whistleblower notification provisions**.



# Trading Secrets



## Introducing Seyfarth's BioLoquitur Blog

*By Seyfarth Shaw LLP (April 7, 2017)*

Seyfarth's Intellectual Property Practice Group is delighted to announce the launch of [BioLoquitur on LexBlog](#). Seyfarth's IP-life sciences attorneys created this blog as a single resource for executives and corporate in-house counsel seeking timely updates on recent developments, trends, tools, best practices, and discussions in the area of intellectual property—patent law, particularly in the life sciences industry.

The BioLoquitur blog offers an all-inclusive assessment of the law regarding life sciences, including issues related to Hatch-Waxman litigation, patentability and patent eligibility, biosimilars, freedom to operate, patent enforcement, America Invents Act (AIA) proceedings, and patent prosecution.

Our team of bloggers have a deep understanding of the biotechnology, chemical, pharmaceutical, and nanotechnology industries. Our attorneys have handled all aspects of life sciences-related intellectual property, including patent litigation, prosecution, due diligence, counseling, and transactions. Our broad technical training, as well as years of legal experience representing clients in court before the United States Patent and Trademark Office as venture capitalists and in-house counsel, allow our attorneys to work closely with clients to not only understand but achieve their technical, business, and legal goals.

If you would like to receive our BioLoquitur blog updates via email as soon as they are published, please [subscribe by clicking here](#).



# Trading Secrets



## **Seyfarth IP, International, Trade Secrets, and Corporate Attorneys to Participate in ITechLaw 2017 World Technology Conference in Chicago**

*By Seyfarth Shaw LLP (April 12, 2017)*

Seyfarth Shaw LLP is pleased to be a Global Sponsor at ITechLaw's 2017 World Technology Conference in Chicago May 3–5.



The Drake Hotel  
140 East Walton Place  
Chicago, IL 60611

ITechLaw is a not-for-profit organization established to inform and educate lawyers about the unique legal issues arising from the evolution, production, marketing, acquisition and use of information and communications technology.

The World Conference will feature a wide-ranging program and invaluable networking opportunities that will focus on cutting-edge legal topics, including e-commerce, e-contracting, disruptive technologies, data protection developments, and the impact of cognitive technologies in the legal spheres.

This year, Seyfarth Shaw Partner Robert B. Milligan is on ITechLaw's Board of Directors and is the Co-Chair of the Local Representative Committee. Seyfarth Shaw Partners Kevin Woolf and Dan Hart and Seyfarth Shaw Legal Project Manager Kyle Hoover will be leading the interactive workshop "Technology Contract-a-thon." The workshop will take participants into the evolving process, labor and software solutions addressing the "more for less" challenge of efficiently handling technology transactions and contract management.

Please stop by our table during the conference to learn about our Intellectual Property, Corporate, Global Privacy & Security and Trade Secrets, Computer Fraud & Non-Competes Practice Groups. Chicago Partners Michael Wexler, Bob Sell, and Marcus Mintz, and Associate Kristine Argentine are scheduled to attend and participate at the conference.

For more information, [click here](#).



## Seyfarth Shaw, AlixPartners, and Directors Roundtable to Present Cyber Risk Management Program in San Francisco

*By Seyfarth Shaw LLP (April 13, 2017)*

Seyfarth Shaw, AlixPartners, and Directors Roundtable invite you to attend [Cyber Risk Management Facing Boards, C-Suites & General Counsel: Prevention, Crisis Management, and Mitigating Personal Liability](#), a program for corporate directors, executive officers and general counsel, focused on approaches and strategies to forensic preservation of electronically stored information, as well as an expert summary of forensic technologies and methodologies used in the field.

The speakers for this program include:

- Kevin J. Lesinski, Seyfarth Shaw
- Richard D. Lutkus, Seyfarth Shaw
- William L. Prickett, Seyfarth Shaw
- Gretchen Ruck, AlixPartners
- David White, AlixPartners
- Steve Martino, Cisco
- Harpreet Ubhi, Lockton Companies
- M. K. Palmore, FBI

The speakers will address key topics, including:

- Cyber Attacks and Defenses
- Governance, Compliance & Disclosure Issues
- Potential Liability to Government and Shareholders
- Litigation Defense and Insurance Coverage
- Prioritizing Risk Management Dollars
- Different Risks for Different Data Types and Industries



# Trading Secrets



- Incidence Response and Planning

The program is Wednesday, May 10 from 8 to 10:30 a.m. at The City Club of San Francisco, 155 Sansome Street.

There is no fee to attend and continental breakfast will be served.

# Trading Secrets



## Trade Secret Protection: What Every California Employer Needs to Know

*By Seyfarth Shaw LLP (April 14, 2017)*

Seyfarth Shaw attorneys Robert Milligan, Jim McNairy, and Scott Atkinson, joined by James Vaughn of iDiscovery Solutions, are presenting a briefing in Los Angeles on May 10 and a briefing in San Francisco on May 17, focused on trade secret protections.

Trade secret identification and protection is more critical than ever for employers in California. Technology is consuming the way we do business, and new laws concerning trade secrets and the content of employment agreements with California employees makes trade secret identification and protection more critical than ever.



We invite you to join our Seyfarth attorneys along with one of California's leading computer forensics experts in an interactive briefing designed to help California employers navigate these tricky waters and provide best practices for trade secret protection.

Topics include:

- How to best identify and protect trade secrets
- What employers need to know about the DTSA
- The impact of new California Labor Code Section 925
- Effective use of restrictive covenants in employment agreements
- How to catch a trade secret thief
- Responses to potential trade secret theft
- Choosing the right court to protect trade secrets
- Considerations for suing under the DTSA vs California law (or both)

# Trading Secrets



## Are My Customer Lists a Trade Secret?

*By Alex Meier & Eric Barton (April 17, 2017)*

A lawyer's favorite phrase might be "it depends." And when an employer asks whether its customer lists qualify as a trade secret, "it depends" is often the answer. But even if it's difficult to definitively state whether customer lists qualify as a trade secret, the converse—whether customer lists might not constitute a trade secret—can be helpful to assessing how much protection a court will provide.



With the advent of the Uniform Trade Secrets Act ("UTSA"), no state categorically denies trade-secrets status to customer lists. That's because the default definition of a "trade secret" under the UTSA includes compilations of information, and several states modified the default definition to explicitly include customer lists as potential trade secrets. See, e.g., Conn Gen. Stat. § 35-51(d); O.C.G.A. § 10-1-761(4); Or. Rev. Stat. § 646.461(4); 12 Pa. Cons. Stat. Ann. § 5302. Other states opted to mention that a "listing of names, addresses, or telephone numbers" may qualify as a trade secret if the listing, like any trade secret, has independent economic value because it is not readily ascertainable and is subject to reasonable efforts to maintain its secrecy. See, e.g., Co. Rev. Stat. Ann. § 7-74-102(4); Oh. Rev. Code Ann. § 1333.61(D).

States still, however, apply varying degrees of scrutiny before conceding that customer lists constitute a trade secret. In more skeptical jurisdictions, courts decline to confer trade-secrets status on customer lists for one of three reasons.

First, many courts will not recognize a "bare bones" list of customer names and addresses as a trade secret. Instead, the expectation is that identity and contact information must be paired with additional, non-public information before the list is considered "not readily ascertainable." For instance, a customer's credit history, buying habits, specific pricing information, or sales volume can significantly bolster the likelihood that a customer list qualifies as a trade secret. Employer-specific information, like costs, project staffing, or profit margin, when included with a customer list, is equally helpful.

A helpful rule of thumb is the five-column rule; if the customer list contains fewer than five discrete categories of information about each customer, then it may not be sufficiently detailed to warrant trade secret protection. In less favorable jurisdictions, the employer may want to combine multiple sources of information into a single document or spreadsheet. By doing so, the employer might bestow trade-secrets protection on information that, on its own, would be considered readily ascertainable.

Second, some jurisdictions do not permit employers to claim that a customer list developed by the departing employee is a trade secret. In those jurisdictions, it's helpful to compile and maintain a centralized customer list or include company information with the customer list so that the list is not exclusively the product of the employee's efforts.



# Trading Secrets



Third, many other courts consider whether customers in that industry are readily identifiable. For example, a court is unlikely to find a list of dry cleaners in a specific area prepared by a company that sells hangers is a trade secret. On the other hand, even a bare customer list might be a trade secret if it takes substantial and significant efforts to identify customers in the first place.

Identifying whether information is a trade secret is not an inquiry guided by bright lines or categorical rules. Still, these three guideposts allow for a quick triage to determine whether a customer list might not qualify as a trade secret. For cases where the answer is “it depends,” we can help. Contact your Seyfarth trade secrets attorney for state-specific guidance on whether your business’ customer list qualifies as a trade secret and how to protect critical business information.



# Trading Secrets



## Don't Forget to Establish Personal Jurisdiction in Defend Trade Secrets Act Cases

By Eric Barton (April 19, 2017)

It is well known that 18 U.S.C. § 1836, et seq. (the Defend Trade Secrets Act or “DTSA”) finally provides a mechanism for pursuing trade secret claims in federal court. A recent decision, however, serves as an excellent reminder that failure to establish personal jurisdiction over a defendant will nevertheless result in dismissal of your DTSA claim—and potentially your entire case. So, before you rush off and file that DTSA claim in your local federal court, carefully consider if it’s really the right court after all.



In *Gold Medal Products Co. v. Bell Flavors and Fragrances, Inc.*, 1:16-CV-00365, 2017 WL 1365798 (S.D. Ohio Apr. 14, 2017), the plaintiff filed suit in the U.S.D.C. for Southern District of Ohio against its former employee, William Sunderhaus, and his new employer, Bell Flavors, alleging misappropriation of trade secrets and confidential information. As part of its lawsuit, Plaintiff asserted a DTSA claim, which Defendants moved to dismiss for lack of personal jurisdiction.

Gold Medal’s lawsuit alleged that Bell Flavors hired Mr. Sunderhaus to work as a “savory flavorist” with knowledge that he had been employed by Gold Medal in Ohio and had acquired Gold Medal’s trade secrets. It further alleged that Bell Flavors directed Mr. Sunderhaus to work on products competitive with Gold Medal’s products.

Despite the fact that Bell Flavors is not an Ohio company, Gold Medal contended that the Ohio court had jurisdiction because its employee, Mr. Sunderhaus, worked for Gold Medal in Ohio, Mr. Sunderhaus obtained Gold Medal’s trade secrets in Ohio, and Bell Flavors instructed Mr. Sunderhaus to use or disclose those trade secrets for its benefit knowing that Gold Medal would suffer tortious injury in Ohio. The Court focused on two particular aspects of Plaintiff’s argument: (1) Gold Medal’s argument that the state in which the plaintiff felt the effects of the tortious conduct is materially relevant to the jurisdiction argument; and (2) Gold Medal’s argument that the conduct of Mr. Sunderhaus in Ohio, before he was Bell Flavors’ agent, is attributable to Bell Flavors.

In its decision, the Court noted that “Gold Medal errs by placing too much emphasis on the fact that Gold Medal felt the effect of Bell Flavors’s allegedly tortious conduct in Ohio. The Supreme Court in *Walden* ‘rejected’ the theory that personal jurisdiction can be based on intentional acts taken outside a forum state which the defendant knows will cause effects inside the forum state.” *Id.* (citing *Maxistrate Tratamento Termico E Controles v. Super Sys., Inc.*, 617 Fed.Appx. 406, 408 (6th Cir. 2015), cert. denied sub nom. *Maxistrate Tratamento Termico E Controles v. Allianz Seguros S.A.*, 136 S. Ct. 336 (2015).) Instead, the court held that “jurisdiction over Bell Flavors must be based on the contacts that ‘defendant [it]self’ creates with Ohio.”

In this situation, the Court found that Bell Flavors had no direct contacts with Ohio giving rise to trade secrets claims. Gold Medal’s Complaint did not allege that Bell Flavors traveled to Ohio to recruit, interview, or hire Mr. Sunderhaus. It also did not allege that Mr. Sunderhaus took actions in Ohio as Bell Flavors’s agent, nor did it allege that Bell Flavors hired Mr. Sunderhaus for the purpose of obtaining Gold Medal’s trade secret information or for the purpose of helping Gold Medal’s competitors



# Trading Secrets



formulate competing food products. Instead, Mr. Sunderhaus acquired the trade secret information in Ohio by legitimate means and only was alleged to have taken wrongful acts outside of the forum state more than one year later.

For all of these reasons, the Court ultimately concluded that it could not exercise personal jurisdiction over Bell Flavors as to the DTSA claim. In so doing, the Court also dismissed the DTSA claim against Mr. Sunderhaus because Gold Medal conceded at oral argument that Bell Flavors was an indispensable party to the claim. Based on this position, the Court held that it could not “in equity or good conscience proceed with [the DTSA claim] against Sunderhaus, even assuming the Court can exercise personal jurisdiction over Sunderhaus.”

## **Take-Away**

Simply asserting a DTSA claim does not guarantee that you will remain in a particular federal court. Always be careful to ensure that personal jurisdiction exists or you will run the risk of having your trade secret case dismissed before it ever gets off the ground.



# Trading Secrets



## Webinar Recap! Simple Measures for Protecting Intellectual Property and Trade Secrets

*By Patrick Muffo & Kevin Mahoney (April 26, 2017)*

Every day, companies unknowingly give up intellectual property and trade secrets which they could have otherwise protected with simple processes. Poor R&D policies may not capture patent rights on a company invention. A faulty or simply outdated employment agreement may not protect a customer list used by an employee who leaves for a competitor. These pitfalls are easily avoidable by implementing measures on the front end and educating employees on the basics of intangible property and how to protect it.

In this [webinar](#), Seyfarth IP and trade secret attorneys provided a basic overview of what types of intellectual property and trade secrets are protectable, how to protect them, and helpful tips to ensure that a company is doing everything they can to avoid common issues associated with intangible property.

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

- Businesses routinely miss out on opportunities to protect their valuable intellectual property simply because they do not realize that their inventions or developments qualified as intellectual property in the first place. Particularly in light of changes in patent law that reward the first party to file for a patent – regardless of whether they invented something first or not – it is important to be proactive about applying for patent protection as early as possible. If a business believes that an invention may qualify for either a design or utility patent, it should take steps to start the patent application process as soon as possible.
- Copyright and trademark protection are also an important, and often overlooked, component of intellectual property protection. Trademarks are routinely granted for patterns, brands, logos, trade dress, and other identifying images which businesses may have thought were too generic to qualify for such protection. Copyrights are also becoming an increasingly important tool in protecting computer code.
- Trade secrets are also intellectual property, but are governed by an entirely different set of laws and are protected in different ways, often through litigation. Because the recently-enacted Defend Trade Secrets Act of 2016 requires the owner of trade secrets to have taken reasonable steps to protect that information, businesses should identify their processes for identifying what information qualifies as a trade secret and what steps they have taken to protect that information, including the implementation of employee confidentiality agreements. Confidentiality agreements drafted before 2016 need to be updated to include certain whistleblower language as a result of the passage of the Defend Trade Secrets Act.

# Trading Secrets



## Enlisting Government Help to Protect Your Trade Secrets

*By Wayne Bond (April 27, 2017)*

"I'm from the government and I'm here to help." Yeah, right.<sup>1</sup>

Most businesses think protecting their intellectual property is their own responsibility, and it is. But what about when your intellectual property rights are violated by an evildoer? Who are you going to call? While your obvious choice will be the law firm sponsoring this blog, you might also be able to get help from your local prosecutor.

Both State Attorneys General and Federal Prosecutors have tools at their disposal that let them bring the full force of the government to your side—when they are motivated to do so. Speaking at a State Fraud & Prevention Summit in Atlanta recently, Georgia Attorney General Chris Carr announced how his office is available to take action on cybersecurity and data breach fraud cases, and he even pointed to several Assistant AGs in the audience who were there and ready to help.<sup>2</sup> Carr said his state's emphasis on protecting data privacy and security is enhanced by the U.S. Army recently announcing that its new Cyber Command Headquarters (ARCYBER) will be located in Georgia.<sup>3</sup> Other states have similarly dedicated AGs ready to help, and sometimes you can even get local prosecutors to take interest in your case.

At the federal level, the Department of Justice (DOJ) has a "Computer Crime and Intellectual Property Section" (CCIPS) specifically devoted to combating white collar computer and intellectual property crimes. Indeed, the DOJ has several statutes at its disposal to combat such crimes. They include the Economic Espionage Act, 18 U.S.C. § 1831, the Theft of Trade Secrets Act, 18 U.S.C. § 1832, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the new Defend Trade Secrets Act of 2016 ("DTSA"). These laws provide punishments that include fines in the millions of dollars (which can be a multiple of the value of trade secrets stolen) and prison sentences ranging from 10–20 years to life under certain circumstances.

Whether or not white collar prosecutors will be motivated to help when your intellectual property is stolen depends on several things. These include the economic value of the loss, the potential value of the IP to the government (e.g., if it has military application), whether the IP was exported to foreign & restricted countries, the method by which the IP was stolen (e.g., by drones or hackers using methods

---

<sup>1</sup> Ronald Reagan is quoted as saying "The most terrifying words in the English language are: I'm from the government and I'm here to help." <https://www.brainyquote.com/quotes/quotes/r/ronaldreag128358.html>.

<sup>2</sup> "Keynote: Protecting Georgians in the Era of Innovation" presentation by Attorney General Christopher M. Carr, April 25, 2017, at SMG Fraud & Data Breach Prevention Summit.

<sup>3</sup> November 16, 2016 Article on U.S. Army web site. See also "Army Cyber Command Announces Augusta's Fort Gordon as New Headquarters, Creating 1,5000 Jobs," Augusta Economic Development Authority.



# Trading Secrets



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

*By J. Scott Humphrey, Dawn Mertineit & Robyn Marsh (May 4, 2017)*

In Seyfarth's second webinar in its series of 2017 Trade Secret Webinars, Seyfarth attorneys Scott Humphrey, Robyn Marsh, and Dawn Mertineit focused on trade secret and client relationship considerations in the banking and financial services industry, with a particular focus on a firm's relationship with its FINRA members. The webinar included practical steps financial institutions can implement to protect trade secrets and client relationships; tips on what to do if your trade secrets are improperly removed or disclosed or if a former employee is violating his/her restrictive covenant agreements; how to prosecute a case against a former employee who is a FINRA member; and the impact of the Protocol for Broker Recruiting on trade secrets and client relationships.



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

- Remember that you can seek court injunctive relief (Temporary Restraining Order and, possibly, Preliminary Injunction) before proceeding in FINRA.
- The definition of a trade secret varies but company, but you must take adequate steps to protect them as a company, and the information cannot be publicly available or easily discovered, to merit enforcement under the law.
- Employers can take steps at all stages to protect their confidential information—don't forget to implement on-boarding and off-boarding procedures, as well as policies and procedures that will be in effect during an employee's tenure, to protect your information before a problem arises.



