ABA Section of Intellectual Property Law, Trade Secrets and Interferences with Contracts Committee Annual Trade Secret Law Report 2018

This 2018 edition contains contributions or assistance from the following lawyers and law students: Klaus H. Hamm, Sara J. O'Connell, Katherine E. Ruiz Díaz, Robert B. Kornweiss, Jonathan Schmalfeld, Michael Annis, Byron Brown, Michelle Browning Coughlin, Graham Matherne, Sean Williamson, Matthew M. D'Amore, Hong Zhang, Anthony C.K. Kakooza, Dillon Kellerman, Dan Matos, Jun Ho Lee, Robert Garcia, Kibum Byun, Austin Abir, Johan Dib, Stephanie Barnhart, Giancarlo Gibson, Isaac Syed, Jing Yang, Christina Huang, DJ Healey, Matthew Horowitz, James Gale, Kyle Pedraza, and Samuel Edelstein.

U.S. Supreme Court

***Food Marketing Institute v. Argus Leader Media*, 139 S.Ct. 2356 (2019).** The Supreme Court ruled for businesses seeking to maintain confidentiality of information provided to government entities who receive requests for the information under the Freedom of Information Act ("FOIA"). FOIA's Exemption 4 shields from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Abrogating *Nat'l Parks & Conservation Ass'n. v. Morton*, 498 F.2d 765, 767 (D.C. Cir. 1974), which had been followed by nearly every other court, the Supreme Court held that Exemption 4 does not require a showing of "substantial competitive harm." Instead, the Supreme Court held that Exemption 4 applies "where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy." In this case, a South Dakota newspaper, *Argus Leader*, filed a FOIA request for data collected by the United States Department of Agriculture ("USDA") about store-level annual food-stamp redemption, which retailers did not publicly disclose. Invoking Exemption 4, the USDA did not provide the data, but the district court ordered its release following a trial that determined its disclosure would not cause substantial competitive harm to participating retailers. The Food Marketing Institute, a trade association representing grocery retailers, intervened and appealed, and the Eighth Circuit affirmed. The Supreme Court reversed, holding that the plain meaning of the term "confidential" does not require a heightened showing of substantial competitive harm, and criticized the D.C. Circuit's approach of relying on legislative purpose and history to impose this requirement when the plain meaning of the law yielded a clear statutory interpretation.

1st Circuit

***Maine Pointe, LLC v. Collins*, 2018 WL 5303038 (D. Mass. 2018) (unpublished)**. Maine Pointe, a global supply chain and operations firm, sought damages and injunctive relief against Collins and MTC International Consulting for improper download of Maine Pointe's confidential information after Collins's resignation as a Maine Pointe consultant. Maine Pointe claimed Collins misappropriated confidential client information and Maine Pointe guide books from a password protected Dropbox account he had access to when working for Maine Pointe. Due to the nature of this type of Dropbox account, any information accessible to Collins through the account is destroyed once the user unlinks his personal computer. While the court held that Maine Pointe could be able to establish that the allegedly misappropriated information qualified as a trade secret under Massachusetts law, it nonetheless denied the request for preliminary injunction because Maine Pointe failed to establish the other elements necessary to obtain injunctive relief.

***Ooyala, Inc. v. Dominguez*, 2018 WL 3360759 (D. Mass. 2018) (unpublished)**. Ooyala is a California-based technology company that markets cloud-based video platform services and products which allow customers to curate, publish, monetize, measure and analyze video content on electronic devices. Defendant Brightcove, a Massachusetts company, is the leading provider of the cloud-based video services and Ooyala's biggest competitor. Ooyala brought trade secret misappropriation claims under Massachusetts and federal law against Brightcove and several individuals. Seeking employment from Brightcove, Defendant Perez-Real (a then-Ooyala employee) sent emails to Defendant Garcia-Dominguez (a Brightcove employee and former Ooyala employee), containing current Ooyala client contracts, Ooyala strategies for competing with Brightcove, communications with prospective customers, salesforce reports, and client lists.

Brightcove claimed that the information was too vague to be of use, and that the various customer lists with contact information were not secret because the individuals has publicly accessible LinkedIn profiles listing their job titles and places of employment. The district court disagreed, and enjoined Brightcove from using or disclosing the information. The court also ordered Brightcove to return or cease to retain any and all information that originated or was derived from these emails. Finally, the court ordered Brightcove to refrain from communicating with any of the 22 companies identified by Ooyala, where the contact was based on information included in or derived from the emails from Perez-Real.

***Pawelko v. Hasbro, Inc.*, 2018 WL 6050618 (D.R.I. 2018) (unpublished), *report and recommendation adopted,* 2019 WL 259117 (D.R.I.) (unpublished)**. Pawelko claimed to be the inventor of an original, innovative crafting product and idea known as "Liquid Mosaic," which she submitted to Hasbro, Inc. after signing a non-disclosure agreement. After a conference call presentation that included a five-page slide deck and three sample craft projects, Hasbro passed on the idea. Pawelko claims Hasbro misappropriated her idea submission and used it to develop Play Doh Plus and DohVinci, two new product lines that incorporated elements and features of "Liquid Mosaic." Pawelko sued *inter alia* for state and federal trade secret misappropriation. The district court granted in part and denied in part Hasbro motion for summary judgment. The district court granted summary judgment against the federal Defend Trade Secrets Act ("DTSA") claim because the relevant activity took place prior to the DTSA's effective date. Following *Attia v. Google, LLC*, 2018 WL 2971049 (N.D. Cal. 2018), the court deemed that Pawelko's "continuing use" theory fails as a matter of law because her claim was based on current use of alleged trade secrets disclosed via patent applications and product sales by Hasbro prior to the DTSA's enactment. However, the district court denied summary judgment against Pawelko's state trade secrets claim, holding a genuine issue of material fact existed about whether "Liquid Mosaic" was entitled to trade secret protection when Pawelko had allegedly previously disclosed it through craft show submissions, blogposts, YouTube videos and online interviews.

***TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, 2018 WL 4677451 (D.P.R. 2018) (unpublished)**. TLS brought an action against Rodriguez-Toledo and others for, *inter alia*, violation of the Industrial and Trade Secret Protection Act of Puerto Rico and the Defend Trade Secrets Act. TLS stored information about its tax strategies, insurance strategies, customer lists, and other confidential information on a Dropbox business account, for exclusive employee use. Before resigning his position at TLS and working with a TLS competitor, Rodriguez-Toledo transferred confidential documents, including a template of TLS's operating agreement and a Capital Preservation Report ("CPR"), from TLS's Dropbox account. After a non-jury trial, the court held that TLS proved that defendants had violated the both state and federal legislation by misappropriating TLS's CPR.

2nd Circuit

***AUA Private Equity Partners, LLC v. Soto*, 2018 WL 1684339 (S.D.N.Y. 2018) (unpublished).** The plaintiff, a private equity firm that specializes in leveraged and management buyouts, hired the defendant as the vice president of business development and investor relations. The defendant's contract with the plaintiff contained a confidentiality provision and an acknowledgment of the supervisory procedures and compliance manual, which prohibited employees from using any outside communications network. Anticipating her termination, the defendant uploaded

proprietary company files from her laptop to her personal Google account, and then deleted the files from the laptop. The plaintiff performed a forensic search of the defendant's laptop and found the emails she had moved to a personal email. The defendant had collected: investor reports, investor contact information, investor commitment amounts, and other confidential documents. The plaintiff sued under the Defend Trade Secrets Act ("DTSA"), and for breach of contract. The defendant filed a motion to dismiss the complaint arguing the plaintiff failed to sufficiently plead that the defendant used or disclosed the plaintiff's trade secrets. However, the court noted that the complaint survives a motion to dismiss if it plausibly pleads an improper *acquisition* of trade secrets. Finding no definition of "acquisition" in the DTSA, the court considered Black's Law Dictionary definition of "acquisition," as gaining possession or control. The court then held the complaint sufficiently plead that prior to uploading the trade secrets the defendant did not have possession or control of them but had access to them; in other words, she had not acquired them by proper means during her employment.