# Trading Secrets



## Joshua Salinas a Panelist for “Trade Secrets in 2017: Recent Legal Trends and Developments LIVE Webcast”

*By Seyfarth Shaw LLP (May 19, 2017)*

Seyfarth attorney Joshua Salinas will serve on a panel for “Trade Secrets in 2017: Recent Legal Trends and Developments LIVE Webcast,” presented by The Knowledge Group, LLC Live Webcast Series, on May 25, 2017.

Unquestionably, US companies face an increasing threat of cyberattacks from rival companies and foreign governments and the likely targets are trade secrets and other sensitive business information. Since many US companies have overseas operations, the threat of trade secret theft is on the rise which results to billion-dollar intellectual property (IP) theft losses annually.



To address the perceived insufficient legal protection of trade secrets, lawmakers have enacted a series of laws, such as the Economic Espionage Act of 1996 (EEA) and the Defend Trade Secrets Act (DTSA). The US Congress may also support further law and policy efforts aimed at improving trade secret protection. An increase in criminal enforcement efforts is also expected as President Trump indicates the value he gives on IP protection.

In this two-hour LIVE Webcast, a panel of distinguished professionals and thought leaders organized by The Knowledge Group will help businesses and IP counsel understand the recent legal trends and developments in relation to trade secrets. They will provide a comprehensive outlook for the year ahead and will also underscore best practices in protecting trade secrets.

Key topics include:

- Trade Secret: Current Legal Trends and Developments
- Trade Secret Theft
- Trade Secret Protection under the Trump Administration
- Best Practices to Protect Trade Secrets
- Legislative Outlook



# Trading Secrets



## Seyfarth Attorneys to Speak at the Management Association's 2017 Employment Law Conference

*By Seyfarth Shaw LLP (May 22, 2017)*

Join Seyfarth Shaw's Trade Secrets Co-Chair Michael D. Wexler and Partner J. Scott Humphrey at the Management Association's 2017 Employment Law Conference on Thursday, September 28, 2017. Mr. Wexler and Mr. Humphrey will discuss significant developments in Illinois and Congress, such as the Defend Trade Secrets Act, that have changed the landscape of trade secret and restrictive covenant enforcement.

Understanding the impact of these changes, and the tools now available to employers for trade secret and restrictive covenant enforcement and protection, will help

company's safeguard its most valuable assets and maintain its advantage over competitors.



Please join us for a fast-paced and informative discussion that clarifies recent developments in restrictive covenant and trade secrets law, and provides "best practices" for protecting some of your company's most valuable assets—trade secrets, restrictive covenants, and employees.



## Great Employee or Insider Threat?

*By Guest Author for TradeSecretsLaw.com (May 25, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Charlie Platt, a director at iDiscovery Solutions and a Certified Ethical Hacker. He advises clients on data analytics, digital forensics, and cybersecurity.*



At the airport recently, waiting for boarding, flipping through an issue of United States Cybersecurity Magazine, an article about detecting insider threats caught my eye. It was loosely based on a list of behaviors it claimed were ideal indicators for detecting insider threats. I thought, “Wow, this is great! I know plenty of clients who could benefit from this information.” Insider threats are difficult to detect, and I was excited by the opportunity to get new insight, but I became more and more distraught as I read on. The longer I read, the more I saw myself, and many of my cyber-colleagues, being described by the author’s so-called threat indicators. How could we, the good guys, be mistaken for threats?

I read through the list again, and for each point, I asked, “Is this a reliable indicator of a real threat, or a false positive?” I’ve provided the entire list below with my thoughts on each item.

### **Remotely Accesses the Network While on Vacation, Sick or at Odd Hours**

Would a threat actor access the network at odd times? Certainly possible, but an honest, dedicated employee might also check in while on vacation or out sick. I have spent many sick days at home reading through documents. So have my colleagues. Last vacation, I spent evenings after the kids were in bed logged into the network working on a report due shortly after my return. This triggers both “odd times” and “while on vacation,” yet the activities clearly benefited my employer.

### **Works Odd Hours Without Authorization**

This is fairly similar to the prior indicator, so I will focus on the added caveat “without authorization.” I am assuming we are talking about exempt employees here, where extra work does not impact pay or add additional cost to the company. Dedicated employees work when it’s required, which can be at unexpected and unusual times. Work schedules in today’s world are all about flexibility and self-determined priorities. We entrust our employees to make good decisions on our behalf, get work done and accomplish goals. Now we are going to be suspicious when they do so without asking first? That used to be called self-motivated and able to work independently, and it was considered a good quality for employees to exhibit.

### **Notable Enthusiasm for Overtime, Weekend or Unusual Work Schedules**



# Trading Secrets



This essentially says that if you are enthusiastic and ambitious about your career, if you want to be successful and volunteer when needed, you are a threat and need to be watched. Will interest in how your company works outside of your immediate duties also be considered suspect?

## **Interest in Matters Outside of the Scope of Their Duties**

Well, it's not like I didn't know it was coming, but that doesn't make it any less confounding. Don't we want employees to take an interest in the company, grow into new positions and take on more authority? From decades of performance reviews, I can't tell you how often I've been told I will be promoted when I'm doing the job at the level above me.

## **Unnecessarily Copies Material**

I agree this one could go either way. A lot of data access and movement to local devices can be a true indicator of theft of IP and exfiltration, and it should be monitored. Despite that, it may also indicate an employee who is researching projects and building a local knowledge base for valid company use.

I personally have extensive local (encrypted) stores of data from past projects that I use regularly for reference and as templates on current projects. A software developer who doesn't have a "library" of code for reuse, or a consultant who doesn't keep prior reports for future reference? They may exist, but I haven't met one.

Ultimately, there is a larger problem at play here. This list is based on an industrial-age mentality, but we are fighting an information-age war. And we're failing. We need to start thinking about cyber with an information-age mentality. Our employees are highly educated, invested and dedicated to the success of our organizations. We want to encourage this behavior, not inhibit it. K



## Robert Milligan to Present “Trade Secret Mediations in 2017: What You Need to Know” Webinar

*By Seyfarth Shaw LLP (May 26, 2017)*

Robert Milligan, Seyfarth Partner and Co-Chair of the Trade Secrets, Computer Fraud & Non-Competes Practice Group, will be a panelist for the “Trade Secret Mediations in 2017: What You Need to Know” webinar presented by The Knowledge Group, LLC Live Webcast Series on July 14, 2017.

In most intellectual property cases, particularly in trade secret disputes, mediation can be a highly effective mechanism to resolve conflicts early on. It can enable things that are not possible in court, such as private caucuses between a mediator and each party involved where private resolution of the issue can be offered.



Companies seeking mediation should first know their actual trade secrets and how to protect it. With the help of an experienced mediator, both parties can be able to identify the strengths and weaknesses of the case, and the requirements and risks of proving and disproving trade secret claims.

In this live Webcast, a panel of distinguished professionals and thought leaders organized by The Knowledge Group will help the audience understand the fundamentals of trade secret mediations. They will discuss how to leverage mediation for resolving trade secret disputes and avoid costly, slow and uncertain judicial process.

Key Topics Include:

- Mediating Trade Secret Disputes
- Confidentiality, Counsel and Mediator Ethics
- Selecting a Mediator
- The Role of Counsel in Mediation
- Preparing for a Mediation Session
- Drafting and Enforcing a Settlement Agreement

# Trading Secrets



## Seyfarth's Trade Secrets Group Earns Top Tier Ranking from Legal 500 Second Year in Row

*By Seyfarth Shaw LLP (June 8, 2017)*

The 2017 edition of *The Legal 500 United States* recommends Seyfarth Shaw's Trade Secrets group as one of the best in the country. Nationally, for the second consecutive year, our Trade Secrets practice earned Top Tier.

Based on feedback from corporate counsel, Seyfarth partner [Michael D. Wexler](#) was ranked in the editorial's "Leading Lawyers," and [Katherine E. Perrelli](#), [Robert B. Milligan](#), [Daniel P. Hart](#), [Erik W. Weibust](#), and [J. Scott Humphrey](#) were recommended in the [editorial](#).

*The Legal 500 United States* is an independent guide providing comprehensive coverage on legal services and is widely referenced for its definitive judgment of law firm capabilities. *The Legal 500 United States Awards 2017* is a new concept in recognizing and rewarding the best in-house and private practice teams and individuals over the past 12 months. The awards are given to the elite legal practitioners, based on comprehensive research into the U.S. legal market.



# Trading Secrets



## Trade Secrets May Retain Protections Despite Disclosure to Single Competitor

By Daniel Joshua Salinas & Sierra J. Chinn-Liu (June 9, 2017)

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



The trade secret at issue in *United States v. Liew* concerned methods of producing titanium dioxide (TiO<sub>2</sub>), a white pigment found in anything from paint to Oreo creme, which makes its manufacture a (surprisingly) competitive industry. DuPont has been a leader in TiO<sub>2</sub> production since the 1940s, when it became more efficient to produce TiO<sub>2</sub> through a chloride-based process. DuPont opened chloride plants around the US, including one in Antioch, California and one in Ashtabula, Ohio. The Ashtabula plant was built for Sherwin-Williams, subject to a fifteen-year confidentiality agreement effective through the plant’s sale in the 1970s. The plant was sold multiple times thereafter and was ultimately acquired by a competitor of DuPont who was not bound by any nondisclosure or confidentiality obligations to the company.

DuPont improved its TiO<sub>2</sub> manufacturing process and began incorporating the newer technology into new plants, including a facility in Taiwan. Unlike the Antioch and Ashtabula plants, the new Kuan Yin plant was equipped to extract titanium from lower-grade ore, making DuPont’s the most competitive chloride process.

The Chinese government sought to license DuPont’s TiO<sub>2</sub> technology but ultimately chose a more cost-effective molten-salt option from the former Soviet Union. The Chinese government then tasked Walter Liew, a businessman and US citizen, with bringing chloride TiO<sub>2</sub> production to China. Liew hired two former DuPont employees with TiO<sub>2</sub> experience and with their help, went about securing business, which eventually brought them to their various convictions under the EEA. Liew and the other defendants appealed their convictions to the Ninth Circuit.

One of the defendants’ many arguments on appeal was that the technology at issue was not trade secret material because DuPont sold the Ashtabula plant and, thus, did not take reasonable measures to guard its technology. According to the defendants’ interpretation of *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984), any disclosure of material to any recipient not bound to maintain secrecy destroys trade secret protection, and it was on the government to prove no disclosures ever occurred. The Court rejected defendants’ arguments.

The Ninth Circuit explained that there was no clear or controlling authority addressing whether disclosure to one competitor makes information “generally known” or “readily ascertainable” by “the public” under the EEA’s then-definition of trade secrets.



# Trading Secrets



The Court further stated that the government was not required to prove no disclosures of DuPont's technology occurred; only that DuPont took reasonable measures to guard its technology. The Court found DuPont's selectiveness in employing contractors and use of confidentiality agreements to be reasonable measures. The sale of a plant or information in a recipient or competitor's hands is not the end of the reasonable measures inquiry, particularly if the information disclosed is not part of the trade secret(s) at issue.

This case is significant because it illustrates one of the DTSA's substantial changes to the EEA—the definition of a trade secret. Before the DTSA, trade secrets were defined under the EEA to include information that was subject to reasonable secrecy measures and “derive[d] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.” The Court in *Liew* highlighted that there was no controlling authority holding that the disclosure of a trade secret to a single competitor meant that it was also generally known by “the public.”

The DTSA now defines a trade secrets to include information that was subject to reasonable secrecy measures and “that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use....” It is arguable that the result in this case may have been different under the DTSA's new definition of trade secrets. Specifically, the disclosure of the trade secret to DuPont's competitor may have made it generally known “by other persons who might obtain economic value” from it.

This case also reminds businesses about the potential risks to trade secrets when selling business assets. Building facilities, electronic devices, and any other equipment sold should be vetted to ensure no valuable company information is inadvertently disclosed.





## Court Allows Plaintiff to Amend Complaint to Add Defend Trade Secrets Act Claim After Discovery Reveals Alleged Continued Misappropriation

*By Daniel Joshua Salinas & Lauren Leibovitch (June 12, 2017)*

A Northern District of California court recently held a plaintiff could amend its complaint to add a Defend Trade Secrets Act (“DTSA”) claim when discovery showed continued misappropriation after the enactment of the DTSA on May 11, 2016.

In *VIA Technologies, Inc. v. ASUS Computer International*, No. 14-CV-03586-BLF, 2017 WL 491172 (N.D. Cal. Feb. 7, 2017), VIA filed suit against ASUS, alleging infringement of VIA’s patent and trade secret misappropriation of VIA’s intellectual property related to its USB technology. VIA’s second amended complaint was filed in July 2015 prior to the enactment of the DTSA on May 11, 2016.



During discovery, ASUS produced data related to sales of products that allegedly incorporated VIA’s trade secrets. This data was produced in supplemental productions on November 16, 2016, and on December 22, 2016. VIA claims this data supports the alleged continuation of trade secret misappropriation after the enactment of the DTSA, and therefore, requests to add the claim. VIA claims it also inadvertently overlooked the sales data believing the November 16, 2016, production was merely a “re-production.” VIA filed the instant motion on January 4, 2017, after ASUS refused to stipulate to an amendment to add a claim under DTSA.

After weighing the factors, the Northern District Court granted VIA’s motion for leave to file a third amended complaint. The Court rejected ASUS’s contention that the request to add the DTSA claim should have been six weeks after the November production, and that VIA acted in bad faith when it met and conferred during the holiday period and then filed the instant motion during the expert rebuttal period. The Court held that there was neither undue delay nor bad faith present, and while VIA could have raised the issue in November, the additional four weeks did not cause undue delay. Moreover, the Court explained that VIA understood the November production to be a “re-production,” and met and conferred with ASUS promptly after finding relevant data in the December production.

The Court continued that, ASUS failed to bear its burden of showing prejudice. The Court explained ASUS’s argument that the differences between the CUTSA and the DTSA would require additional discovery was undercut by ASUS’s failure to identify the specific additional discovery and the additional amount of time that would be needed for the additional DTSA claim, and ASUS’s admission that “VIA would be seeking the same relief that it’s currently seeking under the CUTSA, under the same set of facts.”

Finally, the Court reasoned that the proposed DTSA claim was not futile. As VIA explained, the DTSA was enacted on May 11, 2016, and the facts supporting continued trade secret misappropriation were not made available to VIA until November 2016 during discovery.



# Trading Secrets



Continued misappropriation has become of the rising legal developments with DTSA claims, particularly where defendants argue that the DTSA does not apply because the alleged trade secret theft occurred before the enactment of the DTSA.

Yet similar to the holding in *VIA Technologies*, federal district courts in multiple jurisdictions have allowed plaintiffs to proceed with DTSA claims, at least partially, when the plaintiffs can sufficiently alleged that any wrongful misappropriation occurred after the date of the enactment of the DTSA. See, e.g., *Adams Arms, LLC v. Unified Weapons Sys.*, No. 16-cv-01503, 2016 WL 5391394, (M.D. Fla. Sep. 27, 2016); *Syntel Sterling Best Shores Mauritius Ltd v. Trizetto Group, Inc.*, Case No. 15-CV-211 (S.D.N.Y. Sept. 23, 2016) (“as Defendants allege that Syntel continues to use its Intellectual Property to directly compete with Trizetto, the wrongful act continues to occur after the date of the enactment of DTSA”). But see *Avago Techs. United States Inc. v. NanoPrecision Products*, No. 16-cv-03737, 2017 U.S. Dist. LEXIS 13484 (N.D. Cal. Jan. 31, 2017) (dismissing DTSA claim because alleged trade secrets were disclosed before the DTSA came into effect).

Thus, DTSA claimants should ensure they sufficiently allege acts of misappropriation occurring after the DTSA’s May 11, 2017, enactment date to increase the likelihood of surviving early pleading challenges.



## Briefing Recap! Trade Secret Protection: What Every California Employer Needs to Know

*By Daniel Joshua Salinas, Scott E. Atkinson & Robert B. Milligan (June 14, 2017)*

In a series of breakfast briefings, Seyfarth attorneys Robert Milligan, Joshua Salinas, and Scott Atkinson, joined by Jim Vaughn, one of California's leading computer forensic experts, discussed how to navigate the tricky waters and provided best practices for trade secret protection. The briefings covered how to best identify and protect trade secrets, what employers need to know about the DTSA, the impact of new California Labor Code Section 925, how to catch a trade secret thief, and more. [Click here](#) to see the slides from the briefings.



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

- Employers should continue to use caution when using non-California forum selection clauses and choice of law provisions in agreements that are “conditions of employment” with California employees. Attempting to enforce such provisions may not only result in litigation, but may also result in the employer being on the hook for the employee’s attorney’s fees under California Labor Code section 925.
- Employers should update nondisclosure agreements and company policies to include language reference to the Defend Trade Secrets Act whistleblower provisions.
- Employers should remember that mobile devices can be configured differently, and depending on how they allowed them to be configured, can be problematic post departure of the employee. Corporate partitions, company iTunes accounts, and mobile device management systems are all options to consider.

# Trading Secrets



## Emerging Issues In the Defend Trade Secrets Act's Second Year

By Robert B. Milligan & Daniel Joshua Salinas (June 14, 2017)

This blog originally appeared in ALM Intellectual Property Strategist.

One year after its enactment, the Defend Trade Secrets Act (DTSA) continues to be one of the most significant and closely followed developments in trade secret law. The statute provides for a federal civil cause of action for trade secret theft, protections for whistleblowers, and new remedies (e.g., *ex parte* seizure of property), that were not previously available under state trade secret laws. The less than 70 reported DTSA cases to date provide an early glimpse into how courts may interpret the statute going forward and what early concerns about the statute may have been exaggerated.



### Overstated *Ex Parte* Seizure Concerns

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

To curtail potential abuse, the DTSA requires stringent proof of the necessity and propriety of a civil seizure. For example, the DTSA prohibits copying seized property and requires that *ex parte* orders provide specific instructions for federal marshals 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, such as a preliminary injunction, are inadequate.

The DTSA cases to date involving *ex parte* seizure requests reflect that courts are treating the remedy as intended—only in extraordinary circumstances. For example, a federal district court in the Eastern District of Michigan denied an *ex parte* seizure request because the court was not “persuaded that there has been a showing that the defendants would not comply with an order [] issued by way of an injunction under Rule 65.” See, *Dazzle Software II, LLC v. Kinney*, No. 2:16-cv-12191-MFL-MLM (E.D. Mich. 2016). Other courts have applied similar reasoning in denying such requests. See, e.g., *OOO Brunswick Rail Mgt. v. Sultanov*, No. 5:17-cv-00017-EJD, 2017 WL 67119 (N.D. Cal. Jan. 6, 2017) (finding seizure under the DTSA unnecessary and instead ordering the defendant to preserve and deliver the electronic devices at issue).

Courts have also denied *ex parte* seizure requests where the plaintiff fails to substantiate its claims that *ex parte* seizure is needed to avoid the destruction of evidence. See, *Balearia Caribbean Ltd. Corp. v.*



# Trading Secrets



*Calvo*, No. 1:16-cv-23300-KMV (S.D. Fla. Aug. 5, 2016) (“a plaintiff may not rely on bare assertions that the defendant, if given notice, would destroy relevant evidence”).

Nonetheless, a few courts have ordered the *ex parte* seizure of property in DTSA cases. For example, the court in *Mission Capital Advisors, LLC v. Romaka*, No. 1:16-cv-05878-LLS (S.D.N.Y. July 29, 2016) ordered the U.S. Marshall to seize the defendant’s computer at his residence and then copy and delete the plaintiff’s trade secret files at issue. Notably, the court issued its seizure order only after the defendant had purportedly ignored the court’s initial TRO (which did not order the seizure of property) and order to show cause.

Other courts that have ordered the seizure of property in DTSA cases, however, have relied on Federal Rule of Civil Procedure 65 (i.e., Injunctions and Restraining Orders) to authorize the seizure instead of the DTSA. See, e.g., *Earthbound Corporation v. MiTek USA, Inc.*, C16-1150 RSM, 2016 WL 4418013, at 11 (W.D. Wash. Aug. 19, 2016) (granting a TRO requiring defendants to turn over to a neutral third-party expert all flash drives, SD cards, cell phones, and other external devices for forensic imaging); *Panera, LLC v. Nettles*, 4:16cv1181-JAR, 2016 WL 4124114, at 2-4 (E.D. Mo. Aug. 3, 2016) (granting a TRO requiring defendant to turn over his personal laptop and any other materials that may have housed plaintiff’s materials for review and inspection). See also, *Magnesita Refractories Co. v. Mishra*, 2:16-cv-524, 2017 WL 365619, 2 (N.D. Ill. Jan. 25, 2017) (“[*Earthbound*] and [*Panera*] had no problem relying on a Rule 65 temporary restraining order, rather than the DTSA, to accomplish the seizure.”).

We expect the federal district courts to continue the trend in awarding *ex parte* seizure orders only in extraordinary, emergency, and substantiated circumstances.

## Determining the Timeliness Of DTSA Claims

A rising development with the DTSA concerns its application to misappropriation that occurs both before and after the statute’s May 11, 2016, effective date. The decision in *Adams Arms, LLC v. Unified Weapons Sys.*, No. 16-cv-01503, 2016 WL 5391394 (M.D. Fla. Sep. 27, 2016) best illustrates this issue.

The plaintiff in *Adams Arms* alleged that the defendant mislead it in 2014 about defendant’s intent to enter into a commercial relationship in order to induce the plaintiff to disclose trade secrets. The plaintiff further alleged that that defendant wrongfully disclosed and used the plaintiff’s trade secrets on and after May 16, 2016, to enter into and exclude plaintiff from a purchasing contract with a third party.

The defendant in *Adams Arms* moved to dismiss the plaintiff’s DTSA claim on the ground that the alleged misappropriation occurred before the enactment of the statute. The defendant explained that the DTSA has a three year statute of limitations and contains language that provides: “[f]or purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation.” 18 U.S.C. 1836(d). In other words, the defendant argued that any alleged acts of continuing misappropriation should be measured at the time of the initial misappropriation, which in this case occurred before the DTSA’s enactment.

The court rejected the defendant’s argument. The court highlighted: “Section 2(e) specifies that [the] DTSA applies to ‘any misappropriation ... for which any act occurs’ after the effective date.” *Adams Arms*, 2016 WL 5391394, at 6. Thus, the court found that plaintiff had sufficiently alleged a claim for relief based on the unlawful disclosure of trade secrets after the DTSA’s effective date. Notably, the court limited plaintiff’s DTSA claim to a disclosure theory as the Complaint’s allegations and inferences reflected that any unlawful acquisition of trade secrets occurred well before the DTSA’s effective date.



# Trading Secrets



Other courts have adopted Adams Arms' reasoning and allowed plaintiffs to proceed with DTSA claims, at least partially, when the plaintiffs can sufficiently allege that any wrongful misappropriation occurred after the date of the enactment of the DTSA. See, e.g., *Syntel Sterling Best Shores Mauritius Ltd v. Trizetto Group, Inc.*, Case No. 15-CV-211 (S.D.N.Y. Sept. 23, 2016) ("as Defendants allege that Syntel continues to use its Intellectual Property to directly compete with Trizetto, the wrongful act continues to occur after the date of the enactment of DTSA"). But see, *Avago Techs. United States Inc. v. NanoPrecision Products*, No. 16-cv-03737, 2017 U.S. Dist. LEXIS 13484 (N.D. Cal. Jan. 31, 2017) (dismissing DTSA claim because alleged trade secrets were disclosed before the DTSA came into effect); (dismissing DTSA claim because "plaintiff makes no specific allegations that defendant used the alleged trade secrets after the DTSA's May 11, 2016, enactment").

Accordingly, DTSA claimants should ensure they sufficiently allege acts of misappropriation occurring after the DTSA's enactment date to increase the likelihood of surviving early pleading challenges.

## Federal Courts Turning to State Courts for Guidance

Another emerging issue with the DTSA is whether it is fostering its underlying goals of uniformity in trade secret law. In enacting the DTSA, Congress sought to create a uniform standard for trade secret misappropriation, harmonize the differences in trade secret law under the UTSA, and provide uniform discovery.

Because the DTSA does not preempt state laws, trade secret plaintiffs have the option to plead claims under both federal and state laws. Federal district courts that are tasked with analyzing such claims simultaneously are finding similarities between the federal and state statutes, such as the definitions of trade secrets, improper use, or misappropriation. With an often abundance of state decisions addressing these similarities under their respective form of the UTSA, federal courts have turned to these state court decisions for guidance on interpreting the DTSA. See, e.g., *Kuryakyn Holdings, LLC v. Ciro, LLC*, No. 15-cv-703-jdp, 2017 WL 1026025, at 5 (W.D. Wisc. Mar. 15, 2017) ("the court's analysis will use Wisconsin's UTSA, but the analysis would apply as well to the DTSA."); *Henry Schein v. Cook*, No. 16-cv-03166-JST, 2016 WL 3418537 (N.D. Cal. June 22, 2016) (applying California law in its DTSA analysis).

To the extent federal courts continue to look at their respective state courts' decisions for guidance in interpreting the DTSA, the DTSA may ultimately duplicate and amplify the already existing patchwork of differences in state trade secret laws.

## Whistleblower Immunity Remains Largely Untested

One of the unique provisions of the DTSA is that it 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." One of the early concerns with this whistleblower immunity provision is that employees who have wrongfully misappropriated trade secrets and other confidential information may use it as an after-the-fact defense. For example, an employee accused of trade secret misappropriation may later attempt to disclose the trade secret information to an attorney or government official solely to invoke the DTSA's whistleblower protections and not for true whistleblowing.

After one year, the whistleblower immunity provisions remain largely untested. Only one published decision has addressed this immunity provision, which the court characterized as an affirmative defense and declined to rule on the merits of the defense—at least at the pleading stage—before



# Trading Secrets



discovery and the presentation of evidence. See, *Unum Group v. Loftus*, No. 4:16-CV-40154-TSH, 2016 WL 7115967 (D. Mass. Dec. 6, 2016).

Employers should also be mindful that the DTSA places an affirmative duty on them to provide employees notice of the whistleblower immunity provision in “any contract or agreement with an employee that governs the use of a trade secret or other confidential information.” Employers that fail to comply with this disclosure requirement are precluded from recovering attorneys’ fees or exemplary damages under the DTSA.

We expect the whistleblower immunity provision to be a closely followed topic in the DTSA’s second year.

## Conclusion

The most significant takeaway after a year of the DTSA is that it provides trade secret holders with a new option in pursuing their claims. Trade secret holders have an additional mechanism to get their case into federal court and newly available remedies, but also an affirmative obligation to notify employees of the whistleblower immunity provision. Nonetheless, it is yet to be seen whether federal courts will become the overwhelmingly favorite forum for trade secret litigation.

*Reprinted with permission from the June 2017 issue of The Intellectual Property Strategist. © 2017 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved.*





## Illinois Federal Court Allows Inevitable Disclosure Theory in Defend Trade Secrets Act Case

*By Kyla Vick & J. Scott Humphrey (June 28, 2017)*

On May 11, 2017, a [Northern District of Illinois federal court](#) ruled that a Plaintiff properly alleged misappropriation under both the federal Defend Trade Secrets Act (DTSA) and the Illinois Trade Secrets Act (ITSA) in a [case](#) where the employee downloaded files onto a personal thumb drive and then went to a competitor.



Plaintiff Molon Motor and Coil Corporation (“Molon”) contended that its former Head of Quality Control, Manish Desai, downloaded confidential data onto a portable data drive before leaving Molon for a competitor, Nidec Motor Corporation (“Nidec”). Molon further contended that Desai provided the confidential data to Nidec and Nidec then used (and continues to use) the confidential data to compete with Molon. Nidec filed a Motion to Dismiss Molon’s Complaint against Nidec (Molon did not sue Desai) on the basis that Molon could not state a claim under the DTSA or the ITSA because a) Desai downloaded the trade secrets while still employed by Molon, and b) Molon did not make a plausible allegation that Nidec used the trade secrets.

Specifically, Nidec argued that because Desai downloaded the files while still employed by Molon, Desai did not “misappropriate” the trade secrets for purposes of the DTSA and ITSA. Molon countered by citing the definitions of “misappropriation” and “improper means” from the trade secret statutes, which state that “misappropriation” is “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means”. The statutes further state that “improper means” includes “breach or inducement of a breach of a duty to maintain secrecy”. Molon argued that Desai’s actions of downloading files while still employed by Molon qualified as a breach of a duty to maintain secrecy. The Court agreed with Molon, and in doing so, found that a confidential relationship and duty to maintain secrecy was established by Desai’s employment agreement with Molon.

The Court also gave Molon some wiggle room by allowing Molon to use the “inevitable disclosure” doctrine to show that Nidec possesses, and is using, Molon’s trade secrets. Under the inevitable disclosure doctrine, a plaintiff can “prove a claim of trade secret misappropriation by demonstrating that defendant’s new employment will inevitably lead him to rely on the plaintiff’s trade secrets.” *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995). Here, the Court found that Molon’s Complaint should survive a Motion to Dismiss because, at the pleading stage, it is enough for a plaintiff/Molon to allege, “based upon information and belief,” that a competitor is using the trade secrets stolen by a former employee.

However, the Court also emphasized that “Molon will ultimately bear the burden of proving—not just alleging—enough facts such that disclosure is not premised on a mere unsubstantiated fear.” In other words, Molon has won a battle, not the war; and Molon now has to show (presumably through discovery) that Nidec did, in fact, receive Molon’s trade secrets if Molon is to ultimately prevail in this litigation.

# Trading Secrets



## Webinar Recap! Protecting Your Trade Secrets in the Pharmaceutical Industry

*By Justin K. Beyer, Marcus Mintz, Dean L. Fanelli, Ph.D. & Thomas A. Haag, Ph.D.  
(July 5, 2017)*

In Seyfarth's third webinar in its series of 2017 Trade Secrets Webinars, Seyfarth attorneys Justin Beyer, Marcus Mintz, Dean Fanelli, and Thomas Haag focused on how to define and protect trade secrets in the pharmaceutical industry, including: reviewing significant civil and criminal cases in the industry, discussing how federal and state trade secret statutes and decisions may impact the protection of trade secrets, and suggested best practices for protecting trade secrets from invention through sale.



As a conclusion to this well-received [webinar](#), we compiled a summary of takeaways:

- Trade secret laws cover any information which is confidential, kept confidential, and from which the owner derives economic benefit. In order to maintain such protections, owners must be vigilant and proactive about maintaining the secrecy of their trade secret information. One of the ways in which employers should do so is to update their employment agreements to comply with the immunity notice provisions of the Defend Trade Secrets Act, without which the employer may lose the ability to recover attorney's fees or double damage awards.
- In the pharmaceutical and biotechnology space, companies should also take active steps to develop internal guidelines and protocols for the identification and protections of information that may be the subject of trade secret protection, whether that information is related to research and development, strategic business plans, or future opportunities and trends. These steps include, but are not limited to: (i) advising all employees of the confidential and proprietary nature of their work; (ii) limiting access to proprietary and confidential information to only those employees requiring such information; (iii) actively monitoring how information is distributed both internally and externally; and (iv) regularly updating employees of the necessity to maintain confidentiality of all information.
- Trade secrets are particularly valuable with respect to the development of biologics. Given long clinical development timelines, composition patents covering reference biologics may be about to expire or will have already expired, at time of marketing approval. Confidential and proprietary details relating to reference protein drug production, isolation, storage and delivery; as well as its post-transnational modifications, are at least as important to know as the identity of the reference protein's amino acid sequence, when creating a biosimilar. Thus these trade secrets represent potentially enormous barriers to market entry for third party developers of biosimilar versions. They should, therefore, be kept in the strictest confidence.

# Trading Secrets



- If a company does, however, find itself in a situation in which it fears that an employee has or may misappropriate its trade secret information, it should take certain immediate steps, including: (a) reminding the employee of his/her obligations; (b) forensically imaging and reviewing the employee's email communications, downloading history, and/or internet activity; (c) cutting off the employee's access to company confidential information, as soon as notice is provided that the employee is taking a position with a competitor; and (d) if necessary, filing suit to recover and protect the secrecy of the trade secrets. Once trade secrets are disclosed in public, whether properly or improperly, it becomes exceedingly difficult to prove the ongoing secrecy of the information and even harder to put the secret back in its box.



## California Federal Court Finds CUTSA Preemption on Unfair Competition Claim in Uber Row

*By Robert B. Milligan & Sierra J. Chinn-Liu (July 7, 2017)*

The Defend Trade Secrets Act (DTSA) states very clearly that an injunction issued pursuant thereto may not “prevent a person from entering into an employment relationship,” and that any conditions placed on a former employee’s employment in an injunction must be based on “evidence of threatened misappropriation *and not merely on the information the person knows.*” (Emphasis added). This language appears to bar injunctive relief under the DTSA based on the “inevitable disclosure doctrine,” which in some states permits a court to enjoin a former employee from working for a competitor—even in the absence of a signed non-compete agreement—if it can be established that the employee would “inevitably” (even if inadvertently) use his or her former employer’s trade secrets on behalf of a new employer. As a result, when the statute was first enacted, many commentators assumed that claims based on the inevitable disclosure doctrine would quickly be shot down. In practice, however, that does not appear to be the case. At the very least, some recent federal court decisions have sown confusion around this issue.



We recently [wrote](#) about a federal court’s ruling in the Northern District of Illinois that applied the inevitable disclosure doctrine to a DTSA claim. Despite its non-precedential value, this ruling was significant because it interpreted a federal law to allow the application of a doctrine that has been expressly rejected in several states, including California, Maryland, and Virginia, and, again, appears to be barred by the plain language of the DTSA. That case can perhaps be explained by the fact that it was decided on a motion to dismiss, not a motion for injunctive relief, and thus the DTSA’s apparent prohibition on basing an injunction on inevitable disclosure was not necessarily implicated. The same cannot be said about a decision that was issued just three weeks later by the United States Court of Appeals for the Third Circuit, in which the Court applied the inevitable disclosure doctrine in the context of a temporary restraining order. The case is *Fres-co Systems USA, Inc. v. Hawkins*, 2017 WL 2376568 (3rd Cir. June 1, 2017).

In 2016, Kevin Hawkins notified his employer, Fres-co Systems, that he was resigning from his position as a sales representative to work for a direct competitor of Fres-co, Transcontinental Ultra Flex, Inc. He also informed Fres-co that not only will he be working for a direct competitor, but he will be selling a competing product as well. When Fres-co reminded Hawkins of his one-year non-compete and non-solicitation agreement, he refused to confirm that he would not solicit Fres-co customers with whom he had worked while at Fres-co, and would not commit to honoring the terms of his agreement.

Fres-co then filed suit against Hawkins and joined Transcontinental, alleging, among other things, misappropriation of trade secrets under the DTSA and the Pennsylvania Uniform Trade Secrets Act. Fres-co moved for a Temporary Restraining Order to enforce Hawkins’s non-solicitation provision and to prevent the disclosure of any of its trade secrets. Fres-co claimed that Hawkins’s position gave him access to confidential information, including “customer lists, price lists, and marketing and sales strategies.” Hawkins opposed the motion and attached an affidavit in which he denied awareness of



# Trading Secrets



any Fres-co trade secrets and represented that he would not disclose or use any confidential information that he learned at Fres-co while working for Transcontinental.

The district court issued a TRO, observing that neither Hawkins nor Transcontinental would confirm that Hawkins would not “solicit, contact, or communicate with Hawkins’s former Fres-co clients[ ]” and accordingly determined Hawkins would “begin work as a sales representative, the position he occupied while at Fres-co, and be assigned to solicit his former clients.” Notably, the court also held that given his position, Hawkins would “likely use his specialized and confidential knowledge to the detriment of Fres-co.... and Hawkins’s interference with Fres-co’s client relationships would cause immediate irreparable harm to Fres-co.”

Hawkins and Transcontinental appealed to the Third Circuit. The appellate court remanded the case back to the district court because it failed to address three of the four requisite elements for injunctive relief. In so doing, however, the court made an interesting observation in its discussion of the irreparable harm element. Without actually referring to the inevitable disclosure doctrine by name, the court recognized that under the Pennsylvania Uniform Trade Secrets Act and the DTSA, “misappropriation of trade secrets need not have already occurred to warrant injunctive relief; threatened misappropriation is sufficient.” This is not in and of itself a controversial statement, as the DTSA does permit injunctions to be issued based on “threatened misappropriation” (so long as it is not based “merely on the information the person knows”). Citing the lead opinion from the Circuit that applied the inevitable disclosure doctrine to Pennsylvania law (*Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 114 (3d Cir. 2010)), the Third Circuit agreed with the district court, and appeared to apply the doctrine in the context of Fres-co’s DTSA claim: “Given the substantial overlap (if not identity) between Hawkins’s work for Fres-co and his intended work for Transcontinental—same role, same industry, and same geographic region—the District Court was well within its discretion to conclude Hawkins *would likely use his confidential knowledge to Fres-co’s detriment.*” (Emphasis added).