***Duffy v. Ill. Tool Works Inc.*, 2018 WL 1335357 (E.D.N.Y. 2018) (unpublished)**. Plaintiff Duffy brought a class action against Defendants Illinois Tool Works, Inc. and South/Win Limited, alleging state-law causes of action for products liability, negligence, and deceptive business practices. Plaintiff claimed that Defendants Rain-X windshield wash damaged certain windshield washer systems, including his own. Plaintiff filed a motion to compel seeking the formula for Rain-X and the contact information of Rain-X purchasers who complained about the product. The court applied New York substantive law and found that the formula was a trade secret but held that limited disclosure was warranted because plaintiff's expert could not identify the key ingredient in Rain-X production bottles alone, and because reverse-engineering the Rain-X formula would be costly and introduce error. The court granted the portion of the plaintiff's motion seeking the formula for Rain-X and directed the parties to submit a modified Stipulated Protective Order restricting access to the formula solely to plaintiff's counsel and plaintiff's expert. The court denied the portion of plaintiff's motion seeking the unredacted contact information of complaining Rain-X consumers. The court found that the privacy interests of third parties and lack of relevance of the contact information justified denying the request.

***Elsevier Inc. v. Doctor Evidence, LLC*, 2018 WL 557906 (S.D.N.Y. 2018) (unpublished).** Elsevier and Doctor Evidence ("DRE") entered into a contract under which DRE agreed to use its proprietary software to perform data analysis for Elsevier. The parties entered into a confidentiality agreement and a nondisclosure agreement pursuant to the contract. Elsevier brought a breach of contract claim against DRE, and DRE counterclaimed for misappropriation of trade secrets under the Defend Trade Secrets Act ("DTSA") and New York law. The court dismissed DRE's trade secret misappropriation claims because it failed to adequately allege the existence of a trade secret, instead conflating the concept of a "trade secret" with "confidential information." The court found that the nine general categories of confidential information that DRE asserted as trade secrets lacked sufficient specificity to "plausibly support the existence of a true trade secret," and that the pleading failed to include supportive allegations such as the value and secrecy of the claimed trade secrets. Even DRE's most specific assertion (its ontology process and tools) was rejected because DRE did not address the details of the "unique and proprietary process" nor sufficiently allege its value or secrecy. While acknowledging that the confidentiality agreement and the nondisclosure agreement manifested DRE's efforts to protect information, the court nonetheless held that the agreements alone were not enough to suggest the existence of a bona fide trade secret.

***In re Avaya Inc.*, 2018 WL 1940381 (Bankr. S.D.N.Y. 2018) (unpublished)**. Avaya is a technology company which produced a centralized media server called Getaway. The Getaway contains one or two power supply units ("PSUs"). Avaya started purchasing the PSUs from SAE Power Company, but then contracted with a new supplier, Delta, for the purchase of PSUs at a lower price. SAE filed suit against Avaya in New Jersey state court, alleging, among other things, misappropriation of trade secrets. Subsequently, Avaya filed for chapter 11 bankruptcy, automatically staying the New Jersey litigation. The Bankruptcy Court was tasked with estimating the SAE claims for reserve purposes and applied a reasonable royalty measure. The parties agreed that the court should use the 15 *Georgia-Pacific* factors used in patent cases. The court determined that apportionment based on cost was appropriate and that the cost of the components attributable to the trade secrets was only 6.3% of the cost of the entire SAE PSU. Furthermore, the court found that damages are appropriate only for the period of time during which the trade secret remained a secret, measured by the time it would have taken the defendant to obtain the information by proper means such as reverse engineering or independent development. Looking at other factors, the trade secrets were neither technically unique nor critical to the SAE PSU in that a PSU which does not incorporate SAE's trade secrets would have essentially the same abilities and uses. More generally, Avaya offered expert testimony to establish the availability of alternative PSUs, the time and expense required to reverse engineer or develop a PSU de novo, and the portion of the price difference between the SAE PSU and the Delta PSU attributable to the trade secrets. Consequently, the court estimated the misappropriation claim at $1.2 million, a fraction of the damages sought by SAE.

***Medidata Sols., Inc. v. Veeva Sys.*, 2018 WL 6173349 (S.D.N.Y. 2018) (unpublished).** Plaintiff software company Medidata Solutions, Inc. provides solutions for pharmaceutical companies to design, manage and evaluate clinical trials through a product called "CTMS." Defendant Veeva Systems allegedly hired many of Medidata's former high-level employees; including the former senior product manager, vice president of product strategy and executive president of field operations. Prior to their departure, Medidata's former employees allegedly emailed sensitive company data to their personal emails. Many of these documents were labeled "Private and Confidential." In 2016, when Veeva announced their competitor software to Medidata's CTMS program, Medidata sued Veeva under the Defend Trade Secrets Act ("DTSA") and New York State law for misappropriation of trade secrets. Veeva moved to dismiss, which the court denied. The court highlighted the claim that former Medidata employees accessed private and confidential files while still employed and retained them upon joining Veeva. Additionally, the court stressed the allegation that certain former Medidata employees were rewarded "outsized" compensation packages by Veeva to induce those former Medidata employees to violate their confidentiality agreements. The court also noted numerous allegations of acquisition, disclosure and use by Veeva, including disclosures to prospective clients and partners and rapidly deploying software that competed with Medidata.

***Next Commc'ns, Inc. v. Viber Media, Inc.*, 758 F. App'x 46 (2d Cir. 2018) (unpublished).** Next Communications, Inc., and NextGn, Inc. (collectively, "Next") provide long-distance data services for telecommunications carriers. Defendant Viber Media, Inc. makes a popular mobile voice over internet protocol application. Next sued Viber for misappropriating Next's trade secrets proprietary information. After limited discovery, the court granted summary judgment in favor of Viber holding that Next had failed to state the nature of the allegedly secret technology with sufficient particularity under New York state law. The Second Circuit affirmed the district court's

judgment by observing that under New York law, a party must describe the trade secret with "specific and concrete information." In particular, the Second Circuit noted that Next has described its trade secrets differently at each stage of the litigation and failed to describe with particularity any of the mechanisms of its HD Video Cloud Architecture. Furthermore, a PowerPoint slide with unsophisticated graphics, vague labels, and concepts was not specific enough to describe the trade secret with particularity.

***Phoenix Ancient Art, S.A. v. J. Paul Getty Tr.*, 2018 WL 1605985 (S.D.N.Y. 2018) (unpublished).** Phoenix Ancient Art, S.A., Petrarch LLC A/K/A Electrum, and Regulus International Capital Corp. (collectively, "Plaintiffs"), sued J. Paul Getty Trust, the J. Paul Getty Museum, and Timothy Potts (collectively, the "Getty Defendants"), and Livio Russo and Arturo Russo (collectively, the "Russo Defendants"), asserting, inter alia, a trade misappropriation claim under the Defend Trade Secrets Act ("DTSA"). Between summer 2010 and fall 2015, plaintiffs worked to broker a sale of the Torlonia Family's world-famous collection of classical sculptures ("Torlonia Collection"). Plaintiffs alleged that upon being asked by the Russo Defendants to find a buyer for the Torlonia Collection, they engaged in extensive efforts to create an updated English catalogue of the Torlonia Collection. After numerous discussions regarding the Torlonia Collection with the Getty Defendants, who also signed a nondisclosure agreement with plaintiffs, plaintiffs developed and proposed a customized deal structure to minimize the political risks of the sale because the Torlonia Collection is highly valued by the Italian nation. Plaintiffs alleged that the Getty Defendants and the Russo Defendants, after misappropriating the "trade secret" catalogue and deal structure, cut plaintiffs off before concluding the deal to avoid paying their commission. The Getty Defendants moved to dismiss the DTSA claim against them. The Court granted the motion. The court first noted that the DTSA applies only to acts of misappropriation on or after May 11, 2016, the effective date of the Act, and that the parties agreed that the acquisition or use of the alleged trade secrets occurred before the effective date of the DTSA. Then the court agreed with the Getty Defendants that plaintiffs' claim, that the Getty Defendants have concealed plaintiffs' trade secrets by refusing to return the updated catalogue after May 11, 2016, is actionable under only the DTSA's criminal provision, holding there is no private right of action to enforce the DTSA's criminal provision and that a "concealment" theory cannot support a civil claim. Therefore, the court granted the motion to dismiss plaintiffs' DTSA claim.