The Third Circuit was not clear whether its application of the inevitable disclosure doctrine was based solely on the Pennsylvania Uniform Trade Secrets Act, as opposed to the DTSA, although it appears to have been based on both. This could create confusion in states in which the inevitable disclosure doctrine is not permitted by state law (e.g., California, Maryland, and Virginia).

Nevertheless, the Third Circuit’s application of the inevitable disclosure doctrine in a decision addressing the DTSA is the second opinion in less than a month to do so. If other federal courts follow, we could see the spread of the doctrine across the country and into jurisdictions that have expressly banned its application at the state level. Only time will tell whether this trend will continue, or if the federal courts will clarify what the DTSA seems to provide in its plain language: that injunctions keeping a former employee out of work may not be based on their alleged “inevitable disclosure” of trade secrets.



# Trading Secrets



## The Third Circuit Addresses the Defend Trade Secrets Act and Appears to Have Applied the Inevitable Disclosure Doctrine

*By Erik Weibust & Andrew Stark (July 11, 2017)*

The Defend Trade Secrets Act (DTSA) states very clearly that an injunction issued pursuant thereto may not “prevent a person from entering into an employment relationship,” and that any conditions placed on a former employee’s employment in an injunction must be based on “evidence of threatened misappropriation and not merely on the information the person knows.” (Emphasis added). This language appears to bar injunctive relief under the DTSA based on the “inevitable disclosure doctrine,” which in some states permits a court to enjoin a former employee from working for a competitor—even in the absence of a signed non-compete agreement—if it can be established that the employee would “inevitably” (even if inadvertently) use his or her former employer’s trade secrets on behalf of a new employer. As a result, when the statute was first enacted, many commentators assumed that claims based on the inevitable disclosure doctrine would quickly be shot down. In practice, however, that does not appear to be the case. At the very least, some recent federal court decisions have sown confusion around this issue.



We recently [wrote](#) about a federal court’s ruling in the Northern District of Illinois that applied the inevitable disclosure doctrine to a DTSA claim. Despite its non-precedential value, this ruling was significant because it interpreted a federal law to allow the application of a doctrine that has been expressly rejected in several states, including California, Maryland, and Virginia, and, again, appears to be barred by the plain language of the DTSA. That case can perhaps be explained by the fact that it was decided on a motion to dismiss, not a motion for injunctive relief, and thus the DTSA’s apparent prohibition on basing an injunction on inevitable disclosure was not necessarily implicated. The same cannot be said about a decision that was issued just three weeks later by the United States Court of Appeals for the Third Circuit, in which the Court applied the inevitable disclosure doctrine in the context of a temporary restraining order. The case is *Fres-co Systems USA, Inc. v. Hawkins*, 2017 WL 2376568 (3rd Cir. June 1, 2017).

In 2016, Kevin Hawkins notified his employer, Fres-co Systems, that he was resigning from his position as a sales representative to work for a direct competitor of Fres-co, Transcontinental Ultra Flex, Inc. He also informed Fres-co that not only will he be working for a direct competitor, but he will be selling a competing product as well. When Fres-co reminded Hawkins of his one-year non-compete and non-solicitation agreement, he refused to confirm that he would not solicit Fres-co customers with whom he had worked while at Fres-co, and would not commit to honoring the terms of his agreement.

# Trading Secrets



Fres-co then filed suit against Hawkins and joined Transcontinental, alleging, among other things, misappropriation of trade secrets under the DTSA and the Pennsylvania Uniform Trade Secrets Act. Fres-co moved for a Temporary Restraining Order to enforce Hawkins's non-solicitation provision and to prevent the disclosure of any of its trade secrets. Fres-co claimed that Hawkins's position gave him access to confidential information, including "customer lists, price lists, and marketing and sales strategies." Hawkins opposed the motion and attached an affidavit in which he denied awareness of any Fres-co trade secrets and represented that he would not disclose or use any confidential information that he learned at Fres-co while working for Transcontinental.

The district court issued a TRO, observing that neither Hawkins nor Transcontinental would confirm that Hawkins would not "solicit, contact, or communicate with Hawkins's former Fres-co clients[ ]" and accordingly determined Hawkins would "begin work as a sales representative, the position he occupied while at Fres-co, and be assigned to solicit his former clients." Notably, the court also held that given his position, Hawkins would "likely use his specialized and confidential knowledge to the detriment of Fres-co.... and Hawkins's interference with Fres-co's client relationships would cause immediate irreparable harm to Fres-co."

Hawkins and Transcontinental appealed to the Third Circuit. The appellate court remanded the case back to the district court because it failed to address three of the four requisite elements for injunctive relief. In so doing, however, the court made an interesting observation in its discussion of the irreparable harm element. Without actually referring to the inevitable disclosure doctrine by name, the court recognized that under the Pennsylvania Uniform Trade Secrets Act and the DTSA, "misappropriation of trade secrets need not have already occurred to warrant injunctive relief; threatened misappropriation is sufficient." This is not in and of itself a controversial statement, as the DTSA does permit injunctions to be issued based on "threatened misappropriation" (so long as it is not based "merely on the information the person knows"). Citing the lead opinion from the Circuit that applied the inevitable disclosure doctrine to Pennsylvania law (*Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 114 (3d Cir. 2010)), the Third Circuit agreed with the district court, and appeared to apply the doctrine in the context of Fres-co's DTSA claim: "Given the substantial overlap (if not identity) between Hawkins's work for Fres-co and his intended work for Transcontinental—same role, same industry, and same geographic region—the District Court was well within its discretion to conclude Hawkins *would likely use his confidential knowledge to Fres-co's detriment*." (Emphasis added).

The Third Circuit was not clear whether its application of the inevitable disclosure doctrine was based solely on the Pennsylvania Uniform Trade Secrets Act, as opposed to the DTSA, although it appears to have been based on both. This could create confusion in states in which the inevitable disclosure doctrine is not permitted by state law (e.g., California, Maryland, and Virginia).

Nevertheless, the Third Circuit's application of the inevitable disclosure doctrine in a decision addressing the DTSA is the second opinion in less than a month to do so. If other federal courts follow, we could see the spread of the doctrine across the country and into jurisdictions that have expressly banned its application at the state level. Only time will tell whether this trend will continue, or if the federal courts will clarify what the DTSA seems to provide in its plain language: that injunctions keeping a former employee out of work may not be based on their alleged "inevitable disclosure" of trade secrets.





## The Smartphone: A Treasure Trove of Evidence in Trade Secrets Cases

*By Guest Author for TradeSecretsLaw.com (July 13, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Supreet Singh, a senior consultant at iDiscovery Solutions, Inc.*

It's hard to believe the first smartphone was released over 20 years ago. At that time, few thought it would become such an integral part of our lives. Additionally, this year marks the 10th anniversary of the iPhone and its introduction altered the world of digital forensics. Smartphones contain a wealth of personal and sensitive information like passwords, security or access codes, account numbers, electronic communications, and much more. But they are more than mere containers of data. Between the operating system, installed applications, and service providers, there's a wealth of information that can provide dramatic insight into conversations, activities, habits, preferences, and movements of the phone's user.



There are essentially three places where smartphone related data can be found: on the phone itself, with mobile app providers (e.g. Facebook, Snapchat, or Yelp), and with the service provider (e.g. AT&T or Verizon). Data from all three sources can be very useful in civil lawsuits, criminal cases, or internal investigations, depending on the needs of the case.

Let's look at data stored locally on the phone and captured by mobile application providers. Many mobile apps require access and store data you're not aware of, enabled by permissions sometimes given without a second thought. Common examples are photo editing apps accessing camera and media files and navigation apps accessing your GPS (Global Positioning System). Some apps seek permissions to access user data not needed for app functionality, like gaming apps accessing text messages or contacts. Many apps transmit and receive data between phone and remote servers, meaning a copy of user content may be collected and stored on those remote servers in the name of a better user experience.

The third player, service providers, collect and store information like historical call records, including locations of cell towers a phone connected to. This can be powerful evidence in relatively simple cases or highly complex crimes. Let's use a middle-of-the-road example: serial bank robbery. If a bank crew robbed different banks at different locations, and they carried phones turned on during the thefts, then cell tower logs from in and around each bank's location could be analyzed to narrow down persons of interest, as it would appear unlikely for people other than the robbers to be at all the same locations on the dates and times of the thefts.

Smartphone data can be a key source of evidence in litigation or investigations. Preserving and retrieving it in a manner that is admissible and defensible in court is vital. Many smartphones can be



# Trading Secrets



wiped remotely, so they usually should be turned off when seized, and stored in a secured location with no cellular, WiFi, or Bluetooth connectivity. Smartphones may present challenges to many forensic investigators due to their frequently changing systems. Capturing all associated data can be difficult – interpreting it even more so. We have had great success with custom tools developed to speed up the extraction, analysis, and mapping of usage data.

Counsel should be aware there's more to smartphones than meets the eye. At a minimum, the first step in litigation or investigations should be to preserve data from any smart device, and seek expert forensic assistance. It could make an invaluable impact in your next case.



## The Neutral Corner: Using Forensic Neutrals in Trade Secret Disputes

*By Guest Author for TradeSecretsLaw.com (July 20, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Daniel Garrie, senior partner and co-founder of Law & Forensics.*

*This post originally appeared on the Legal Executive Institute blog.*

The dirty secret of trade secret disputes is that even if you win, it can be difficult to get back to where you started. It's like closing the stable door after the horses have run off with trade secret disputes. A court or arbitration panel may not have trouble reaching findings of fact and conclusions of law, but the secrets are still out there. And ensuring that the trade secret information is entirely removed from the offending company's systems is a lot harder than rounding up wild horses.



Enter the forensic neutral. Forensic neutrals can help sort out the technical messes that often accompany trade secret disputes by:

- Helping to draft compliance with forensic protocols;
- Ensuring adherence to said protocols;
- Determining the existence and veracity of digital evidence;
- Forensically analyzing deleted or corrupted data for evidence of wrongdoing;
- Helping to obtain injunctive or preliminary relief, including “ex parte seizure” orders under the 2016 Defend Trade Secrets Act of 2016 (DTSA);
- Performing settlement-related or court-ordered purging of data from systems;
- Validating the removal of data from systems; and
- Auditing systems to ensure compliance with a court order or regulatory mandate.

The DTSA provides for a variety of situations in which a forensic neutral can be valuable. It states that an “owner of a trade secret that is misappropriated may bring a civil action under this subsection if the

# Trading Secrets



trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.”

As remedies, parties can seek damages and/or injunctive relief and, in certain situations, the DTSA allows for “ex parte seizure” of property if “necessary to prevent the propagation or dissemination of the trade secret.” Because ex parte seizure applications are brought by the plaintiff without any notice to the defendant, and thus subject to potential abuse by an unscrupulous plaintiff, the DTSA sets out an extremely high standard that the plaintiff must meet, via sworn affidavit or verified complaint, to obtain an ex parte order. Forensic neutrals can be especially useful when “ex parte seizure” or other types of preliminary, injunctive relief is sought, as these types of relief often require the highly technical identification, collection, transfer and deletion of trade secret data.

## Making Sure Your Secrets are Deleted

Or consider another common trade secret scenario where employees go to work for a direct competitor of their former company, bringing with them gigabytes worth of confidential data. In response, the former employer seeks to enforce a confidentiality agreement that requires employees leaving the company to turn over all company data on their devices and accounts. The company invokes the arbitration clause in the employment agreement, and the arbitrator is prepared to rule in favor the company. Yet, the question remains: how can the arbitrator ensure an adequate remedy for the company? While it may be simple in theory to order the employees and their new employer to return the data and delete it from their systems, effectuating such an order, and ensuring actual, complete and continuing compliance, can be complicated.



One solution is to utilize a forensic neutral to help prepare a protocol for the identification and deletion of all the company’s data in the possession of the employees and ensure compliance with the protocol. The exact scope of the forensic neutral’s work can vary depending on the needs of the case, but the goal is to ensure the demands of the order are met from both a technical and legal perspective.

Forensic neutrals combine experience and training on both the technical and legal issues in these matters. As attorneys, forensic neutrals can help parties understand the technical requirements set forth by a protective order, draft necessary protocols and monitor compliance with a court order. As technologists, they can also perform the technical work themselves. This can save significant time and money, can often lead to quicker and more effective dispute resolutions, and can reassure the injured party that its trade secrets have been fully purged and protected.

While forensic neutrals can add value in many situations, not every case calls for one. Forensic neutrals are most useful in situations involving large volumes or highly sensitive electronically stored data; forensic protocols; collecting and analyzing data; purging data from computer systems; and/or performing deleted file analysis.



# Trading Secrets



## Robert Milligan to Speak on the “Injunctive Relief” Panel at the Sedona Conference on Developing Best Practices for Trade Secret Issues

*By Seyfarth Shaw LLP (July 21, 2017)*

Robert B. Milligan, Seyfarth Partner and Co-Chair of the Trade Secrets, Computer Fraud & Non-Competes Practice Group, will be a speaker for the “Injunctive Relief” panel at the Sedona Conference on Developing Best Practices for Trade Secret Issues on December 8 at 8:30 a.m., in Scottsdale, Arizona.



The panel will discuss:

- The uses of equitable solutions in trade secret disputes
- How parties and courts can craft case-specific remedies
- How to ensure that, while offering the virtue of flexibility, equity is not whim

The Sedona Conference is an assembly of thought leaders in the areas of antitrust laws, complex litigation, and intellectual property rights; and it brings together the brightest minds with the goal of creating practical solutions and recommendations on tipping point issues.



## How to Catch Trade Secrets Thieves Who Try to Cover Their Tracks: A Forensic Perspective

*By Guest Author for TradeSecretsLaw.com (July 24, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Jonathan Karchmer, a senior managing consultant at iDiscovery Solutions with experience in managing projects dealing with computer forensic examination and experience advising counsel regarding intellectual property and trade secret theft.*



It was a matter of hours. A simple thing really. Was an email sent at 10:00 a.m. or at 2:00 p.m.? An entire case hung in the balance; if the email was sent at 10:00 a.m., the custodian had prior knowledge, if at 2:00 p.m., then not. Unfortunately, the email had been extracted and produced on multiple occasions during the litigation, each showing a different time. iDS was called in to do two things: First, determine the correct time the email was sent, and second, explain to the court how the time could have been incorrectly reported so often without nefarious intent.

This type of analysis is common, and iDS is frequently called upon to examine computer media and authenticate electronic documents. Many projects deal with determining precisely when a document was first created or last altered. Apart from just looking at the documents in question—which contain an abundance of data themselves—we often find ourselves examining computer systems to determine whether the system date or time has been changed.

Changing the date and/or time on your computer is easy and when done on a Windows system, the change is instant and transparent to the user. What happens behind the scenes is less obvious, however. There are easily half a dozen or more artifacts we examine that will tell us when the date/time on a Windows system may have been manipulated—I'll discuss a few of them here:

### 1. Event Logs

The Windows operating system records and logs significant system events and other notifications, storing this information in Event Logs or .evtx files. A feature of these files is that within each entry, the current system date/time is recorded along with a record number that increments by one for each new log entry. Regardless of what the system date/time is set to, if the latest event's record number is currently "x," the next record number will always be x+1. Because of this, system/date time changes are clearly obvious to examiners—we need only look for instances where the current number does not agree with the succession of numbers. Additionally, Windows also considers a date/time change to be a significant event, meaning if the date/time is changed, it is recorded as its own event. Unfortunately, event logs do not hang around forever, so we also look elsewhere to be thorough.

### 2. USNJrnl Entries





# Trading Secrets



Windows system hard drives have a transactional journal which records events surrounding file creation, renaming, changing, and deletion (to name a few). USNJournal entries also include an updated sequence number (or USN), where newer transactions have greater USN values. The date/time is also recorded in USNJournal entries. This combination gives examiners another potential investigative tool—when USN values fall out of sync with the recorded date/time, clock manipulation likely occurred. While USNJournal entries are also transitory, they can be found in many places on the hard drive, including volume shadows and in empty disk space. This makes them valuable in terms of their ability to tell a story about what has happened on a hard drive and to the host operating system, including date and time changes.

### 3. Time Stomping

Software tools exist that let users change the dates associated with documents. Timestomp and others like it can change the dates/times associated with files that users see in Windows Explorer. This can be an effective means of fooling a casual user, but the Windows system stores more data for each file and folder than what's displayed by Explorer. Dates that are visible in Explorer come from a file system element called the Standard Information Attribute (SIA). Behind the scenes, another set of attributes called the Filename Attributes (FNA) also record dates/times. While the SIA can be manipulated, the FNA cannot. Comparisons can be made between the two to highlight to the examiner any instances where dates/times were likely changed on files themselves.

Tools like Timestomp leave their own signature (e.g. anomalies in metadata)—but that type of analysis will be discussed in another blog post. As far as the email we started with? It was sent at 2:00 p.m., so no prior knowledge. Once that was cleared up, the case settled within 24 hours. In many instances, dates and times are critical to litigation, so if there is any doubt, or if dates and times shown don't appear to make sense, it might help to have an expert take a look.



## How to Address Wipers in Trade Secret Cases

By Guest Author for TradeSecretsLaw.com (August 2, 2017)

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Bobby R. Williams, Jr., a senior consultant at iDiscovery Solutions.*

When litigation looms or a data preservation notice is sent out, key individuals or parties might try to delete data to avoid discovery – despite well-publicized horror stories regarding data destruction, phone and email wiping, and the risks of spoliation and sanctions. In many cases, if we find an absence of evidence during an examination, we typically also find evidence of destruction. We refer to these individuals as “Wipers.”



Wipers are the folks who roll the dice and try to game the system. They have enough knowledge to know how to destroy data, feel like they can get away with it, and take a chance. “The document is gone, aha!” might say the Wiper. However, Wipers still run into problems they didn’t anticipate. Even if they manage to delete or destroy the incriminating document or email, they’ve usually taken the time to install and run data destruction software, leaving behind associated artifacts showing the download and usage of such software. Another thing Wipers usually don’t consider: they leave behind other artifacts and data that gives us a clear picture of the document. Data showing when the document was created or modified, the folder it was saved in, even who opened it, when, and how many times. In trying to cover up the original footprints, they invariably left new footprints. And sometimes, even when a Wiper believes they completely deleted the document itself, it sometimes resides in a snapshot or backup they did not see.

“Amateurs!” says the super-duper IT-savvy group of Wipers with IT backgrounds. This group of Wipers takes it to another level – they sometimes wipe their entire hard drive, install a fresh instance of their operating system, and rebuild their system from scratch. “The whole computer is gone, aha!” These Wipers have no choice but to own up to what they did. Hard drives do not yet wipe themselves. As a client once told me, nothing says “culpability” like a freshly-wiped hard drive that was wiped when it should have been preserved.