***Saniteq, LLC v. GE Infrastructure Sensing, Inc.*, 2018 WL 4522107 (E.D.N.Y. 2018) (unpublished), *report and recommendation adopted*, 2018 WL 4357475 (E.D.N.Y. 2018) (unpublished).** Plaintiff Saniteq, LLC, is a research and development company focused on ultrasonic flowmeters which measure the speed and flow of liquids and gases within industrial pipes. Defendant GE Infrastructure Sensing, Inc. ("GEIS") manufactures, sells and distributes similar products. The parties entered into a nondisclosure agreement regarding the development of commercial flowmeters. Based on this relationship, Dennis Diorio was employed as an independent consultant by Saniteq until March 2015 and then moved on to consult for GEIS until November 2015. Saniteq alleges that trade secrets were misappropriated from the discussions and through Diorio's consultancy work for both parties. After filing suit, GEIS discovered that Diorio had retained his GEIS laptop until April 2016 and that it contained references to Saniteq trade secrets. However, there was no evidence of access to the trade secrets after May 11, 2016 (the effective date of the Defend Trade Secrets Act ("DTSA") nor, more broadly, any evidence of use at all. GEIS moved for summary judgment. On the DTSA claim, the court held that concealment of a trade secret after the DTSA's effective date does not create a private right of action and

emphasized that there was no indication that Congress intended to provide a private right of action under the DTSA for concealment of a trade secret. On the trade secrets claim under New York common law, the court focused on whether GEIS used trade secrets belonging to Saniteq and pointed out that Saniteq failed to show any "suspicious similarity" of GEIS' products to Saniteq's, and also that there was no evidence of use of the trade secret information on the GEIS-Diorio laptop.

***Universal Processing, LLC v. Zhuang*, 2018 WL 4684115 (S.D.N.Y. 2018) (unpublished).** Defendant Zhuang worked at Plaintiff Universal Processing. As a marketing associate, Zhuang had access to confidential information including marketing information, financial information, client lists, business models, pricing formulas, customer data and social media sites, and applications with specific Universal usernames and passwords. Zhuang also signed a confidentiality memorandum that required the "strictest confidence of all information" including data, workflows, client and vendor information, directories and databases. Prior to leaving the company, Zhuang allegedly forwarded emails containing information such as a marketing program financial model to her email account. Universal sued Zhuang and Argus Merchant Services LLC, Zhuang's new employer, alleging breach of contract and misappropriation of trade secrets. The court granted Zhuang's motion to dismiss on the grounds that Universal's pleadings failed to sufficiently allege that the marketing program constituted a trade secret, absent allegations as to its value, competitive advantage, and secrecy. The court further held that that listing other broad, general categories of information, without reference to other criteria, is insufficiently specific to plead the existence of a trade secret.

3rd Circuit

***Christian v. Lannett Co.,* 2018 WL 1532849 (E.D. Pa. 2018) (unpublished).** Christian, a terminated manager, brought various claims against her former employer, Lannett. Lannett asserted a counterclaim for trade secret misappropriation under the Defend Trade Secrets Act of 2016 ("DTSA"). Lannett alleged that Christian retained company trade secrets and improperly disclosed them to third parties. The court dismissed the purported disclosures to Christian's husband because they took place in 2013, well before the DTSA was enacted. The only disclosure that continued beyond the effective date of the DTSA was Christian's disclosure of the purported trade secrets to her counsel in response to a court order. However, the court found that this disclosure fell within the immunized disclosure parameters defined by the DTSA. This DTSA provision allows for an individual to disclose trade secrets "in confidence . . . to an attorney . . . solely for the purpose of reporting or investigating a suspected violation of law."

***Jazz Pharms., Inc. v. Synchrony Grp., LLC*, 343 F. Supp. 3d 434 (E.D. Pa. 2018)**. Jazz, a California based pharmaceutical company manufactured a drug called Xyrem. In an effort to increase marketing support for the drug, Jazz engaged in business discussions with Synchrony, a pharmaceutical marketing firm. The parties entered into a Master Services Agreement ("MSA"), which included provisions mandating the protection of Jazz's confidential information and the return or destruction of such information once the relationship had ended. Synchrony had access to valuable information concerning all aspects of Jazz's medical marketing and development plans for Xyrem and other sleep-related drugs. Approximately three months prior to the end of the MSA term, Synchrony informed Jazz of its interest in working for a competitive pharmaceutical company. Synchrony then notified Jazz in writing of its intention to terminate their relationship.

Synchrony returned some, but not all, of Jazz's confidential information. Jazz filed suit asserting violation of the Defend Trade Secrets Act and the Pennsylvania Uniform Trade Secrets Act. Synchrony filed a motion to dismiss, which the court denied. The court found the complaint sufficiently alleged misappropriation in two ways. First, Jazz pleaded that the Synchrony had disclosed its trade secrets to acquire the competitor's business and knew that it did not obtain Jazz's consent. Second, under the inevitable-disclosure doctrine, the Third Circuit holds that where there is substantial overlap between Jazz and its competitor (role, industry, geographic region), a court may find that there will likely be disclosure of the confidential information to Synchrony's detriment. Synchrony offered no assurances that it would isolate its personnel who had worked with Jazz from working with the competitor, which plausibly moved the allegations beyond speculation.

***Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659 (E.D. Pa. 2018)**. Sandhu worked at Teva in regulatory affairs and then as Senior Director until her termination in 2016. Sandhu signed a confidentiality agreement prohibiting her from improperly disclosing trade secrets or confidential information when she became an employee at Teva. During her employment at Teva, Sandhu was in a romantic relationship with Desai, the chief executive officer of Apotex, a competing company. Teva discovered that Sandhu had shared confidential information about Teva's products in development with Desai and ultimately Apotex. One of the documents was a Complete Response Letter ("CRL") for one of Teva's generic drug products, which included confidential correspondence from the Food and Drug Administration ("FDA") regarding how a new drug may gain approval. An investigation revealed that Sandhu had emailed documents marked as "confidential" that contained trade secrets to Desai at his Apotex email address. Teva alleged that Sandhu, Desai, and Apotex misappropriated its trade secrets in violation of the Defend Trade Secrets Act ("DTSA") and the Pennsylvania Uniform Trade Secrets Act ("PUTSA"). The court found that although the allegedly misappropriated trade secrets were acquired and used before the enactment of the DTSA, Teva sufficiently asserted a DTSA claim because it alleged that its competitor continued to use its trade secrets after the DTSA's enactment. The CRL contained confidential comments from the FDA regarding a drug application that Apotex used to "speed the regulatory approval" of its competing generic product. The spreadsheet Sandhu uploaded to her personal drive detailed the regulatory status of dozens of pre-approval and post-approval products. Those documents contained information that was not available outside Teva because it was classified as confidential and Teva took measures to restrict access to it. Therefore, the court concluded the misappropriation claims under the DTSA and PUTSA may proceed.

4th Circuit

***360 Mortg. Grp., LLC v. Home Point Fin. Corp.*, 740 Fed. App'x. 263 (4th Cir. 2018) (unpublished).** Mortgage Group, a lender that funds and services residential mortgage loans, brought an action against its competitor, Stonegate, for trade secret misappropriation in violation of North Carolina's Trade Secrets Protection Act. When Mortgage Group began experiencing financial troubles, its account executive responsible for overseeing broker relationships, Lisa Glenn, entered into employment discussions with Stonegate. In an attempt to increase her offer, Glenn gave Stonegate Mortgage Group's broker customer lists obtained from Mortgage Group's secure online database and several charts showing the amount and status of Glenn's funded loans. The district court entered summary judgment in favor of Stonegate, finding that the information provided did not contain trade secrets and that Mortgage Group failed to show the alleged

misappropriation was a proximate cause of the damages. The Fourth Circuit affirmed. Specifically, Mortgage Group relied on a report from its chief operating officer, WeissMalik, that after Glenn resigned, Mortgage Group's loan sales in North Carolina continued to decline even though its nationwide sales began to improve. The court found that WeissMalik's conclusions were speculative and did not support the proposition that the decline in sales in North Carolina was related to misappropriation of customer information, rather than resulting from Glenn's resignation or from any other event. Additionally, WeissMalik's calculation as to Stonegate's profits was speculative and did not establish a connection between the profits and the purported misappropriation because WeissMalik relied on aggregate financial information. Stonegate presented evidence of other causes for the decline in Mortgage Group's business, such as Mortgage Group's funding problems, customer complaints, and failure to replace Glenn.