On a recent project, iDS took possession of a computer used by a long-time office administrator who worked for the defendant for several years. Examination of the computer’s hard drive showed that it appeared to be brand new – it was never used. The drive did not even have a user profile for the administrator, despite the computer being used daily. It turns out the administrator opted to have IT wipe their hard drive before providing it to counsel. Instead of handing over their documents and email for preservation, the administrator now had to explain to management and legal counsel why they instead chose to destroy all the data on their computer. A potential case destroyer, but at the very least, a move that usually leads to sanctions or adverse inference instructions.

At the end of the day, Wipers pretty much announce to everyone that they’re wiping. Facing the music is often the easiest route, and it certainly puts counsel in the best position to protect their client.

# Trading Secrets



## Webinar Recap! Trade Secret Protection: What Every Employer Needs to Know

*By Robert Milligan & Daniel Joshua Salinas (August 11, 2017)*

In Seyfarth's fourth webinar in its series of 2017 Trade Secrets Webinars, Seyfarth attorneys Robert Milligan and Joshua Salinas were joined by Jim Vaughn, one of California's leading computer forensics experts, presented [\*Trade Secret Protection: What Every Employer Needs to Know\*](#). The panel focused on how to help employers navigate the tricky trade secrets waters and provided best practices for trade secret protection.



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

- Employers should review their non-disclosure and non-compete agreements to determine whether they have accurately defined the scope of categories of their confidential information, as well included the whistleblower immunity language required under the Defend Trade Secrets Act. Additionally, they should determine ensure their agreement complies with recent changes in non-compete law, including legislative changes in Nevada, Oregon, Idaho, and Alabama.
- Employers should consider how they treat employee personally owned devices for work as well as corporate issued mobile devices. Getting access to those devices may prove to be challenging upon an employee's departure. Having a policy and technology in place to allow the employer to gain access to their data is critical.
- Effectively protecting trade secrets includes not only creating an internal culture of confidentiality with employees but also limiting information made available to vendors and subcontractors and having appropriate trade secret protection agreements with third-parties.



## Key Employee Departures and Trade Secret Risk Assessment

*By Guest Author for TradeSecretsLaw.com (August 24, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Charlie Platt, a director at iDiscovery Solutions.*

It's Friday afternoon and the conversation goes a little like this, "Wait, what? They're leaving? Where are they going? Is there any opportunity to help them reconsider?"

When a key employee departs an organization, it can take a toll on clients and colleagues, productivity, and morale. What follows is a rush of activity: current projects are reviewed, transition plans are quickly drawn up and put in place, and decisions are made about how to replace the departing employee and how to communicate the departure to the rest of the firm and clients.



Unfortunately, this can also raise questions of concern for the organization, such as, "Did they take any electronic documents with them and, if they did, how can we tell?" Today, employees have easy access to more information than ever before and even greater opportunity to walk away with company data. While most don't, too many make the choice to take something. Despite best efforts and safeguards, the prevalence of mobile devices, cloud storage, USB devices, etc. provide several possible avenues for a misguided employee to take sensitive company data with them when they depart.

Assessing a single avenue (e.g., USB devices) is not very complicated and can be very insightful. One of my iDS colleagues, Arnold Garcia, [recently wrote about USB devices](#) and how we can determine the history of their usage on a computer. This can be a big help in understanding if an employee took electronic documents upon departing an organization. Along with USB issues, some other questions to consider are:

- Did the employee have access to any valuable company assets (client lists, pricing, designs, etc.)?
- Did the employee visit any cloud storage and/or personal email websites recently and frequently?
- Was there any recent abnormal network or file access?
- What's the risk to the business?



# Trading Secrets



- What are the recommended next steps (if any) for further investigation?

Assessing the overall risk of data theft across a variety of potential data sources has historically been time consuming and expensive. The right experts, like those at iDS, armed with proven methodologies and proprietary tools, can quickly assess all the available evidence, paint a detailed and reliable picture of the departed employee's last days or hours, and determine the potential risk involved. With this assessment, you can make an informed, evidence-based decision on how to proceed.

When key employees leave, it can be a difficult time for an organization. Using a qualified forensic examiner is a must to take some of the guesswork out of the process and give you good, solid evidence.

# Trading Secrets



## File Share Platforms and Business Risk

*By Corey Bieber (September 5, 2017)*

The use of open file sharing platforms in business continues to increase in 2017; Dropbox alone has over 200,000 active business accounts. Unfortunately, the convenience of these platforms and the increase in use by businesses attracts the attention of hackers as well. File sharing platforms and accounts have a high “hack value”—the overall value of the accounts on the dark web—due to the relative ease with which account can be obtained and the sensitivity of the information stored on these platforms.



The risk associated with the use of file share platforms is twofold. First, company supported file share is attractive to attackers because it is guaranteed to contain sensitive information. Second, file share platforms available to employees outside of the company—e.g. the employee Google Drive account—may be used to store company information, but likely do not use the same security standards as those enforced by the company. Attacks on file share platforms are also very real. In August of 2016 Dropbox forced users to reset their passwords based on a breach—60 million account credentials compromised—that had been discovered but was executed four years earlier in 2012.

Thus, it is important that businesses educate their employees on the risks of sharing information on these platforms and apply strict administrative and technical safeguards mitigate the risk of attack.

### Common File Share Attack Approach

The most common approach attackers use to compromise file share platforms is phishing. Phishing is a technique by which the attackers sends out a legitimate looking (albeit fake) email which entices the employee to click on a link and provide information—such as login credentials—which goes directly to the attacker. Alternatively, the phishing attack may convince the employee to download an infected file to the same ends. Once the attacker has compromised the file share, he or she can either steal information directly, escalate privileges to access more information, obtain additional account credentials, or sell the information on the dark web. Access to the file share can also be used to perform a Denial of Service (“DoS”) attack by downloading or uploading large volumes of data thus congesting the network and preventing legitimate use.

Despite Google’s perceived safety, two major phishing attacks have been reported on Google accounts in the last two years. In late 2016, over a million google accounts were compromised by a malware attack known as Gooligan, designed to steal credentials allowing access to the victims Google services. Gooligan infected an estimated 13,000 devices per day during its lifecycle. Again in early 2017, Google accounts were targeted with a message requesting the user to download a file. When the user selected the link to download the file a face service that looked like a legitimate google service would request access to the users Gmail account.





# Trading Secrets



## Mitigating Risk

Businesses can mitigate the risk of file share attacks by implementing strict policies and sanctions regarding their use. For example, all non-business file share sites can be blocked on the company's network. Strict policies and monitoring should be in place to gain access to file share sites and employee accounts with such access should be closely monitored. Businesses should also implement test "phishing campaigns"—sending out company controlled phishing emails—to educate employees on what these email look like and how to avoid them. Phishing tests also help businesses understand their risks by monitoring the number of employees who click on the bogus links. Whereas businesses have less control over employees loading data on to personal file share accounts, strict sanctions should be in place regarding this activity and employees should be aware of these sanctions.



## Wisconsin High Court Affirms High Summary Judgement Bar to Trade Secret Misappropriation Claims

*By Kevin Mahoney (September 6, 2017)*

A recent decision from the Supreme Court of Wisconsin affirmed a trial court's grant of summary judgment in favor of a defendant accused of conspiring to misappropriate its competitor's trade secrets. By a 4-3 decision in *North Highland Inc. v. Jefferson Machine & Tool Inc.*, 2017 WI 75 (July 6, 2017), the Court found that plaintiff North Highland, Inc. ("North Highland") had failed to present sufficient evidence of misappropriation or conspiracy to proceed beyond the summary judgment stage, prompting a notably sharp exchange with dissenting Chief Justice Patience D. Roggensack and a second dissent by two other justices.

Highland is a Wisconsin-based manufacturer of industrial products. One of the companies it distributed its products to was Bay Plastics, Inc., owned by Frederick Wells. Prior to 2011, Wells decided to form a separate company to manufacture the products which Bay Plastics sold, including some of the products which it purchased from North Highland. Wells formed Jefferson Machine & Tool Inc. ("Jefferson Machine") along with Dwain Trewyn—Wells owned 75% of Jefferson Machine and Trewyn owned the remaining 25%. At the time of Jefferson Machine's formation, Trewyn was employed by North Highland in sales. Trewyn did not have a non-competition agreement with North Highland, but also did not inform North Highland that he would also be working at Jefferson Machine.

When Tyson Foods issued a request for quotes to several vendors for 3,000 trolleys to be used in one of its plants, North Highland was on the list of approved bidders receiving the request while Jefferson Machine was not. The employee responsible for preparing North Highland's bid was Trewyn. Less than three weeks after the request was issued, Trewyn obtained approval from Tyson to submit a bid on behalf of Jefferson Machine as well, even though it had not been on the approved bidder list. Trewyn was also responsible, along with Wells, for preparing Jefferson Machine's bid. Trewyn did not disclose to North Highland that he was preparing bids on behalf of both North Highland and Jefferson Machine for the same Tyson Foods request. Despite not having initially been an approved bidder, Jefferson Machine submitted a lower bid than North Highland and was awarded the Tyson Foods contract. After North Highland discovered the circumstances behind its lost bid, it terminated Trewyn and threatened to seek injunctive relief against Jefferson Machine, which resulted in Tyson Foods cancelling the contract and awarding it to neither company.

North Highland filed suit against Trewyn, Bay Plastics, Wells, and Jefferson Machine for breach of contract, breach of fiduciary duty, conspiracy, tortious interference, and misappropriation of trade secrets under Wisconsin state law. While it settled its claims against Trewyn and its claims against Bay Plastics were dismissed, North Highland proceeded on its claims against Wells as an individual for civil conspiracy to breach Trewyn's fiduciary duties to North Highland, as well as its claim that Wells had misappropriated North Highland's trade secrets—in this, its confidential bid information on the Tyson

# Trading Secrets



Foods project—in violation of the Wisconsin Trade Secrets Act.. Wis. Stat. § 134.90. The trial court entered summary judgment in favor of defendants on those counts, finding that North Highland failed to present evidence sufficient to defeat a motion for summary judgment. The Court of Appeals affirmed, although its unpublished opinion focused on the issue of whether North Highland's bid constituted a trade secret under Wisconsin law, finding that it did not. *North Highland, Inc. v. Jefferson Mach. & Tool. Inc.*, No. 2015AP643, ¶ 25, unpublished slip op. (Wis. Ct. App. Apr. 28, 2016).

In affirming the Court of Appeals' decision, the majority first noted that it was doing so on different grounds, and specifically without reaching the question of whether or not a bid would qualify as a trade secret under the circumstances presented. 2017 WI 75, ¶ 4, n. 4. Instead, the majority focused on whether or not North Highland had presented sufficient evidence of its claims to survive a motion for summary judgment. In finding that North Highland had not done so, the Court placed considerable emphasis on the fact that both defendants Trewyn and Wells had testified that, even though Wells was aware of Trewyn's involvement in setting the bid amounts for both North Highland and Jefferson Machine, Trewyn had not disclosed the amount of North Highland's bid to Wells. *Id.* at ¶¶ 11-13. While acknowledging the considerable circumstantial evidence suggesting collusion between Trewyn and Wells in formulating Jefferson Machine's bid, the majority found that such evidence was insufficient in light of "unrebutted deposition testimony" from Wells and Trewyn:

North Highland contends that the evidence submitted to the circuit court on summary judgment is sufficient to allow a reasonable inference that Wells conspired with Trewyn....Based on this evidence of Wells and Trewyn's working relationship at Jefferson Machine, an inference may be drawn that Trewyn shared his knowledge of the Tyson bid with Wells. However, the unrebutted deposition testimony supports the opposite conclusion. There is no evidence of the formation and operation of a conspiracy....As set forth more fully above, Trewyn similarly testified that Wells had no knowledge Trewyn was bidding on the Tyson project for North Highland. He stated that he did not discuss his work on the Tyson project with Wells and that he did not tell Wells that he submitted a bid for North Highland.

*Id.* at ¶¶ 30-32.

Because North Highland had not submitted any evidence in opposition to summary judgment rebutting that deposition testimony, the majority found that it had failed to meet its burden of showing that there was some basis for a jury to find that there was either a conspiracy or that Wells had misappropriated North Highland's confidential information.

Chief Justice Roggensack dissented from the majority's decision in strong terms, finding that the circumstances of the bidding process on their own created a sufficient factual question that should have been submitted to the jury while nothing that "[e]vidence of misappropriation of trade secret information does not have to be direct evidence. Circumstance evidence must also be considered..." *Id.* at ¶ 109. The dissent's claims of what that circumstantial evidence showed, however, prompted a rebuke from the majority accusing the dissent of "misinform[ing]" those who read it, "cherry-pick[ing]" certain parts of the record, and "creat[ing] its own facts." *Id.* at ¶ 42, n. 12. A separate dissent by Justice Bradley agreed that the case should have been submitted to the jury, while discussing at length the conclusion that a bid could constitute a trade secret under Wisconsin state law.

## Conclusions and Takeaways



# Trading Secrets



On their face, the undisputed facts underlying the majority's decision would appear to create more than enough circumstantial evidence to defeat a summary judgment motion and submit North Highland's claims of misappropriation to a jury. The same individual (Trewyn) created the bids submitted by two bidders for the same job—his employer and the side company which he did not tell his employer about. Trewyn's and Wells' testimony that the former did not tell the latter about the amount of North Highland's bid, and the Supreme Court of Wisconsin's emphasis on that testimony as "unrebutted"—seems to be an instance of a defendant testifying "I did not do what I am accused of doing," and a court finding that self-serving testimony to be dispositive in favor of the defendant. Direct evidence of misappropriation of trade secrets, wherein a defendant flatly admits to misappropriation or where documentary evidence exists of same, is understandably rare.

Regardless, parties seeking to prove misappropriation claims under Wisconsin law are now on notice as to the importance of finding some direct evidence of misappropriation in defeating a motion for summary judgment. Expedited discovery—especially the imaging of electronic devices in cases where parties may delete evidence of the sharing of trade secrets among defendants—will continue to be of particular importance in misappropriation actions. While the Court's decision does not offer binding precedent on the issue of whether or not a bid can constitute a trade secret under Wisconsin state law, three dissenting justices found that such information could qualify as a trade secret while the majority refused to address the issue either way.



## Locating Digital Breadcrumbs: Programs Can Run, But They Can't Hide

*By Guest Author for TradeSecretsLaw.com (October 4, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Jonathan Karchmer, a senior managing consultant at iDiscovery Solutions.*

Determining whether programs or malware actually ran on a system is an important goal of seasoned examiners when investigating computer evidence. Generally, there are several artifacts left behind anytime executables are run—regardless of whether the program is Outlook, Chrome, or something malicious. Today we'll cover some artifacts we encounter on Windows systems.



**Prefetch:** This could be the most well-known artifact that examiners focus on when looking to see which programs have run on a system. Around since Windows XP, its purpose is to launch applications faster and decrease errors that might occur on first launch. From an investigation standpoint, Prefetch files can provide details about not only when applications launched, but where they were launched from. On current systems, metadata—such as dates of execution—are embedded in these files.

We do see instances where Prefetch files are deleted by those who want to hide their tracks, since this process is not difficult. These files are also deleted regularly during the normal course of operation—something to consider. In instances where Prefetch is not enabled or when no Prefetch files are left behind, we have other places on the system to look for evidence of program execution—for example, the registry.

**UserAssist:** Focused on Graphic User Interface (GUI) programs, this utility tracks the run count of executables, as well as the last date and time of execution. Its information is embedded in a registry hive file for the user account under which the executable was run; important to note in case there are rogue or multiple user accounts on a system. UserAssist also provides context around how a given executable was run; i.e. it can help answer whether the program was launched from a shortcut file or run directly. For experienced investigators, this can be a powerful detail when piecing together a timeline of activity, as well as differentiating between applications that were clicked-on directly versus those launched through another process.

**ShimCache:** This Windows-based Application Compatibility Database, stored in the SYSTEM registry hive, assists with executable compatibility across different operating system versions. Basically, ShimCache tracks programs for purposes of determining whether they will run on the current system. Older programs sometimes don't get along with newer operating systems, so when a program runs, ShimCache checks it for compatibility. A caveat is that programs may be listed here even if they were simply browsed and not executed—so it's important to note which programs are also flagged as having



# Trading Secrets



run. For examiners, the ShimCache is a go-to for systems like servers where Prefetch may be disabled—as it can help examiners determine if/when malware was executed on a system.

**AmCache:** This file, its own registry hive, tracks the filename and path of executables that have been run while also providing a hash value of the executable, which can be useful in tracking whether those executables also appear on other systems. With this information, examiners may discover that executables are being run from other volumes besides the local C: drive, like USB devices. This could focus investigations on rogue USB usage, as well as rogue users on premises.

Why do computers track so much information about you? Microsoft and other developers are constantly looking to improve the “user experience” to allow your operating system to make helpful suggestions. For instance, over time, your system may offer to open a recently used program or a recently used document for you. Thankfully, for skilled forensic investigators like those I work alongside at iDS, the same artifacts also help us track down malware or rogue user activity, which can be key to locating valuable evidence.





## Big Brown v. PowerPoint Pilferers in Trade Secret Spat

*By Eric Barton (October 10, 2017)*

Earlier this week, the United Parcel Service, Inc. (“UPS”) filed a lawsuit in the Northern District of Georgia, Atlanta Division, against several unidentified UPS pilots, who are referred to in the complaint as “John Does 1-5.” The lawsuit alleges that “[i]n August 2017, certain UPS employees developed strategic plans regarding the Company’s aircraft. These plans were developed for, among other things, reporting to senior executives of the Company in late August 2017 so that they could make certain strategic business and financial decisions. Portions of these plans were included in a PowerPoint presentation created by this limited group of UPS employees (the “PowerPoint”). In preparation for the meeting, a very limited number of UPS employees had access to the PowerPoint for the purpose of its drafting and editing.” (Complaint, ¶ 7.) The lawsuit goes on to allege that the PowerPoint contained highly confidential and trade secret information. (*Id.* at ¶¶ 9-10.)



The complaint further states that “[a]t some point, an unknown UPS pilot wrongfully obtained a copy of the PowerPoint. The unknown UPS pilot knew that the PowerPoint contained UPS’s trade secrets. On or about September 27, 2017, the unknown UPS pilot posted statements on an online pilot discussion forum about UPS’s confidential strategic plans regarding its aircraft. At the same time, the unknown UPS pilot also posted on the website a link to a Dropbox folder where individuals could view and download the PowerPoint that was wrongfully obtained by the unknown UPS pilot.” (*Id.* at ¶ 13.) UPS alleges that the unknown pilot also “disclosed the contents of the PowerPoint to other individuals without the permission or authority of UPS.” UPS does not speculate as to the motive behind the alleged publication of the PowerPoint or the identity of the “other individuals” involved, but claims that the unknown UPS pilots “presently maintain copies of the PowerPoint without the permission or authority of UPS.” (*Id.* at ¶ 17.)