***AirFacts, Inc. v. de Amezaga*, 909 F.3d 84 (4th Cir. 2018).** AirFacts is a developer and licenser of software used to audit ticket prices for airlines and travel agencies. Diego de Amezaga worked for AirFacts, during which he developed flowcharts and proration spreadsheets for AirFacts, designed to improve AirFact's auditing process. De Amezaga emailed these documents to his personal email account prior to resigning from AirFacts and joining American Airlines. AirFacts sued de Amezaga for trade secret misappropriation in violation of the Maryland Uniform Trade Secrets Act. The Fourth Circuit held that the district court erred in concluding the flowcharts were not trade secrets because they were an overview of publicly available information. The flowcharts were inherently valuable because de Amegaza spent significant time arranging the data using his personal insight. Further, the flowcharts improved AirFacts efficiency in the performance of its contractual obligations. AirFacts took steps to maintain the secrecy of the flowcharts through companywide nondisclosure agreements. The Fourth Circuit also affirmed the district court's finding that de Amegaza did not misappropriate the proration documents. De Amegaza emailed the proration documents to his personal email account within the scope of his employment and only to answer questions from AirFacts after his resignation. While a person can misappropriate trade secrets if he knows or has reason to know he acquired them by improper means, AirFacts did not present credible evidence that de Amezaga knew his actions were improper.

***CSS, Inc. v. Herrington*, 306 F. Supp. 3d 857 (S.D. W. Va. 2018).** CSS, a software provider, sued its former employee, Herrington, and its competitor, Compiled Technologies, for misappropriation of trade secrets in violation of the West Virginia Uniform Trade Secrets Act. While employed by CSS, Herrington helped develop CSS's software for land indexing and estate management that was used by county clerks. CSS alleged that Herrington disclosed to Compiled Technologies the source code for CSS's software programs, a detailed knowledge of the working of the programs, what county clerks needed, and how the software operates to meet such needs. The court found that CSS did not take reasonable efforts to keep the source code secret because it uploaded the source code files on the county's servers, which were accessible by third parties that had contracted with the county. Therefore, a third party could access the source code by proper means. The court held that knowledge of how the program worked was not a trade secret because a competitor could study the source code obtained through proper means to gain a detailed knowledge of the workings of the programs. Further, knowledge of what county clerks needed was not a trade secret because a competitor could call the county clerks and ask them what they needed. Finally, combining all the information together would enable a competitor to discern how the software operated to meet the county clerks' needs.

5th Circuit

***Apogee Telecom, Inc. v. Univ. Video Servs, Inc*., 2018 WL 6220177 (W.D. Tex. 2018) (unpublished).** Defendant had hired a former employee of the plaintiff. Plaintiff sued the defendant for misappropriation of trade secrets. Defendant moved for a stay because the plaintiff had previously sued its former employee (now defendant's employee) in California state court for misappropriating trade secrets and related torts. In the later filed federal case, the plaintiff sued the defendant employer, based on misuse of the trade secrets in a project. The district court found the trade secrets in issue were the same in both cases. The district court, however, noted the defendants were different in the two cases, in the first it was the employee only, and in the later it was the employer. Further, the district court found that even though the underlying trade secrets were the same, the alleged acts of misappropriation were different. Accordingly, the district court denied the stay.

***CGC Royalty Investments I, LLC v. Order Simplicity, LLC*, 2018 WL 3589085 (N.D. Tex. 2018) (unpublished).** Plaintiff CGC Asset ("CGC") licensed its Order Management Software ("OMS") to defendant Order Simplicity, LLC ("OS") under an agreement that prohibited OS from assigning its rights to OMS without prior written consent. Thereafter, defendant MyndShft Technologies, LLC expressed interest to CGC in utilizing OMS in its business, and CGC introduced MyndShft to OS. Eventually, MyndShft acquired OS, and informed CGC that it now had rights to OMS pursuant to the license between CGC and OS. CGC filed suit for, among other things, trade secret misappropriation under the Texas Uniform Trade Secrets Act and the Defend Trade Secrets Act. The court granted CGC's preliminary injunction on its trade secret claims. The court ruled CCG sufficiently established that the software's source code likely includes trade secrets. The court also held that MyndShft acquired the trade secret through improper means. CGC showed breach of contract in OS assigning its rights to OMS to MyndShft without first obtaining CGC's written consent. Defendants tried to evade CGC's theory by arguing the consent provision was merely a right to object to an assignment. But the district court found it was instead a requirement to obtain prior written consent.

***SPBS, Inc. v. Mobley*, 2018 WL 4185522 (E.D. Tex. 2018) (unpublished)**. This case addresses the Texas Uniform Trade Secrets Act ("TUTSA") provision for a preliminary injunction based on "threatened disclosure." The court citing prior cases, held that "'[T]o establish threatened disclosure, the law requires [Plaintiff] to show disclosure of specific trade secrets would benefit [an employee's new employer].'" The court found that it is probable the former employee would use the trade secret information for his benefit or for his new employer. Among other things, the court found that it should consider the whether the trade secrets would be useful to the new employer in light of the new employers' markets and existing business model and strategies. When assessing a trade secret's potential benefit to a new employer and its detriment to an old employer, courts consider whether they compete in the same markets for the same products and services. Finding that the former employee and his new employer actually had competed for contracts with the same or overlapping services, the court held the plaintiff was threatened with misappropriation based on the history of past misappropriation. The court further found an injunction was merited because of breach of the former employee's non-compete agreement with his former employer.

***TLS Mgmt. & Mktg. Servs., LLC v. Mardis Fin. Servs.*, 2018 WL 3698919 (S.D. Miss. 2018) (unpublished).** TLS was a tax preparation service, which contracted with defendants to develop

and service existing and new business. TLS had a proprietary database of confidential information about its existing customers' needs and the most recent developments in the field. The court found the defendants had destroyed documents in discovery, and as a sanction entered a default against them. The district court then examined each cause of action plead by TLS, focusing first on the trade secret misappropriation claim, followed by other claims for unfair competition, tortious interference, federal trademark law, and breach of contract. The court rejected the defendants' arguments that these claims were simply different theories on the same facts, finding that the facts alleged showed distinct causes of action, even where the underlying theft of trade secrets was part of each claim. The district court had a two-day bench trial on damages, and thereafter made a detailed computation of damages for each claim. The court calculated lost profits, expectancy damages, actual losses, and the Defendants' profits derived from the trade secrets alleged in the operative complaint. The court eliminated any overlapping damages, and then determined whether pre-judgment interest should be awarded and at what rate.

***WorldVentures Mktg., LLC v. Rogers*, 2018 WL 4169049 (E.D. Tex. 2018) (unpublished).** This case includes claims under the Texas Uniform Trade Secrets Act and the Defend Trade Secrets Act. Plaintiff WorldVentures Marketing is a multi-level marketing firm, and Defendant Rogers had been a long-term sales representative. Rogers left and formed a competing company. WorldVentures sued Rogers for misappropriating confidential information regarding its representatives. Rogers responded that the names of its representatives and their levels in the organization were public information. WorldVentures, however, explained the valuable secret was the "genealogy" of those members, and in fact its nondisclosure agreement specifically identified the "genealogy" information as a trade secret. Rogers argued that there was no evidence he had used this information. The court, however, held that for purposes of a preliminary injunction a plaintiff need not establish that a defendant actually used any trade secrets; the fact that a defendant is in a position to possibly use trade secrets is sufficient to warrant injunctive relief.

6th Circuit

***In re: Nat'l Prescription Opiate Litig.*, 325 F. Supp. 3d 833 (N.D. Ohio 2018), *vacated and remanded,* 2019 WL 2529050 (6th Cir. 2019).** This case is a multidistrict litigation wherein public entities have sued manufacturers, distributors, and retailers of prescription opiate drugs. In the course of discovery, the court ordered the Drug Enforcement Agency ("DEA") to produce, under a strict protective order, data maintained in the DEA's Automation of Reports and Consolidated Orders System ("ARCOS"). Because ARCOS data contains law-enforcement sensitive information and confidential commercial information of the reporting manufacturers, distributors and retailers, the DEA does not release ARCOS data publicly. Media outlets served public records requests upon various parties asking for copies of the ARCOS data furnished to those parties in the course of discovery in the MDL. Those various parties objected. The media outlets argued that the ARCOS data was stale historic information not entitled to protection under trade secret, privacy or law enforcement exceptions to the Freedom of Information Act. The court disagreed, holding that ARCOS data submitted by prescription opiate distributors contained confidential business information of the responding distributors and retail pharmacies and, more importantly, sensitive law enforcement information. The court noted that FOIA exempts from public disclosure any "confidential commercial information, the disclosure of which is likely to cause substantial competitive harm," the court finding that the FOIA exemption was "co-extensive" with the protection afforded under federal trade secret law. With the "trade secret" concept as part of the

analysis, but again, with more emphasis on the "sensitive law enforcement" data contained in the ARCOS database and relying upon the strict Protective Order entered in this case, the court denied the media outlets' request for copies of the ARCOS data that had been produced in discovery in the MDL.

***Sheffield Metals Cleveland, LLC v. Kevwitch*, 2018 WL 1290990 (N.D. Ohio 2018) (unpublished).** Plaintiff Sheffield Metals Cleveland, LLC brought suit against defendant, a former employee, for misappropriation of trade secrets and violation of post-employment restrictive covenants. Defendant's nondisclosure and noncompetition agreement with Sheffield, as well as her severance agreement, contained terms prohibiting the use or disclosure of trade secrets and requiring the return of all Sheffield's confidential and proprietary information. A forensic analysis of defendant's work laptop showed that, during her employment with Sheffield, she repeatedly sent company information from her work email to her personal email, including marketing strategies and product comparisons. Defendant did not respond to Sheffield's requests for the return or those documents. On cross-motions for summary judgment, the court concluded that Sheffield failed to support its misappropriation claim because it lacked sufficient proof of unauthorized use or disclosure to third parties. Defendant's subsequent work for a competitor and solicitation of Sheffield's customers were not enough for Sheffield's trade secret misappropriation claim to survive summary judgment.

7th Circuit

***Bay Fasteners & Components, Inc. v. Factory Direct Logistics, LLC*, 2018 WL 1394033 (N.D. Ill. 2018) (unpublished).** Bay Fasteners & Components ("BFC") sued its former president, Palmer, and its competitor, Factory Direct Logistics ("FDL"), and FDL's president, Long, for trade secret misappropriation in violation of the Defend Trade Secrets Act ("DTSA"). As president, Palmer was privy to a wide range of BFC's confidential information, including customer contact information, customer production specifications, and buying practices. BFC alleged Palmer intended to use such confidential information to FDL's competitive advantage. The defendants moved to dismiss, arguing that broad and conclusory references to customer data was insufficient to state a claim. The court rejected this argument, nothing that the customer lists fell under the DTSA's broad definition of a trade secret and that trade secrets may be alleged generally. Further, the DTSA did not require heightened pleading and it was sufficient for BFC to allege that the defendants vowed to use BFC's trade secrets to their advantage. A nondisclosure agreement in an employee handbook and restricted office access were sufficient security measures at the dismissal stage given Palmer's position as president. However, information BFC disclosed to FDL via email without obtaining a promise of confidentiality was not reasonably protected. Finally, the court held a plaintiff is not required to plead improper means, only misappropriation.

***Call One, Inc. v. Anzine*, 2018 WL 2735089 (N.D. Ill. 2018) (unpublished).** Anzine worked for Call One, a telecommunications service provider. Anzine was subject to confidentiality provisions prohibiting Anzine from emailing confidential information without supervisor approval. One such provision stated that employees "must be advised of any confidential data [to which] they have been granted access. Such data must be marked or otherwise designated 'confidential.'" Prior to Anzine's resignation from Call One, Anzine received a customer report from Call One's sales director. The report contained detailed customer information but was not marked confidential. Anzine had emailed the report to her husband so he could print the document from Anzine's home

office and later deleted it from her company issued laptop. Call One discovered this after Anzine's resignation and filed suit. Anzine emailed a copy of the report to her attorney to prepare for litigation. Call One alleged Anzine misappropriated its trade secrets in violation of the Defend Trade Secrets Act by emailing the report to her husband and attorney without authorization from Call One. The court found there was no evidence of misappropriation and did not address whether the report was a trade secret. The court held that a jury could not reasonably find that Anzine acquired the report by improper means when Call One did not mark it confidential as required. Further, Anzine's deleting the report from her computer did not permit an inference that she knew the document was confidential. The court also held that merely sending the report to her personal email account was not sufficient to establish improper means under the circumstances.

***Motorola Sols., Inc. v. Hytera Commc'ns Corp.*, 314 F. Supp. 3d 931 (N.D. Ill. 2018).** Hytera moved to dismiss Motorola's complaint for trade secret misappropriation after Motorola waited ten years to sue for trade secret misappropriation. The court allowed limited discovery on the issue of whether Hytera concealed the theft of trade secrets so as to toll the statute of limitations. After the close of limited discovery, which had already been extended several times, Motorola moved to compel a forensic examination of the computers of key Hytera witnesses. After an initial hearing, the court tentatively allowed the forensic examination upon representations from counsel that the forensic examination would not run afoul of Chinese law and would be accomplished quickly. However, the court later denied the motion, expressing extreme frustration with the amount of resources devoted to the limited discovery and Motorola's attempts to expand the discovery to obtain information concerning misappropriation of the trade secrets. The court distinguished the statute of limitations issue from the liability issue and held that Motorola failed to adequately explain how the information it hoped to obtain from the forensic examination of Hytera's computers was relevant to a potential equitable tolling of the statute of limitations. Because Motorola never had access to Hytera's computers in the first place, even if Motorola learned through the forensic examination that Hytera employees deleted trade secret documents on their computers, it would not be relevant to why Motorola could not discover the theft sooner. Further, the court held that the forensic examination was not proportional to the needs of the case and is a drastic step even in general discovery.

8th Circuit

***CPI Card Grp., Inc. v. Dwyer,* 294 F. Supp. 3d 791 (D. Minn. 2018).** Plaintiffs moved under the Defendant Trade Secrets Act ("DTSA") and the Minnesota Uniform Trade Secrets Act ("MUTSA") to preliminary enjoin certain of its former employees and their new employer from further use or disclosure of information and materials plaintiffs alleged they had specifically developed for a particular customer, as well as other information one of the defendants had forwarded to his personal email account that plaintiffs had marked "confidential." The court denied plaintiffs' motion, finding that plaintiffs had not shown a fair chance of prevailing on their misappropriation claims. As to the information allegedly developed for a particular customer, the court found plaintiffs failed to meet their burden of showing that the allegedly misappropriated information qualified as a "trade secret," principally due to a perceived lack of reasonable measures to keep the information secret, including evidence that the customer actually shared the information with third parties without restriction. Further, the court found that although some of plaintiffs' alleged trade secret material had been marked "confidential," plaintiffs had failed to show that specific information was either used by defendants or disclosed to others by them.

Lastly, testimony presented at the hearing relating to information contained within presentation materials titled "Strategic Plan" and "Market Opportunities" was found to likely be information "generally known to" others in the industry, precluding a finding that the information qualified as trade secret.

***CPI Card Grp., Inc. v. Dwyer,* 2018 WL 4815572 (D. Minn. 2018) (unpublished).** In ruling on plaintiffs' motion to compel discovery, the court determined that plaintiffs had sufficiently disclosed the details of the alleged trade secret information to require defendants' response to plaintiffs' discovery requests. The court further ruled, though, that plaintiffs would be required to supplement their interrogatory responses and specifically designate the information they were contending to be "trade secret" in the near future. The court ruled that plaintiffs could amend their trade secret designations based off what was found in discovery, but that plaintiffs' designations could not include caveats or reservations. The designations had to be definite and complete and could not be representative examples. Additionally, plaintiffs were not permitted to respond in a "summary fashion" or say that "certain aspects" of a general description include a trade secret.

***Cy Wakeman, Inc. v. Nicole Price Consulting, LLC,* 284 F. Supp. 3d 985 (D. Neb. 2018).** Plaintiff brought suit against a former employee contending that certain of plaintiff's business training materials had been misappropriated and used by defendant to plaintiff's economic detriment. On plaintiff's motion for preliminary injunction, the court found that plaintiff's alleged trade secret information, the mere existence of customer relationships between plaintiff and certain of her clients, did not have independent economic value to others even if that information was secret and of perceived importance to plaintiff and her ability to generate revenues. According to the court, "secrecy does not equal economic value." As such the subject information did not qualify as trade secret under the Nebraska Trade Secrets Act and the motion for preliminary injunction was denied.