The lawsuit alleges just two causes of action: (1) violation of the Defend Trade Secrets Act; and (2) violation of the Georgia Trade Secrets Act. No immediate injunctive relief was sought (likely because the identity of the pilots is currently unknown), but contemporaneous with filing suit, UPS also filed an Emergency Motion to Conduct Limited Expedited Discovery, with the stated purpose of “(1) identifying the unknown individuals who obtained the PowerPoint without permission or authorization of UPS; and (2) gathering and preserving any information necessary for UPS to pursue its claims against the Defendants.” UPS promptly supplemented its Emergency Motion, identifying three custodians from whom they wished to subpoena and requested responses within five calendar days of service.

The lawsuit is styled *United Parcel Service, Inc. v. John Does 1-5*, United States District Court, Northern District of Georgia, Atlanta Division, Civil Action File No. 1:17-cv-03843-CAP.

# Trading Secrets



## Webinar Recap! The Defend Trade Secrets Act–The Biglaw Partner and Forensic Technologist Perspective

*By Robert B. Milligan (November 20, 2017)*

Robert Milligan, along with Certified Forensic Computer Examiner Jim Vaughn, presented [The Defend Trade Secrets Act – The Biglaw Partner and Forensic Technologist Perspective webinar](#) for Metropolitan Corporate Counsel on Thursday, November 2. They focused on the key features of the DTSA and compared its key provisions to the state Uniform Trade Secrets Act (UTSA) adopted in many states, and they provided practical tips and strategies concerning the pursuit and defense of trade secret cases in light of the DTSA and some predictions concerning the future of trade secret litigation.



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

- The Defend Trade Secrets Act provides trade secret owners a new federal property right and provides them additional options and remedies when their trade secrets are stolen.
- Employers should consider how they treat employee personally owned devices for work as well as corporate issued mobile devices. Getting access to those devices may prove to be challenging upon an employee's departure. Having a policy and technology in place to allow the employer to gain access to their data is critical.



## Computer Fraud and Abuse Act

# Trading Secrets



## Supreme Court Refuses to Hear Password-Sharing Case, Leaving Scope of Criminal Liability Under Computer Fraud and Abuse Act Unclear

*By Scott E. Atkinson (October 16, 2017)*

On Tuesday, October 10, 2017, the United States Supreme Court [denied certiorari](#) in *Nosal v. United States*, 16-1344. Nosal asked the Court to determine whether a person violates the Computer Fraud and Abuse Act's prohibition of accessing a computer "without authorization" when using someone else's credentials (with that other user's permission) after the owner of the computer expressly revoked the first person's own access rights. In denying certiorari, the Court effectively killed the petitioner's legal challenge to his conviction in a long-running case that we have extensively covered [here](#), [here](#), [here](#), [here](#), [here](#), [here](#), and [here](#) (among other places). The denial of certiorari leaves further development of the scope of the CFAA in the hands of the lower courts.



Nosal's conviction resulted from accessing his former employer's proprietary database in order to set up a competing business using credentials shared by an insider, his former executive assistant.

David Nosal was a recruiter employed by the executive search firm Korn/Ferry. To serve its clients and place executives in response to talent searches, Korn/Ferry maintained a confidential, proprietary database of detailed personal information about more than 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 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. (See [18 U.S.C. § 1030\(a\)](#).) Nosal was ordered to pay a sizable restitution award to Korn/Ferry and was sentenced to a year and a day in prison.

Ninth Circuit panel split on whether the case is "about password sharing," and its amended opinion left unclear the scope of CFAA liability.

The *Nosal* case actually took two trips to the Ninth Circuit, but it was the latter trip that resulted in the recently denied certiorari petition ("*Nosal II*"). The Ninth Circuit's opinion revealed internal divisions over not just the scope of the CFAA, but even what the case was about. Judge Reinhardt opened his dissenting opinion by flatly declaring, "This case is about password sharing." Judge Reinhardt argued that the majority's opinion upholding Nosal's conviction could criminalize all sorts of common password sharing conduct among friends and family. To rebut Judge Reinhardt's position, the majority focused on Korn/Ferry's explicit revocation of access to Nosal, noting that, "Unequivocal revocation of computer



# Trading Secrets



access closes both the front door and the back door.” In the panel’s original opinion, the majority opinion directly contradicted Judge Reinhardt, stating, “This appeal is not about password sharing.” The court noted that mere violation of a website’s terms of service would not result in CFAA liability.

The Ninth Circuit declined to rehear *Nosal II* en banc, but the panel majority issued an amended opinion clarifying its perspective that the statute’s mens rea requirement for criminal liability—i.e. that the access be “knowing[] and with intent to defraud”—means that “the statute will not sweep in innocent conduct, such as family password sharing.”

## **Supreme Court declines to resolve alleged circuit split, leaving lower courts to develop the law.**

Nosal then [petitioned](#) the United States Supreme Court for review, arguing that there was a circuit split over whether “the [computer] owner’s intentions, expectations, and contractual or agency relationships” are relevant to assessing whether access to a computer is “authorized” under the CFAA. Nosal contended that the First, Fifth, Seventh, and Ninth Circuits consider these factors, but that the Second and Fourth Circuits consider them to be irrelevant and view the CFAA as a simple anti-hacking statute where a defendant is liable for circumventing a technological barrier. Nosal argued that the Ninth Circuit’s “construction of the CFAA threatens to criminalize a broad swath of innocuous activity that ordinary people engage in every day.”

The Solicitor General [opposed](#) the petition on behalf of the United States. The United States argued that there was no real circuit split because the authorities that Nosal identified did not involve a circumstance where credentials were revoked but a former employee circumvented the revocation by using a different employee’s credentials to access the system. It framed the question narrowly, as whether the Ninth Circuit erred in upholding Nosal’s conviction.

In [reply](#), Nosal argued that the distinctions identified by the United States regarding the case law in other circuits made no practical difference, and that the real divide is over whether the CFAA is an anti-hacking statute that requires circumventing a technological barrier, or if it is something broader, where the computer owner’s intent, expectations, and relationships are examined. Nosal further noted that the Ninth Circuit stood alone in categorically holding that an account-holder’s authorization is inadequate to avoid liability; Nosal argued that the First, Fifth and Seventh Circuits at least left the door open to reading “authorization” flexibly to include “password-sharing and other forms of derivative authorization consistent with the owner’s interests and reasonable expectations.”

Without Supreme Court intervention to clarify the standards for liability under the CFAA, it will fall to the circuits to continue to develop the contours of the law.

Ultimately, it is not clear that *Nosal II*’s statements articulate a workable test for criminal liability that does not place large swaths of the public in potential legal jeopardy. For example: What happens if a user of a video streaming subscription service stops paying for the service, has her access credentials invalidated (or, to use *Nosal II*’s terminology “unequivocally revoked”) as a result of nonpayment, then uses a friend’s log-in information to access the service, intending to get—for free—the service that she once paid for? It is difficult to see how either the “unequivocal revocation” or “knowingly and with intent to defraud” caveats on the *Nosal II* panel’s analysis prevent at least the [potential](#) for CFAA criminal liability. It remains to be seen how lower courts will interpret the CFAA and apply *Nosal* and its peers in circumstances less fraught than the facts of *Nosal*. Will *Nosal* have an unintentionally broad reach? Or will it be reduced to an outlier? Only time will tell.



## Non-Competes & Restrictive Covenant



# Trading Secrets



## Webinar Recap! 2016 National Year In Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law

*By Robert B. Milligan, Michael Wexler & Daniel Joshua Salinas (February 7, 2017)*

We are pleased to announce the webinar “2016 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 [webinar recording](#).

In Seyfarth’s first installment of its 2017 Trade Secrets Webinar series, Seyfarth attorneys reviewed noteworthy cases and other legal developments from across the nation over the last year in the areas of trade secrets and data theft, non-competes and other restrictive covenants, and computer fraud. Plus, they provided their predictions for what to watch for in 2017.



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

- The DTSA can be a powerful tool to protect intellectual capital. However, in order to take full advantage of the DTSA, businesses should carefully check their agreements with employees, handbooks and equity awards to make sure they contain language mandated by the Defend Trade Secrets Act.
- 2016 was a record year for data and information security breaches. Organizations should alert and train employees on following company policies, 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.
- Several states enacted laws to limit the scope and duration of non-competes in 2016. There were also some significant decisions limiting their scope and enforceability in 2016 as well. Companies should have their non-disclosure and non-compete agreements reviewed to ensure that they comply with the latest state and federal laws, including the new Defend Trade Secrets Act.

# Trading Secrets



## In Georgia, the Blue-Pencil Only Strikes Overly Broad Non-Competes and Does Not Rewrite Them

*By Stephanie Stewart (February 27, 2017)*

In Spring 2011, the Georgia legislature passed a new restrictive covenant statute, which, for the first time, allowed Georgia courts in reviewing non-competition agreements between employer and employee to blue-pencil or “modify a covenant that is otherwise void and unenforceable so long as the modification does not render the covenant more restrictive with regard to the employee than as originally drafted by the parties.” O.C.G.A. § 13-8-53(d). Since the new Georgia statute only applies to agreements executed after its enactment, there has been limited litigation concerning the meaning and scope of this provision.



Most of the litigation between 2011 and the present has involved requests by a party that the Court strike an offending provision in a non-compete agreement. Recently, the Northern District of Georgia was given the opportunity to determine whether Georgia’s blue-pencil provision also gives Georgia courts the authority to modify an unenforceable non-compete provision. In *LifeBrite Labs., LLC v. Cooksey*, No. 1:15-CV-4309-TWT, 2016 WL 7840217, at \*1 (N.D. Ga. Dec. 9, 2016), the former employer, LifeBrite, sued its former employee, Cooksey, after she began working for a competitor company. Cooksey’s non-compete provision provided as follows:

7.2. Non-Competition. For as long as she is employed and for a period of one (1) year thereafter, employee shall not participate, directly or indirectly, as an owner, employee, consultant, office management position, in any proprietorship, corporation, partnership, limited liability company or other entity, engaged in any laboratory testing that is being sold by employee on behalf of company.

The Northern District of Georgia found that this provision was overbroad and unenforceable as it did not contain any geographic limitation. Consequently, the Court considered whether or not Georgia’s blue-pencil rules allowed it to modify the non-compete provision to insert a reasonable geographic limitation. In reasoning through the analysis, the Court referred to pre-2011 cases in which Georgia courts interpreted a similar non-compete provision in the context of sale of business agreements. In those cases, Georgia courts held that the blue-pencil marks but it does not write. Thus, the NDGA declined to enforce Cooksey’s non-compete and held that in applying Georgia’s blue-pencil statute, “courts may not completely reform and rewrite contracts by supplying new and material terms from whole cloth.”

The NDGA also noted that Georgia’s employers are “sophisticated entities” which “have the ability to research the law in order to write enforceable contracts; courts should not have to remake their contracts in order to correct their mistakes.” This case is simply further caution to Georgia employers to review their non-competition agreements for overbreadth, vagueness, and the absence of essential limiting terms. As always, the attorneys at Seyfarth Shaw LLP are available to assist in these endeavors.

The *LifeBrite Laboratories, LLC v. Cooksey* case was dismissed with prejudice on January 25, 2017.

# Trading Secrets



## Can You Say P-e-c-u-l-i-a-r-i-t-i-e-s? Seyfarth's Cal-Peculiarities Guide is Here Highlighting Quirks in California Restrictive Covenant and Trade Secret Law

*By James D. McNairy & Robert B. Milligan (May 9, 2017)*

Seyfarth Shaw LLP has released its 2017 Edition of *Cal-Peculiarities: How California Employment Law Is Different*. Included within the publication is an overview of how California law is different in the areas of restrictive covenants, trade secrets, and computer fraud. For example, highlights include:

- But for a narrow exception, new law provides that a California employer cannot in an employment agreement with an employee who primarily resides and works in California require the employee to (1) adjudicate outside of California a claim arising in California, or (2) accept the application of substantive law other than California's with respect to a controversy arising in California. Cal. Labor Code § 925.
- Also, although the Defend Trade Secrets Act of 2016 (DTSA) provides for a federal cause of action for trade secret misappropriation that may be pled in California courts, case law interpreting and applying the preemptive scope of California's Uniform Trade Secrets Act (CUTSA) may impact what state law tort claims can be pleaded in conjunction with a DTSA claim, even where no CUTSA claim is pleaded.
- Finally, in 2016, the Ninth Circuit published its opinion in *United States v. Nosal*, 844 F.3d 1024 (2016), where the court held that unequivocal revocation of computer access makes use of a password shared by an authorized system user to circumvent the revocation of a former employee's access a crime.

Cal-Pecs provides many more useful details in the areas of areas of restrictive covenants, trade secrets, and computer fraud law. Cal-Pecs is available in an [eBook](#) to approved requestors.

[Submit Request](#)





## The Latest East Coast/West Coast Conflict: Massachusetts Courts Consider the Application of California Law in Non-Compete Litigation

*By Erik Weibust & Dallin Wilson (June 21, 2017)*

Harkening back to the rivalry between the Boston Celtics and Los Angeles Lakers in the 1980s, Massachusetts courts (as well as others around the country) have increasingly been asked to analyze the application of California law in litigation related to non-competition agreements. As many readers of this blog know, non-competition agreements are generally not enforceable under California law. Thus, even where the subject agreement contains a forum selection clause outside of California, or where the employee may have worked in another state, former employees are increasingly racing to file first in California courts or arguing that California law should be applied, thereby hoping to avoid any restrictions on mobility.



The Business Litigation Session of the Suffolk Superior Court in Massachusetts recently analyzed these issues in a pair of cases involving the application of California law to cases and agreements outside of the state. In *FTI, LLC, et al. v. Duffy, et al.*, three of the plaintiffs' former employees resigned and shortly thereafter filed suit in California seeking a declaration that the former employees' non-competition agreements were unenforceable. Five months later, the plaintiffs filed a lawsuit in Massachusetts, alleging breach of the non-competition agreements, trade secret misappropriation, breach of fiduciary duty, unfair competition, and other business torts. The defendants moved to stay the case pending final resolution of the California case. One of the former employees also moved to dismiss the claims against him for lack of personal jurisdiction.

The Massachusetts court refused to stay the case, holding that although when duplicative lawsuits are filed in different jurisdictions, the later-filed action is typically stayed, courts have discretion to give preference to the later-filed action when that action will better serve the interests involved. Specifically, the court held that there was minimal overlap between the cases because the California case only sought to void the non-competition agreement, whereas the Massachusetts case involved other claims. Moreover, the agreement was governed by Maryland law and a California court has no greater expertise in applying Maryland law than a Massachusetts court. Finally, the court held that Massachusetts had an equally strong interest in the case because the plaintiffs alleged that the defendants committed various business torts while working at the plaintiffs' office in Massachusetts.

The court also rejected the employee's argument that it lacked personal jurisdiction over him. The court found that the employee had sufficient minimal contacts with Massachusetts where he supervised six employees, regularly traveled to Massachusetts to supervise those employees, and billed a total of 132.3 hours for plaintiff while he was in Boston in 2014 alone. The court also determined that the employee would not be unfairly burdened by having to defend himself in Massachusetts because he lived in New York and having filed a suit in California, he revealed that he was willing to travel across the country to litigate the case.

One month later, the same court was asked to dismiss a breach of contract claim where the agreement contained a Massachusetts forum selection and choice of law provision and the former employee lived



# Trading Secrets



and worked in California. In [Oxford Global Resources, LLC v. Hernandez](#), the defendant argued that the forum selection and choice of law clauses were unenforceable and that the doctrine of forum non conveniens required the case to be heard in California.

Illustrating what some believe has been a shift by the Massachusetts Business Litigation Session recently toward less stringent enforcement of restrictive covenant agreements, the court agreed with the defendant, finding that the subject agreement was a contract of adhesion, noting that the defendant was an entry-level employee who had no meaningful opportunity to negotiate the choice of law provision. The court rejected the plaintiff's argument that the contract contained a section where the defendant acknowledged that he had read the agreement and had the opportunity to have an attorney review it. The court held that the boilerplate language contained in that section did not change the fact that the defendant had no bargaining power with respect to the choice of law and forum selection clause.

The court further determined that the choice of law provision was an attempt to circumvent California's strong public policy against the enforcement of non-competition agreements. If the agreement had not contained the choice of law provision, the court held that California law would govern because the defendant was a California resident who was hired in California to service California clients, notwithstanding that the plaintiff's principal place of business was in Massachusetts. The court also rejected the plaintiff's argument that the agreement did not violate California law because it only barred the defendant from using the plaintiff's confidential information. The court noted that the agreement's definition of confidential information was overly broad and went far beyond what was permitted under California and Massachusetts law.

Lastly, the court found that it would be unfair to compel the defendant to defend himself in Massachusetts. In weighing the relevant private and public interests, the court found that all of the relevant events occurred in California and all of the plaintiff's alleged harm was incurred there. The court also took into consideration that the defendant interviewed for the job in California, was trained in California, did all his work in California, and reported to supervisors in California. Moreover, all of the relevant witnesses were located in California and could not be compelled to testify in Massachusetts. Thus, California was the appropriate forum in which to litigate the claims.

These two cases highlight important issues for employers seeking to enforce non-competition agreements that may implicate California law. First, even where an agreement contains a non-California forum selection clause, courts may not enforce the agreement where the employee had no meaningful opportunity to negotiate the provisions and it appears to be an effort to circumvent California law. Second, courts may refuse to apply a non-California choice of law provision where the employee lives and works exclusively in California. Third, just because an employee was first to file a lawsuit in California, courts will not automatically stay a later filed action in another state, particularly where additional claims are asserted. And finally, while we have blogged on this topic many times before, primarily in conjunction with [legislative efforts](#) to curb enforcement of non-compete agreements, it may ultimately be the Massachusetts courts that bring the Commonwealth closer in line with California when it comes to the enforceability of post-employment restrictive covenants.

Who said there's no East Coast-West Coast rivalry anymore?



# Trading Secrets



## Nevada Enacts New Non-Compete Law

*By Robert B. Milligan & Lauren Leibovitch (July 6, 2017)*

On June 3, 2017, Governor Sandoval signed Assembly Bill 276 into law, amending Nevada Revised Statute 613, which governs non-competition agreements. Notably, the law adds requirements to the enforceability and validity of non-competition agreements, and importantly, now allows courts to “blue-pencil” non-competition agreements, overturning Nevada Supreme Court’s recent decision in *Golden Road Motor Inn, Inc. v. Islam*.