***Farmers Edge Inc. v. Farmobile, LLC*, 2018 WL 2869005 (D. Neb. 2018) (unpublished), and *Farmers Edge Inc. v. Farmobile, LLC*, 2018 WL 3747833 (D. Neb. 2018) (unpublished).** Farmers Edge acquired an entity which had formerly employed the individuals who formed Farmobile, a competing business, developing similar technology to the former employer. After their departure, and after Farmers Edge completed its purchase of the former employer, Farmobile filed an application to patent aspects of the subject technology. Farmers Edge sued, accusing the individuals of misappropriating the trade secrets of its predecessor-in-interest, based on the Defend Trade Secret Act ("DTSA") and the Nebraska Trade Secrets Act ("NTSA"). Initially, Farmers Edge avoided dismissal of its DTSA claim by alleging that that, although Farmobile was created before enactment of the DTSA, the complained of misappropriation continued well after enactment. At summary judgment, however, the court dismissed the DTSA claim finding that the only potential disclosure of the alleged trade secret information occurred when Farmobile's pending patent application published in August 2015, before enactment of the DTSA. The court also dismissed the NTSA claims after making factual findings that, under the NTSA's more demanding standards, none of plaintiff's allegedly misappropriated information qualified as a "trade secret," principally because the information was found to be ascertainable by proper means. After judgment had been entered against plaintiff on all asserted claims, the court held a bench trial to determine whether the DTSA claims were made or maintained in bad faith. Denying defendant's request for attorney's fees, the court explained that the lack of case law on the recently-enacted DTSA provided some support for the plaintiff's subjective believe that there could have

been a continuing misappropriation DTSA claim. The court also found that the presence of a state-law misappropriation claim, even though ultimately rejected, mitigated against a finding that there was an improper purpose in maintaining the DTSA claim.

***Goodbye Vanilla, LLC v. Aimia Proprietary Loyalty U.S. Inc.*, 304 F. Supp. 3d 815 (D. Minn. 2018).** The court granted defendant's motion for summary judgment on plaintiff's misappropriation claim brought under the Minnesota Uniform Trade Secrets Act ("MUTSA"). Plaintiff claimed defendant misappropriated a one-page email containing proprietary information on how to use an analytical modeling tool. The court found that plaintiff failed to establish how this single page email was a "trade secret" under the MUTSA. The court further found there was no evidence that this email, which was designed to be sent to third parties, was "misappropriated" by the defendant or that there was ongoing misuse or misappropriation of this alleged trade secret.

***Prime Therapeutics LLC v. Beatty,* 354 F. Supp. 3d 957 (D. Minn 2018).** The court ruled that plaintiff's strategic plans and its pricing, margins, and purchase history of pharmaceutical drugs constituted "trade secrets" under the federal Defend Trade Secrets Act ("DTSA") and Minnesota Uniform Trade Secrets Act ("MUTSA"). However, for purposes of plaintiff's motion for preliminary injunction, plaintiff did not meet its heavy burden of showing inevitable disclosure of those trade secrets. The court found that plaintiff's former employee was working a job which was purposefully designed and sufficiently distinct so that disclosure of plaintiff's trade secrets was unlikely. Also, there was no evidence of any wrongdoings by that former employee, nor was there any evidence that former employee had any document containing plaintiff's asserted trade secrets. Finally, plaintiff failed to show irreparable injuries because if defendants did misappropriate plaintiff's trade secrets, the harm would be a loss of business, which could be reparable through monetary damages.

***Schenck Process LLC v. Zeppelin Sys. USA, Inc.*, 2018 WL 4279223 (W.D. Mo. 2018) (unpublished).** The court denied plaintiff's motion for a temporary restraining order, finding that plaintiff did not show it was likely to succeed on the merits of its claims brought under the Defend Trade Secrets Act ("DTSA") or the Missouri Uniform Trade Secrets Act ("MUTSA"). At this point in litigation, plaintiff was relying on the inevitable disclosure theory to show actual or threatened misappropriation. The court rested its denial of the MUTSA claim primarily on the fact that Missouri does not recognize the doctrine of inevitable disclosure. Additionally, plaintiff failed to show that its former employee would be required to divulge plaintiff's alleged trade secrets at the employee's new job.

***Tension Envelope Corp. v. JBM Envelope Co.*, 876 F.3d 1112 (8th Cir. 2017).** The court upheld dismissal of plaintiff's claims for misappropriation under the Missouri Uniform Trade Secrets Act ("MUTSA"). The two claimed trade secrets at issue were: (1) the identity of plaintiff's customers; and (2) the unique requirements of those customers. The court ruled that, under Missouri Supreme Court precedent, "customer contacts" are generally protectable through claims regarding breach of fiduciary duties, but they are not protectable under the MUTSA as trade secrets. The court also found that, under Missouri precedent, customer preferences and requirements are not trade secret because that type of information is obtainable through legitimate means. A customer's preferences and requirements are the customer's information, not the seller's information. Because this information can be gathered from the customers themselves, it is not a protectable trade secret.

***US Polymers-Accurez, LLC v. Kane Int'l Corp*., 2018 WL 4491168 (E.D. Mo. 2018) (unpublished).** The court denied the parties' cross motions to dismiss the various trade secret claims brought under the Defend Trade Secrets Act ("DTSA"), Missouri Uniform Trade Secrets Act ("MUTSA"), and New York trade secrets law. Defendant claimed that plaintiff's various claims were preempted by the MUTSA which "displace[s] conflicting tort, restitutionary, and other laws . . . providing civil remedies for misappropriation of a trade secret." Mo.Rev.Stat. § 417.463.1. The court found that, because it had not yet determined as a matter of law that the underlying information qualified as a trade secret, it would be premature to find plaintiff's other claims preempted by the MUTSA. The court went on to find these various other claims could extend beyond the asserted trade secret claims, and that it was premature to dismiss these other claims as merely derivative of the MUTSA claim. The court also denied plaintiff's motion to dismiss defendant's DTSA and New York common law trade secret misappropriation counterclaim. While plaintiff claimed defendant failed to sufficiently plead its trade secret claims, the court disagreed and found that additional specificity as to the precise trade secrets misappropriated was not required at the motion to dismiss stage.

9th Circuit

***Attia v. Google LLC*, 2018 WL 2971049 (N.D. Cal. 2018) (unpublished).** Plaintiffs failed to adequately plead the existence of a "pattern of racketeering activity" for a civil RICO trade secret misappropriation claim by providing a list of six unrelated lawsuits in which other plaintiffs brought trade secret misappropriation claims against Google. This tactic of relying on other lawsuits runs afoul of Rule 11, which requires that attorneys have sufficient knowledge of the factual allegations in their pleadings to justify signing the document. Furthermore, plaintiffs' theory that "ongoing use" of trade secrets can somehow constitute *two* predicate acts under RICO "is entirely unsupported and illogical" because a single trade secret dispute does not serve as the basis for two predicate acts under RICO merely because a defendant did not stop the alleged use. Finally, plaintiffs cannot pursue RICO claims based on trade secret misappropriation that occurred before the Defend Trade Secrets Act (DTSA) came into effect, but defendants are not estopped from arguing the "very narrow question of whether Plaintiffs can possibly allege continued trade secret misappropriation on or after [date of enactment of the DTSA] to allege a predicate act required for RICO *standing* when they have also alleged that the trade secrets at issue were extinguished in 2012."

***Bal Seal Eng'g v. Nelson Prod*., 2018 WL 4697255 (C.D. Cal. 2018) (unpublished).** Denying defendant's motion for summary judgment on plaintiff's claim of trade secret misappropriation based on allegations that defendant obtained top-level drawings and design solutions from its customers. Although reverse engineering is a defense to a misappropriation of trade secrets claim, the possibility that a trade secret might be or could be reverse engineered is not a defense. Also, trade secrets were adequately identified where plaintiff identified customers together with specifications for design solutions for that customer. Where drawings were marked as proprietary and were accompanied by terms and conditions of sale that specified that the "products and information" of plaintiff are proprietary and may not be shared, a reasonable factfinder could conclude that plaintiff's efforts to keep trade secrets secret were reasonable under the circumstances.