First, the new law establishes that a non-competition agreement is void and unenforceable unless the agreement satisfies four requirements. The agreement must: (1) be supported by valuable consideration; (2) not impose a restraint greater than what is required to protect the employer; (3) not impose an undue hardship on the employee; and (4) impose restrictions that are appropriate in relation to the valuable consideration supporting the agreement.

Second, the law establishes that a non-competition agreement may not restrict a former employee from providing services to a former customer or client if (1) the former employee did not solicit the former customer or client; (2) the customer or client voluntarily chose to leave and seek the services of the employee; and (3) the former employee is otherwise complying with the non-competition agreement.

Third, the law provides that a non-competition agreement is only enforceable during the time in which the employer is paying the employee’s salary, benefits, or equivalent compensation if an employee is terminated because of a reduction in force, reorganization, or similar restructuring.

Finally, the law allows “blue-penciling,” which overturns Nevada Supreme Court’s recent decision in *Golden Road Motor Inn, Inc. v. Islam* (for a discussion of that decision [click here](#)). “Blue penciling” refers to a court’s ability to strike or modify unreasonable terms or provisions from a non-compete agreement, and enforce the revised agreement. In *Golden Road Motor*, the Court refused to adopt the “blue pencil” doctrine because the Court stated it was not its role to rewrite the parties’ contract and that courts are not empowered to make private agreements. The Court held that an unreasonable clause in a non-competition agreement rendered the entire agreement unenforceable. Now, under Nevada’s amended law, the court is empowered to revise a non-competition agreement to the extent necessary and enforce the revised agreement.

Employers should review their existing non-competition agreements for compliance with the Nevada law.



# Trading Secrets



## Robert Milligan to Present “Growing Importance of trade Secrets in Protecting Emerging Technology” Webinar

*By Seyfarth Shaw LLP (July 6, 2017)*

Robert B. Milligan, Seyfarth Partner and Co-Chair of the Trade Secrets, Computer Fraud & Non-Competes Practice Group, will be a panelist for the “Growing Importance of Trade Secrets in Protecting Emerging Technology” webinar presented by ITechLaw’s Intellectual Property Committee on July 11, 2017 at 11:00 a.m. Eastern.

With the growth of artificial intelligence and self-driving technology, we are seeing a growing reliance by companies on trade secret protection. Robert Milligan will provide for an informative discussion regarding this important topic. Specifically, he will cover:

- Increasing reliance on trade secrets to protect cutting edge technologies
- *Waymo v. Uber*: lessons learned
- How the new U.S. federal trade secret law helps trade secret owners





## Illinois Employers Should Not Depend on Blue Pencil to Enforce Restrictive Covenants

By Marcus Mintz & Emily Kesler (July 31, 2017)

Illinois is one of several jurisdictions that recognizes the authority of courts to blue pencil or judicially modify otherwise unenforceable restrictive covenants to be enforceable. See, e.g. *Weitekamp v. Lane*, 250 Ill. App. 3d 1017, 1028, 620 N.E.2d 454, 462 (4th Dist. 1993) (affirming judicial modification of 300-mile non-compete to specific county); *Arpac Corp. v. Murray*, 226 Ill. App. 3d 65, 80, 589 N.E.2d 640, 652 (1st Dist. 1992) (affirming the circuit court's modification of restrictive covenant when it was modified "only slightly" and holding that the balance of the restrictions were reasonable and necessary to protect Arpac's legitimate business interests).

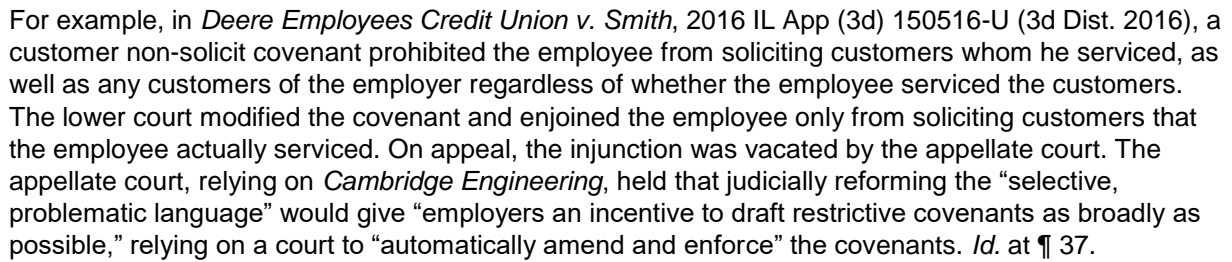


Recent reported decisions, however, cast doubt on the availability of judicial modification in all but exceedingly limited circumstances. In the past three years, only a handful of cases even mentioned judicial modification and, of those cases, not one actually modified, or affirmed the modification of, an otherwise unenforceable covenant. See *AssuredPartners, Inc. v. Schmitt*, 2015 IL App (1st) 141863, ¶ 52 (2015) (refusing to modify restrictive covenants because "deficiencies too great to permit modification"); *Bankers Life & Cas. Co. v. Miller*, No. 14 CV 3165, 2015 WL 515965, at \*3 (N.D. Ill. Feb. 6, 2015) (deciding choice of law, noting that "Illinois courts are circumspect in their modification" and that "Illinois courts look skeptically at modifications, and may modify covenants only after ensuring that fairness is not harmed"); *Fleetwood Packaging v. Hein*, No. 14 C 9670, 2014 WL 7146439, at \*9 n.7 (N.D. Ill. Dec. 15, 2014) (rejecting a proposed modification that would create a durational limitation where none existed before, noting that "[e]ven when courts have found judicial reformation to be warranted, the challenged restrictive covenants needed only slight modification to become reasonable").

The current trend is largely based on the public policy considerations articulated in *Cambridge Engineering, Inc. v. Mercury Partners 90 BI, Inc.*, in which the First Appellate District, in dicta, refused to modify otherwise unenforceable restrictive covenants because it would encourage employers to draft overly broad restrictive covenants:

Such reformation, if permitted by courts, would give employers an incentive to draft restrictive covenants as broadly as possible, since the courts would automatically amend and enforce them to the extent that they were reasonable in the particular circumstances of each case. This could have a severe chilling effect on employee posttermination activities; an employee unschooled in the law cannot be expected to know to what extent such a covenant is enforceable, particularly since courts apply a multifactor reasonableness standard instead of a bright-line rule. Thus it is possible that under such a regime, an intentionally overbroad covenant could end up tying an employee's hands for years although a majority of courts would find it unreasonable on its face. Hardship to employees is one significant factor to consider in determining the propriety of a restrictive covenant.

378 Ill. App. 3d 437, 456, 879 N.E.2d 512, 529 (1st Dist. 2007).



The take away to employers in Illinois is to not depend on judicial modification to save overly broad restrictive covenants. Restrictive covenants should be narrowly tailored to only prohibit activity that threatens an employer's legitimate business interests (confidential information and/or customer relationships) and no broader. Employers are advised to frequently review their existing agreements with their legal counsel to make sure the agreements remain enforceable.

# Trading Secrets



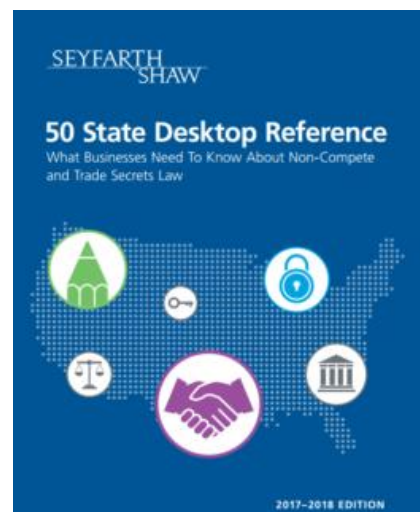
## Now Available! 2017-2018 Edition of the Trade Secrets and Non-Competes 50 State Desktop Reference

*By Seyfarth Shaw LLP (August 4, 2017)*

### 50 State Desktop Reference: What Businesses Need to Know About Non-Compete and Trade Secret Law

It has been an extraordinary year regarding trade secret and non-compete issues. We saw more and more cases filed in federal court asserting claims under the Defend Trade Secrets Act ("DTSA") and for alleged violations of non-competes. Some states passed legislation further narrowing the use of non-compete agreements, and some media outlets, academics, and regulators have continued their criticism of such agreements. We expect over the next year, the law to continue to develop regarding the DTSA's application, definitions, scope, limitations, benefits and interpretation with regard to the immunity provisions. Our 50 State Desktop Reference is a useful guide to know how the law is currently applied in each state.

Seyfarth's Trade Secrets, Computer Fraud and Non-Competes Practice Group is pleased to provide the 2017-2018 Edition of our one-stop 50 State Desktop Reference, which surveys the most-asked questions related to the use of covenants and intellectual capital protection in all 50 states. For the company executive, in-house counsel, or HR professional, we hope this guide will provide a starting point to answer your questions about protecting your company's most valuable and confidential assets.



### How To Get Your Desktop Reference

To download the pdf of 2017-2018 Edition of the 50 State Desktop Reference, [click here](#).

To request a hard copy of the Desktop Reference, click on the button below.

**Submit Request**

# Trading Secrets



## Robert Milligan to Present “Understanding and Exploring the DTSA” CLE Webinar

*By Seyfarth Shaw LLP (August 23, 2017)*

On September 7, at 3:00 p.m. – 4:00 p.m. Eastern, Robert Milligan will present “Understanding and Exploring the DTSA” CLE webinar.

The Defend Trade Secrets Act of 2016 establishes federal jurisdiction over trade secret theft and creates a federal cause of action for trade secret misappropriation. It affords damages and injunctive relief and further allows an aggrieved party to obtain an ex parte seizure of property necessary to prevent the propagation or dissemination of a trade secret. However, the law also provides immunity for certain disclosures, such as in a court filing under seal or to a government official for the purpose of reporting a suspected violation of law. Notice of the immunity provisions must be included in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.



Drafting notification clauses to be included in employment contracts and independent-contractor agreements, and reviewing other measures by which employers, can ward off challenges to the documents’ sufficiency.

In this LIVE webcast a team of thought leaders, professionals and practitioners assembled by The Knowledge Group will help the audience understand and explore the Immunity Provisions of the DTSA. Speakers will also provide their expert thoughts and opinions concerning this significant topic.

### Key Topics

- DTSA Overview
- Federal/state jurisdiction
- Damages and attorneys’ fees
- Injunctive Relief
- *Ex parte* seizure
- Immunity Provisions



# Trading Secrets



- Notification Procedures
- Employee Contracts
- Contractor Agreements



# Trading Secrets



## Robert Milligan to Present Defend Trade Secrets Act Webinar

*By Seyfarth Shaw LLP (October 24, 2017)*

Robert Milligan, along with Certified Forensic Computer Examiner Jim Vaughn, is presenting *The Defend Trade Secrets Act – The Biglaw Partner and Forensic Technologist Perspective* webinar for Metropolitan Corporate Counsel on Thursday, November 2 at 1:00 p.m. Eastern.

On May 11, 2016, President Obama signed the Defend Trade Secrets Act (DTSA), which Congress passed on April 27, 2016. With President Obama's signature, the DTSA has now become the law of the land, and a federal civil remedy for trade secrets misappropriation now exists.



What does the passage of the DTSA mean for your company? In this webinar, you will hear from Robert Milligan, partner and co-chair of the Trade Secrets, Computer Fraud & Non-Competes practice group at Seyfarth Shaw, as well as Certified Forensic Computer Examiner Jim Vaughn of iDiscovery Solutions.

The presenters 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. They 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. You will also learn about digital forensics and how the preservation and analysis of workstations, networks, cloud storage, external devices and other data storage areas can help you in your investigation.

The panel will specifically address the following topics:

- Brief history of the DTSA
- What does the DTSA provide?
- Provisions unique to the DTSA
- DTSA's whistleblower immunity provision
- DTSA's notice requirements for agreements entered into or updated as of today
- Where to start with digital forensics



# Trading Secrets



- Strategies in trade secret litigation in light of the DTSA
- What should an employer or business do now?

This is the final installment of the 2017 four-part program, The Director's Series – Essential Litigation Webinars, produced by Law Business Media, publishers of Metropolitan Corporate Counsel, In-House Tech and In-House Ops.

# Trading Secrets



## Federal Court Rules Against Calzone Franchisor in Meaty Lawsuit Against Former Franchisee

*By Erik Weibust & Anne Dunne (December 14, 2017)*

In a meaty decision involving the intersection of restrictive covenant and franchise law, the United States District Court for the Southern District of Ohio recently denied a request by D.P. Dough Franchising, LLC (“D.P. Dough”), a calzone restaurant franchisor known for late night delivery in college towns across the nation, to enjoin its former franchisee, Edward Southworth, from operating a series of Eddie’s Calzones shops in Athens, Georgia, and Columbia, South Carolina—where D.P. Dough did not even have locations at the time.



D.P. Dough asserted six different causes of action against the defendant, including (1) breach of the franchise agreement, (2) misappropriation of trade secrets, (3) copyright infringement, (4) trademark infringement, trade dress infringement, Ohio Deceptive Trade Practices Act and unfair competition, (5) tortious interference with prospective of contractual business relationships, and (6) unjust enrichment.

In holding that D.P. Dough had failed to establish a likelihood of success on the merits, the court noted that Southworth operated his D.P. Dough franchise for more than two years without a franchise agreement; as such, he was not bound by the disclosure requirements contained within. With respect to the trade secrets claim, the court held that the recipes were posted on the wall of each D.P. Dough location and employees were not required to sign non-disclosure agreements. Additionally, the court held that the Ohio Deceptive Trade Practices Act preempted the claims for tortious interference with prospective or contractual business relationships and unjust enrichment.

The court next held that D.P. Dough failed to establish that it would suffer irreparable harm if defendant was allowed to continue to operate its shops in Athens and Columbia, because there is no D.P. Dough location within 60 miles of the Columbia shop, and Southworth had opened his Eddie’s Calzones shop in Athens before D.P. Dough later opened a competing restaurant. In addition, Eddie’s Calzones had removed any potentially infringing content from its menu in Athens prior to the D.P. Dough location’s opening, thereby mitigating any danger of confusion. The court held that with respect to the Athens market, any harm suffered by D.P. Dough would be the result of normal competition, not violation of the franchise agreement.

Third, the court concluded that Eddie’s Calzones would suffer harm if the injunction issued. Specifically, Eddie’s Calzones has approximately 35 employees who would likely lose their jobs.

Finally, the court determined that while the public has an interest in the enforcement of reasonable restrictive covenants, its interests are also served by fair competition.

This decision illustrates that even outside of the employment context, courts will only enforce restrictive covenants that are reasonably tailored to protect legitimate business interests.



## Legislation

# Trading Secrets



## Will the Massachusetts Legislature Finally be Able to Keep Its New Year's Resolution to Pass Non-Compete Reform?

*By Katherine Perrelli, Erik Weibust, Dawn Mertineit & Andrew Stark (January 25, 2017)*

Last Friday, on January 20, 2017, the Massachusetts Legislature began its annual tradition of attempting to promulgate non-compete and trade secret reform in the Commonwealth. A [new bill](#) has been filed by the same legislators who began this process back in 2009, Senator William Brownsberger and Representative Lori Ehrlich, which brings many of the past proposals to the table with some new additions as well. As we reported in [July](#) and [November](#), the House and the Senate were unable to bridge their differences and agree on a compromise bill in 2016.



The bill seeks to adopt much of the Uniform Trade Secrets Act. In addition, it would formally recognize the inevitable disclosure doctrine, providing that “threatened misappropriation may be enjoined upon principles of equity, including, but not limited to, consideration of party conduct before or after commencement of litigation and circumstances of potential use, upon a showing that information qualifying as a trade secret has been, or inevitably will be, misappropriated.”

On the non-compete side, the bill notably limits non-competes (with some exceptions) to a duration of one year from the date of termination, requires that the employee receive the non-compete prior to a formal offer of employment or two weeks prior the commencement of the his or her employment, and requires consideration beyond continued employment for post-hire non-competes. The bill also requires courts to apply the bright-line “red pencil” approach if the non-compete agreement fails to satisfy any of bill’s requirements, but grants courts the discretion to reform or otherwise revise an agreement to comply with certain safe harbors set forth in the bill.

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:

- An agreement must expressly state that the employee has the right to consult with counsel prior to signing;
- Employers must review all non-competes with their employees at least once every three years for them to remain valid and enforceable;
- For post-hire non-competes, notice must be given at least ten days before the agreement becomes effective;

# Trading Secrets



- If the employee has breached his or her fiduciary duties, or taken property of the employer, the duration of the non-compete may be extended to two years;
- A geographic reach of any non-compete is that is limited to “areas in which the employee, during any time within the last 2 years of employment, provided services or had a material presence or influence is presumptively reasonable”;
- A restriction that “protects legitimate business interest and is limited to only the specific types of services provided by the employee at any time during the last 2 years of employment is presumptively reasonable”;
- Employers have ten days after the termination of employment to “notify the employee in writing by certified mail of the employer’s intent to enforce the noncompetition agreement.” If the employer fails to do so, the non-compete is deemed waived by the employer. That being said, this requirement does not apply if the employee has unlawfully taken the employer’s property or already breached the non-compete, a non-solicit, an anti-piracy/no-raid covenant, a confidentiality agreement, or a fiduciary duty;
- Non-compete agreements would not be enforceable against (1) employees who are not exempt under the Fair Labor Standards Act, 29 U.S.C. §§ 201-209, (2) undergraduate or graduate students engaged in short-term employment, (3) employees terminated without cause or laid off, (4) employees who are 18 or under, and (5) non-employees who perform services for less than one year; and
- If the employee is a resident of, or has been working in, Massachusetts for at least thirty days immediately prior to the termination, Massachusetts law will apply, rendering any out-of-state choice of law provision unenforceable.

Notably absent from the bill is the inclusion of a provision requiring “garden leave,” forcing employers to pay former employees bound by non-compete agreements fifty percent of their highest annualized salary over the last two years of employment for the restricted period. Such a provision has appeared in many of the proposed bills in the past few years.

We will continue to monitor these developments and report back with any updates. Perhaps 2017 is the finally year for non-compete and trade secret reform in Massachusetts after all. Readers of this blog know all too well, however, that this may just be another New Year’s resolution that the Massachusetts Legislature is not able to keep.

A special thanks to our friend [Russell Beck](#) for his thoughtful analysis of, and input into, the latest proposed legislation.



# Trading Secrets



## Missouri Legislator Introduces Bill to Ban Restrictive Covenants

*By J. Scott Humphrey (April 3, 2017)*

Since July 1, 2001, Missouri law with respect to non-solicitation clauses has been fairly straightforward. Specifically, [§ 431.202 of the Missouri Statutes](#) states that a covenant not to solicit between an employer and an employee is presumed reasonable if it is no longer than one year in duration and designed to protect confidential information, customer relationships, and/or good will. Section 431.202 also states that the statute does not apply to covenants not to compete, thereby allowing the courts to decide the enforceability of a non-competition clause on a “case-by-case” basis. (Id. § 3).



A Bill, however, currently pending in the Missouri House of Representatives seeks to abolish Missouri’s non-solicit statute and ban all restrictive covenants except for those restrictive covenants found in a “business to business” setting. Specifically, House Bill 479, introduced by Representative Keith Frederick (R), seeks to eliminate all types of restrictive covenants (non-compete, non-solicit, and non-hire) except when the restrictive covenants involve the sale of a business or are between two corporations engaged in a joint venture. [The Bill](#) would go into effect August 28, 2017. Thus, any restrictive covenant agreement between an employer and an employee that is a) controlled by Missouri law and b) entered into after August 28, 2017, would be unenforceable.

In addition to House Bill 479, a recent Federal Court decision in the Eastern District of Missouri also has the attention of non-compete lawyers. In [Durrell v. Tech Electronics, Inc.](#), plaintiff Robert Durrell brought suit against his former employer, Tech Electronics, Inc., alleging that he was wrongfully terminated and retaliated against for taking FMLA leave. Durrell’s Complaint further alleges that the restrictive covenants found in his Employment Agreement are unenforceable due to a lack of consideration. The Court denied Tech’s Motion to Dismiss Durrell’s restrictive covenant claims by ruling that at-will employment is “not a source of consideration under Missouri contract law.” Notably, the Court did not address § 431.202’s specific language that a non-solicitation clause is enforceable if it protects confidential information, customer relationships, and/or good will. In fact, the Court does not even mention § 431.202 in its opinion. (Probably because the Court was only asked to address whether “at-will employment” is sufficient consideration for enforcing a restrictive covenant).

We will continue to monitor House Bill 479 (the Bill is currently in “Executive Session”) as well as the Durrell case, and will provide all relevant updates on this blog.



# Trading Secrets



## Massachusetts Legislature Schedules Hearing on Non-Compete Reform

*By Katherine Perrelli, Erik Weibust & Andrew Stark (October 3, 2017)*

The Massachusetts legislature is back at it again. Under new leadership, the Joint Committee on Labor & Workforce Development recently scheduled a hearing for October 31, 2017 on the non-compete reform bills proposed in January of this year. While we know little about the hearing, the bills to be discussed are presumably Senate Bill S.988 and companion House Bill H.2366. These identical bills were filed in January 2017 by the same legislators who began this process back in 2009, Senator William Brownsberger and Representative Lori Ehrlich.



As we previously [reported](#), the proposed law brings many past proposals to the table with some new additions as well. We also reported in [July](#) and [November](#) of 2016 that the House and the Senate were unable to bridge their differences and agree on a compromise bill that year. For a detailed overview of the bills likely to be discussed in the upcoming hearing, please see our prior [report](#).

We will continue to monitor these developments and report back with any updates. Perhaps 2017 is finally the year for non-compete and trade secret reform in Massachusetts after all. Readers of this blog know all too well, however, that this may just be another of the many attempts that the Massachusetts Legislature is unable to see through to its fruition.



# Trading Secrets



## International

# Trading Secrets



## \$1.2 Million Dispute Between West Mountain Environmental and the Shanghai Hehui Environmental Technology

By Wan Li, Robert B. Milligan & Craig B. Simonsen (April 5, 2017)

**Seyfarth Synopsis:** An environmental remediation technologies company is in the midst of litigation in Chinese courts over a \$1.2 million contract to provide its technology to a Chinese company. According to the Chinese entity, the technology provider failed to deliver the unit in a “timeframe that was agreed.”

The West Mountain Environmental Corp. (WMT) had issued a [press release in October 2016](#) that it had sold its first indirect thermal desorption technology (TPS) unit in China to Shanghai Hehui Environmental Technology, Co. Ltd. (Hehui). WMT valued the contract at approximately \$1.2 million.



Historically, WMT had operated in China since 2012 and has treated, it claims, over 100,000 tons of contaminated soil and oil sludge using TPS technology. TPS’ patented indirect thermal desorption technology is “recognized in the industry as one of the most efficient and safest technologies for the removal of hazardous contaminants.” WMT asserts that TPS was one of the first western environmental remediation technologies successfully transferred to China which has been recognized as a top 100 environmental technology in the 3iPET Program supported by the Ministry of Environmental Protection.

This sale, WMT indicated, represented the first time that TPS technology had been used as part of a process to treat waste purified terephthalic acid (PTA) sludge. “PTA is required for the manufacture of polyester fibre, polyethylene terephthalate (PET) bottle resin and polyester film and China is the largest producer of PTA at over 50 million tonnes per year.”

Now according to a recent [WMT press release](#), it received notice that a lawsuit had been filed against it by Hehui, claiming that WMT failed to deliver the TPS unit in a “timeframe that was agreed.” As a consequence, a Chinese Court ordered that WMT’s bank accounts be frozen until a hearing is held on March 27, 2017, in Shanghai.

Subsequently WMT was informed by its Chinese legal counsel that its motion to remand its contract dispute with Hehui to arbitration in conformance with the terms of the contract between the parties was denied. The [release](#) indicated that Chinese Intermediate Court ruled that as the contract between the parties did not specify an arbitrator, so the Intermediate Court would hear the case. As a result of the ruling and based on the recommendation from Chinese legal counsel, WMT will file an objection of jurisdiction to the Intermediate Court on April 5, 2017, at which time an official hearing for the case will be set.



# Trading Secrets



This case illustrates how very careful parties need to be in preparing contracts, especially in international cases. Deals in China may be especially complicated as the law varies in different provinces.

For more information on this or any related topic please contact the authors, your Seyfarth attorney, or any member of the [International Employment Law Team](#), the [Intellectual Property](#), or the [Trade Secrets Teams](#).

# Trading Secrets



## Robert Milligan to Present “Effective Use of Non-Compete Agreements by International Employers” Webinar

*By Seyfarth Shaw LLP (July 10, 2017)*

Robert B. Milligan, Seyfarth Partner and Co-Chair of the Trade Secrets, Computer Fraud & Non-Competes Practice Group, will be a speaker for the “Effective Use of Non-Compete Agreements by International Employers” webinar presented by Practising Law Institute (“PLI”) on August 10, 2017 at 1:00 p.m. Eastern.

Multi-national employers often find that the appropriate use of non-compete agreements provides a business advantage in the marketplace. Companies often struggle however in implementing a consistent strategy and approach, particularly with the challenges presented by a mobile workforce and continual changes in applicable law. Please join us for an informative presentation by two leading employment lawyers who specialize in formulating non-compete strategies for multi-national employers.



Robert B. Milligan of Seyfarth Shaw LLP and Yvonne Gallagher of Harbottle & Lewis LLP will cover the following topics:

- Creating and maintaining a comprehensive non-compete strategy
- Solutions for addressing the continual changes in applicable law through choice of law, forum, and arbitration provisions
- Discussion of applicable law in key forums and recent developments in United States and Europe
- Integrating non-compete strategy with trade secret and confidential information protections





# Trading Secrets



## Social Media and Privacy



## WannaCry Ransomware Attack: What Happened and How to Address

*By Richard Lutkus, EnCE, EnCEP, CEH (May 15, 2017)*

*Cross Posted from [Carpe Datum Law](#)*

Recently, a widespread global ransomware attack has struck hospitals, communication, and other types of companies and government offices around the world, seizing control of affected computers until the victims pay a ransom. This widespread ransomware campaign has affected various organizations with reports of tens of thousands of infections in as many as 99 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as *WannaCry*, *WCry*, or *Wanna Decryptor*, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly.

The risk posed by this ransomware is that it enumerates any and all of your “user data” files like Word, Excel, PDF, PowerPoint, loose email, pictures, movies, music, and other similar files.. Once it finds those files, it encrypts that data on your computer, making it impossible to recover the underlying user data without providing a decryption key. Also, the ransomware is persistent, meaning that if you create new files on the computer while it’s infected, those will be discovered by the ransomware and encrypted immediately with an encryption key. To get the decryption key, you must pay a ransom in the form of Bitcoin, which provides the threat actors some minor level of anonymity. In this case, the attackers are demanding roughly \$300 USD. The threat actors are known to choose amounts that they feel the victim would be able to pay in order to increase their “return on investment.”

The ransomware works by exploiting a vulnerability in Microsoft Windows. The working theory right now is that this ransomware was based off of the “EternalBlue” exploit, which was developed by the U.S. National Security Agency and leaked by the Shadowbrokers on April 14, 2017. Despite the fact that this particular vulnerability had been patched since March 2017 by Microsoft, many Windows users had still not installed this security patch, and all Windows versions preceding Windows 10 are subject to infection.

The spread of the malware was stemmed on Saturday, when a “kill switch” was activated by a researcher who registered a previously unregistered domain to which the malware was making requests. However, multiple sources have reported that a new version of the malware had been deployed, with the kill switch removed. At this time, global malware analysts have not observed any evidence to substantiate those claims.

### **You should remain diligent and do the following:**

- Be aware and have a security-minded approach when using any computer. Never click on unsolicited links or open unsolicited attachments in emails, especially from sources you do not already know or trust.
- Ensure that your antivirus and anti-malware are up-to-date.

# Trading Secrets



- Apply Security Updates! Enable automatic updates and reboot weekly. Systems that are receiving automatic updates should already be protected against this malware. If you aren't sure, visit <https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update>.
- Backup your data! The risk of malware is losing your data. If you perform regular backups, you won't have to worry about ransomware. Make sure you utilize a backup system that is robust enough to have versioning so that unencrypted versions of your files are available to restore. Make sure your backup system isn't erasing your unencrypted backups with the encrypted ones!

**If your organization is the victim of a ransomware attack, please contact law enforcement immediately.**

- Contact your [FBI Field Office Cyber Task Force](#) immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
- Report cyber incidents to the US-CERT and [FBI's Internet Crime Complaint Center](#).



## ABA Encourages Encryption of Emails When Transmitting Confidential Client Information

*By Erik Weibust & Andrew Stark (May 22, 2017)*

In a [recent formal Ethics Opinion](#), the American Bar Association stressed that lawyers must make reasonable efforts to prevent inadvertent or unauthorized access to confidential information relating to the representation of their clients. The ABA recognized that in the age of constant cybersecurity threats, law firms are targets for hackers for two reasons:



- (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

The Opinion further recognizes that while the Model Rules of Professional Conduct do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with his or her client, electronic communication involves risks that are constantly changing.

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

- (1) The sensitivity of the information;
- (2) The likelihood of disclosure if additional safeguards are not employed;
- (3) The cost of employing additional safeguards;
- (4) The difficulty of implementing the safeguards; and
- (5) The extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

When making these reasonable efforts to safeguard electronic communications and storage, Model Rule 1.4 may require the lawyer to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of



# Trading Secrets



the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. The Opinion stresses that reasonable efforts might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as the ABA stressed avoiding the use of the telephone, fax and mail in its 1999 Formal Opinion 99-413.

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



## Technically Speaking, Cybersecurity Isn't About Speaking Technically

*By Guest Author for TradeSecretsLaw.com (July 6, 2017)*

*As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Charlie Platt, a director at iDiscovery Solutions and a Certified Ethical Hacker. He advises clients on data analytics, digital forensics, and cybersecurity.*



These days cybersecurity seems to be all about technology. Pen testing, firewalls, port scanning, SIEM, zero-day, IPS, AES256, SHA, DMZ, NIDS, TLS, SS7 – I'll stop. I could go on, but you get the idea. And I have a vested interest in keeping your attention.

Acronyms and geek-speak abound, and we are ever on the lookout for the next latest and greatest technical solution to secure our digital assets. Unfortunately, that perfect technical solution doesn't exist and never will. How can I be so sure? Because no matter how well built, or how well thought out our technical solution may be, humans are involved. When humans are involved, they will be the weakest link, and we can't (yet) re-engineer humans with a technical solution.

How do most attacks happen? Despite what movies and TV would have you believe, it's not legions of hackers actively pounding down our cyber doors. Most successful attacks happen because a person did something: they made a mistake, clicked a link, visited a suspicious website or plugged in an infected USB device. They were naïve or unaware of the damage that could arise from their actions and let their guard down. Which brings us to the theme of this column. Cybersecurity isn't about speaking technically; it's about communication.

We, as representatives of our organizations, must have a vested interest in security, and we should be communicating with our co-workers and peers about it. The clarity and simplicity of those communications are vital to our maintaining a secure environment; acronyms and technical jargon only serve to confuse and alienate the very audience we are trying to reach.

And about that audience? Earlier I said we can't re-engineer humans, which is true, but, in a sense, we can re-program them. How? I know re-programming people sounds nefarious, especially in a conversation about cyber, but the answer is to educate them. We educate them by clearly and consistently communicating the risks involved in working with company data in an unsecure fashion. We explain what our expectations are, and how their actions can contribute to or detract from our efforts to control those risks. It's vital to use language that isn't technical, that doesn't alienate or confuse and that clearly outlines how they can improve security.

The security of our organizations rests with our employees. Employees can range from weak links to stalwart defenders, and it's up to us to help them move toward the "defender" role. Without proper communication, most employees won't know the critical part they play or how to change their behavior to be alert for suspicious activity – or what to do when they observe it. If our cybersecurity





# Trading Secrets



conversations always revolve around acronyms and technical jargon, our business associates and nontechnical employees will believe that security is the domain of security professionals, assume the risk is being handled by those in charge and proceed with a lack of awareness as to how they themselves may be undermining that presumed security.

Many of the cases that I have worked on over the past several years have come down to employees making mistakes, doing so with honest intentions, yet ending up subverting the security of the entire organization.

On the other side, we also need to consider post-incident response, when communications become even more critical. To paraphrase Helmuth von Moltke, no plan survives first contact. Once incident response has been engaged, communications within the organization – including security response teams, legal counsel and senior management – become critical to properly containing and responding to the event. Communications external to the organization – such as clients, contractors and the media – quickly become the public face of the event. Making sure these are clear, accurate and accessible to the appropriate audience can be the difference between a controlled event and chaos.

But that's a column for another day. For today, let's take a minute to reaffirm the importance of open and clear communications within our organizations about security and the roles we all play, as our best defense must always include education and awareness. As inside counsel, you can help by playing the role of universal translator between the technical security team and the nontechnical business units and management. Naturally speaking, all you have to do is speak naturally.

# Trading Secrets



## Webinar Recap! Protecting Trade Secrets in the Social Media Age

*By Justin K. Beyer, Dawn Mertineit & Ryan Behndleman (October 20, 2017)*

In Seyfarth's final webinar in its series of 2017 Trade Secrets Webinars, Seyfarth attorneys Justin Beyer, Dawn Mertineit, and Ryan Behndleman presented [\*Protecting Trade Secrets in the Social Media Age\*](#). The panel focused on how to define and protect trade secrets on social media.

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



- By allowing social media in the workplace, companies are exposed to multiple risks, including the theft of confidential information and potential embarrassment to the company. It is imperative that companies craft a social media policy that will not only protect the company, but will also work within the company's individual structure.
- In defining an employee's obligations as it relates to social media usage, companies should make sure they have policies in place (as well as a provision in any employment agreements) regarding the ownership of company social media accounts. Having clear, written policies and agreements can eliminate or reduce the need for costly and time-consuming litigation to determine who owns company-related social media presences.
- Finally, due to the concern about employer involvement in an employee's social media presence, employers should be mindful to abide by direction provided by state legislation as well as the National Labor Relation Board's interpretation of what constitutes improper interference in speech activities. Because of this, it is important to craft any social media policy with a view toward protecting company assets and reputation, without being perceived to infringe on the speech or privacy rights of employees.



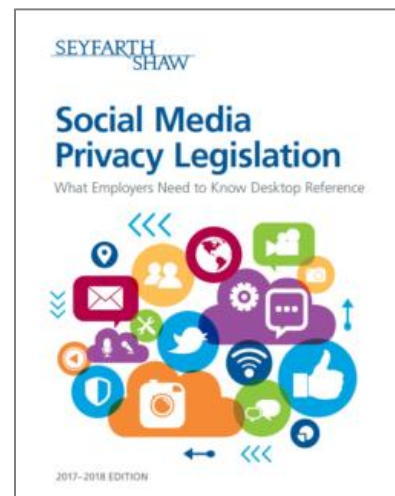
## Now Available! Seyfarth Shaw's 2017-2018 Edition of the Social Media Privacy Legislation Desktop Reference

*By Seyfarth Shaw LLP (November 20, 2017)*

There is no denying that social media continues to transform the way companies conduct business. In light of the rapid evolution of social media, companies today face significant legal challenges on a variety of issues ranging from employee privacy and protected activity to data practices, identity theft, cybersecurity, and protection of intellectual property.

Seyfarth Shaw is pleased to provide you with the 2017–2018 edition of our easy-to-use guide to social media privacy legislation and what employers need to know. The Social Media Privacy Legislation Desktop Reference:

- Describes the content and purpose of the various states' new social media privacy laws.
- Delivers a detailed state-by-state description of each law, listing a general overview, what is prohibited, what is allowed, the remedies for violations, and special notes for each statute.
- Provides an easy-to-use chart listing on one axis the states that have enacted social media privacy legislation, and on the other, whether each state's law contains one or more key features.
- Offers our thoughts on the implications of this legislation in other areas, including trade secret misappropriation, bring your own device issues and concerns, social media discovery and evidence considerations, and use of social media in internal investigations.
- Concludes with some best practices to assist companies in navigating this challenging area.



### How To Get Your Desktop Reference

To request the 2017–2018 Edition of the Social Media Privacy Legislation Desktop Reference as a pdf or hard copy, please submit a request [here](#).



## Acknowledgments:

Special thanks to Olivia Wada, Colleen Vest, and Nicole Bandemer for their work in putting together this year in review.



Atlanta

Boston

Chicago

Hong Kong

Houston

London

Los Angeles

Melbourne

New York

Sacramento

San Francisco

Shanghai

Sydney

Washington, D.C.

"Seyfarth Shaw" refers to Seyfarth Shaw LLP. Our London office operates as Seyfarth Shaw (UK) LLP, an affiliate of Seyfarth Shaw LLP. Seyfarth Shaw (UK) LLP is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with registered number 556927. Legal services provided by our Australian practice are provided by the Australian legal practitioner partners and employees of Seyfarth Shaw Australia, an Australian partnership. Our Hong Kong office "Seyfarth Shaw," a registered foreign law firm, is a Hong Kong sole proprietorship and is legally distinct and independent from Seyfarth Shaw LLP, an Illinois limited liability partnership, and its other offices.