***Becton, Dickinson & Co. v. Cytek Biosciences Inc*., 2018 WL 2298500 (N.D. Cal. 2018) (unpublished).** Dismissing claims under Defend Trade Secrets Act ("DTSA") and California Uniform Trade Secrets Act ("CUTSA") (with leave to amend) because plaintiff failed to sufficiently identify trade secrets ("design review templates," "fluidics design files," and "source code files" are too broadly stated, and the inclusion of phrases "such files included" and "such as" further expanded the scope of the allegations). All other claims were also dismissed because they were based on the same wrongdoing as the CUTSA claim, and thus were preempted; these claims include: aiding and abetting DTSA violation; violation of California unfair competition law; breach of contract; breach of implied covenant of good faith and fair dealing; inducing breach of contract; unjust enrichment; breach of confidence; and common law conversion.

***BladeRoom Grp. Ltd. v. Emerson Elec. Co*., 331 F. Supp. 3d 977 (N.D. Cal. 2018).** "The court must dispel the notion that a plaintiff can never prove ownership of a trade secret without expert testimony. Information need not be complex, novel or outside the understanding of a layperson to constitute a trade secret." Nor was expert testimony needed to show that defendant's design was substantially derived from plaintiff's trade secrets; a layperson was able to compare the trade secrets with the evidence of defendant's product and determine whether the product derived from the trade secrets, given defendant's access to plaintiff's confidential information and defendant's prior lack of experience with the product type.

***BladeRoom Grp. Ltd. v. Facebook, Inc.*, 2018 WL 452111 (N.D. Cal. 2018) (unpublished).** While confidentiality is key, "[t]he general notion of novelty applicable in patent infringement cases does not translate into claims for trade secret misappropriation. Trade secrets do not derive value from their novelty, and such a requirement is conspicuously absent from California Uniform Trade Secrets Act's definition of what constitutes a trade secret."

***Bladeroom Grp. Ltd. v. Facebook, Inc*., 2018 WL 514923 (N.D. Cal. 2018) (unpublished).** Defendant's analysis that its product does not "use" plaintiff's trade secrets, conducted in the style of a patent infringement case, is not persuasive when applied to trade secret misappropriation. "[U]nauthorized use need not extend to every aspect or feature of the trade secret; use of any substantial portion of the secret is sufficient to subject the actor to liability." In fact, "an actor is liable for using the trade secret with independently created improvements or modifications if the result is substantially derived from the trade secret." Also, defendant's argument that claims of misappropriation of "combination trade secrets" are inadequate fails. While defendant argues that the combination trade secrets do not detail "how the parts work together to create a trade secret," in fact each combination claim consists of some permutation of specific individual trade secrets that were adequately disclosed.

***Citcon USA, LLC v. RiverPay Inc*., 2018 WL 6813211 (N.D. Cal. 2018) (unpublished).** Finding the following descriptions of trade secret sufficiently particular to survive motion to dismiss for failure to identify trade secrets: five identified payment processing algorithms ("Citcon is not required to hand over the algorithms themselves or otherwise disclose the source code to give the defendants notice of the contours of this claim in order to prepare a defense"); "hardware and software design of the POS devices"; "email and/or telephone numbers of the specific contacts of the clients" and "identifying tokens of Citcon's merchant clients" that are "compiled into a database." However, the following description was insufficient, and the claim based upon it was dismissed: "confidential plans for business development, marketing and sales."

***Experian Info. Sols., Inc. v. Nationwide Mktg. Servs. Inc.*, 893 F.3d 1176 (9th Cir. 2018).** Reversing the district court's grant of summary judgment against an Arizona state law trade secret claim, the panel held that if proper safeguards were maintained, then Experian's lists of names with addresses, which were the product of a "sophisticated process to ensure accuracy and utility," could be protected as trade secrets under Arizona law.

***Freeman Inv. Mgmt. Co., LLC v. Frank Russell Co.,* 729 Fed. App'x. 590 (9th Cir. 2018) (unpublished).** Affirming district court's decision granting summary judgment to defendant on trade secret claims because plaintiff did not point to evidence showing that any of the information in its 492-paragraph trade secret identification document was not generally known. "We refuse to do this work for it." *See Indep. Towers of Washington. v. Washington*, 350 F.3d 925, 929 (9th Cir. 2003) ("[J]udges are not like pigs, hunting for truffles.")" (citation omitted).

***Gatan, Inc. v. Nion Co.*, 2018 WL 2117379 (N.D. Cal. 2018) (unpublished).** Gatan's description of its trade secrets failed to enable Nion to discern the boundaries of the alleged trade secrets and fell short of satisfying Cal. Civ. Proc. Code § 2019.210. Gatan is a manufacturer of spectrometers. "Many of Gatan's designations could include not only any of Nion's spectrometer data but also any company's spectrometer data. For example: 'Details on how to improve dark reference via a script and how to adjust the spectrometer to address beam traps and alignment issues.' . . . Such generic spectrometer concepts do not enable Nion to determine the bounds of discovery or litigation, other than 'spectrometers.'" Also, "some of the designations do not provide information sufficient to prevent Gatan from claiming new alleged trade secrets after the completion of discovery. For example: 'Details on noise characteristics of the electronics contained in various iterations of Gatan lens cards.'" The court ordered Gatan to produce a revised § 2019.210 designation that includes "(i) a summary in plain English of the specific trade secrets at issue and (ii) a numbered list of the trade secrets with a corresponding list of specific elements. for each, as claims would appear at the end of a patent."

***Gradillas Court Reporters, Inc. v. Cherry Bekaert, LLP*, 2018 WL 2197544 (N.D. Cal. 2018) (unpublished).** Plaintiff hired defendants to submit its bid for a government contract, which they did after the deadline for the bid had passed. In order to prove that it would have been awarded the bid if defendants had timely submitted it, plaintiff sought the winning bid information from the government through a FOIA request, but the government refused to provide the documents. Plaintiff then filed a motion to compel discovery from the winner of the contract, Behmke. Behmke claimed its pricing and procurement information was a trade secret and could not be disclosed to its current and likely future competitor. The court held that there was a "substantial need" for the documents and that a protective order would sufficiently protect Behmke's trade secrets. The court ordered the parties to meet and confer to resolve differences regarding the proposed protective order and explained that if the parties could not agree then the court would simply issue the Model Protective Order.

***Human Longevity, Inc. v. J. Craig Venter Inst., Inc.*, 2018 WL 6617633 (S.D. Cal. 2018) (unpublished).** Holding that the complaint failed to allege facts with sufficient particularity to give rise to a plausible inference of the existence of a trade secret within the meaning of the Defend Trade Secrets Act. Plaintiff had alleged that its trade secrets "include, but are not limited to" "processes and data relating to HLI's development of its Health Nucleus," which is a program that "combines intelligence platform integrating genomics, advanced clinical imaging and machine

learning to provide clients with whole body assessment of potential disease and health risks." Plaintiff also alleged that its trade secrets included "bi-weekly business development updates, leadership updates, executive summaries, and weekly reports of all Health Nucleus activities"; "identity and contact information [for] financing or potential financing sources, including . . . high-net-worth individuals" and "negotiating terms and strategies for potential transactions"; "the identity and contact information of clients and potential client[s] . . . including . . . high-net-worth individuals such as Hollywood actors and actresses, corporate executives, NFL team owners, philanthropists and politicians"; "employee contact and compensation information"; "research data, studies, imaging, as well as client results and prognoses"; "HLI's-owned Lenovo laptop computer"; "internal financial reports on HLI's business operations and future forecasts"; audits and industry reports, "including analysis of market competitors"; and "plans, projections and negotiations regarding the potential expansion of HLI's business operations."

***Physician's Surrogacy, Inc. v. German*, 2018 WL 638229 (S.D. Cal. 2018) (unpublished).** Providing a detailed analysis of trade secrets relating to a fertility and surrogacy agency, and finding that lists of pre-screened surrogates, and screening methods and processes including surrogate applications, screening forms, email templates, FAQ pages, intake forms, and benefit lists, are trade secrets. However, the court granted the defendants' motion to dismiss claims of trade secret misappropriation under the Defend Trade Secrets Act (DTSA) because pleading that trade secrets were used "upon information and belief" without alleging specific actions on specific dates after the enactment of the DTSA was insufficient. The court also granted defendants' motion to dismiss plaintiff's claim that defendants violated the Computer Fraud and Abuse Act because plaintiffs failed to allege how or where defendants accessed plaintiff's protected computers.

***Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056 (N.D. Cal. 2018).** Plaintiff embedded piracy tracking tools in its semiconductor electronic design and automation software. Defendants evaluated plaintiff's software for licensing. Through the "spyware," plaintiff allegedly discovered that defendants used evaluation license keys and counterfeit keys to repeatedly and illegally access and copy its programs and materials over the course of the next three years and sued. Defendants counterclaimed that hiding the antipiracy software, using the anti-piracy software to access information on defendants' systems, and then sharing defendants' confidential information with third-parties violated several laws. The court dismissed the counterclaims. Regarding the Computer Fraud and Abuse Act ("CFAA") counterclaim, the court found that while defendants adequately pleaded that plaintiff exceeded authorization to use defendants' computers by using the hidden anti-piracy software, defendants failed to allege facts showing that the type of information secured by plaintiff caused economic damage to defendants, that the computer systems were damaged, or that the "loss" or damages incurred amounted to more than $5,000 in one year, as is required under 18 U.S.C. § 1030(a)(2) and (a)(5). The defendants also failed to plead plausible fraud allegations under 18 U.S.C. § 1030(a)(4). The defendants' counterclaim under California's Comprehensive Computer Data Access and Fraud Act ("CCDAFA") failed for the same reasons as the CFFA claim. The court found the plaintiff's argument that the CCDAFA claims are preempted by California's Uniform Trade Secrets Act ("CUTSA") to be meritless however, because there is no precedent explicitly addressing whether CUTSA would preempt a statutory claim arising under the California penal code.

***Way.com, Inc. v. Singh*, 2018 WL 6704464 (N.D. Cal. 2018) (unpublished).** Way.com, Inc. is an online marketplace for parking spot reservations. Way identified its trade secrets with sufficient

particularity to survive a motion to dismiss by identifying a single spreadsheet that contains those trade secrets. The alleged trade secrets include: "the amount Way is willing to pay parking partners in order to reserve a block of parking spaces; the process by which Way determines how to launch and market certain parking locations; the methods by which Way conducts its accounting operations; and the methods by which Way resolves technical difficulties on its platform." However, the court denied Way's motion for a preliminary injunction because it did not show that it was likely to succeed on the merits. The spreadsheet was available to every employee of the company, whether or not their job responsibilities required them to reference it, and Way did not have nondisclosure agreements with its partners.

***Waymo LLC v. Uber Techs., Inc.*, 2018 WL 466510 (N.D. Cal. 2018) (unpublished).** Holding that Waymo failed to disclose an unjust enrichment theory of damages under the Defend Trade Secrets Act ("DTSA") or California's Uniform Trade Secrets Act ("CUTSA") based on acquisition alone (as opposed to use or disclosure of the trade secrets) under FRCP 26(a), and that it is precluded from asserting any such theory at trial under FRCP 37(c)(1). "Defendants do not dispute that it is generally possible for a plaintiff to disclose, pursue, and preserve a damages theory based on something other than actual, full use of misappropriated trade secrets. Defendants' point is that Waymo has not done so here. This order agrees." "What seems to be going on here is that this civil action began with vehement accusations that Uber had stolen Waymo's alleged trade secrets and used them to jump-start Uber's own LiDAR development for its competing self-driving car program. Yet subsequent discovery and inspections, Uber contends, failed to reveal much, if any, such use. Now, Waymo seeks to fall back to the contingent argument that even if Uber did not use the trade secrets, Uber still stole them and should pay. The problem remains, however, that Waymo did not put Uber on notice of this fallback position and Uber has not had a fair opportunity to organize its defenses around this amorphous possibility. Consequently, Waymo must be held to prove its showcase contention — that Uber used or disclosed Waymo's alleged trade secrets."

10th Circuit

***Swimwear Sol., Inc. v. Orlando Bathing Suit, LLC*, 309 F. Supp. 3d 1022 (D. Kan. 2018).** Plaintiff Swimwear Solution is a single-location bathing suit shop that entered into discussions about a possible acquisition by Defendant Orlando Bathing Suit, which is a chain of bathing suit shops. The parties entered into a nondisclosure agreement, and plaintiff provided defendant with confidential information about its business. Discussions eventually broke down and defendant opened a store next to Plaintiff's store. A lawsuit followed with Plaintiff asserting numerous claims, including misappropriation of trade secrets under New York and Kansas laws. The court granted defendant's motion to dismiss the trade secret claims, holding that plaintiff had waived the right to assert them through the nondisclosure agreement, which had a clause in which the parties waived trade secret protections. The court held that the waiver was clear and was enforceable because it did not violate public policy of either New York or Kansas. New York does not have a trade secret misappropriation statute, but Kansas does. The court held that the waiver does not violate public policy of Kansas, despite the statute, because the statute states that it does not displace contractual remedies.

***Solar Connect, LLC v. Endicott*, 2018 WL 2386066 (D. Utah 2018) (unpublished).** The Court granted an *ex parte* seizure order, pursuant to the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836(b)(2)(B). It held that seizure was necessary because defendants likely would not comply

with an injunction. The court ordered federal law enforcement officers to enter the home office of the defendant and seize computers, tablets, smartphones and storage devices. The order directed a technical expert to accompany the officers for purposes of copying the devices, with plaintiff paying the expert's fees and costs and a $5,000 security in the event of damages resulting from improper seizure. The order also directed that no physical items would be seized, except for the time required to copy them, satisfying the requirement that the seizure order be as narrow as possible. The order directed that the copied material be taken immediately into the court's custody and that defendants have the opportunity to review the seized materials to determine if any are privileged, personal, or irrelevant. The order reasoned that these and other protections satisfied the requirements and protections of the DTSA's seizure provisions.

***Great Am. Opportunities, Inc. v. Kent*, 352 F. Supp. 3d 1126 (D. Colo. 2018).** Defendant is a former sales representative of plaintiff, and previously signed an employment agreement with plaintiff that contained a two year non-compete provision. After defendant resigned from plaintiff, he formed an allegedly competing business, then plaintiff responded by filing suit, including claims of breach of the employment agreement and trade secret misappropriation. The court denied defendant's motion for summary judgment that the employment agreement's non-competition provision was unenforceable under Colorado law. While Colorado has a statute prohibiting non-competition agreements, the statute has an exception for contracts aimed at protecting trade secrets. The court held that the employment contract's non-competition provision was aimed at least in part at protecting trade secrets. If the information defendant allegedly took from plaintiff did indeed qualify as a trade secret, then the agreement would be enforceable. The Court ruled that it could not determine at the summary judgment stage whether the information at issue qualified as a trade secret.

11th Circuit

***Advice Interactive Grp., LLC v. Web.com Grp., Inc.*, 734 Fed. App'x. 712 (11th Cir. 2018) (unpublished).** Plaintiff, an online marketing company, brought action against defendant, an online services provider, alleging copyright infringement and misappropriation of trade secrets arising out of defendant's alleged use of plaintiff's technology for monitoring its clients' online presence and accuracy of information appearing in search engines. Defendant contracted plaintiff to request information and a demonstration of plaintiff's online marketing service. Thereafter, the parties signed two nondisclosure agreements, executed a formal service agreement (pursuant to which defendant agreed to pay for plaintiff's online services) and engaged in ongoing discussions about potential acquisition of plaintiff by defendant. Defendant then cancelled abruptly its service agreement with plaintiff and indicated that it was moving the services "in-house." The United States District Court for the Middle District of Florida granted plaintiff's motion for preliminary injunction enjoining defendant from using or offering for sale its version of plaintiff's service. The court held that no reversible error has been shown and affirmed.

***Smart Profitability Sols., LLC v. Double Check Risk Sols., LLC*, 2018 WL 6380886 (N.D. Ga. 2018) (unpublished).** The court found that plaintiff's inadvertent disclosure of its customer names does not automatically terminate its right to trade secret protection in this information, under the Georgia Trade Secrets Act. The court granted a preliminary injunction for the use of trade secrets and confidential information covered under a non-disclosure agreement, including: (1) using and/or possessing the confidential information contained in (a) plaintiff's August 2017 Insurance

Customer List ("ICL"); (b) plaintiff's December 2017 "Portfolio" and "BTR Portfolio;" or (c) plaintiff's 2018 Strategic Plan Starter; (2) doing business with or soliciting for business: (a) any customer listed on the ICL, plaintiff's December 2017 Portfolio and BTR Portfolio, or 2018 Strategic Plan Starter; (b) all of the specific, individual brokers identified on the ICL, with the exception of Yates Insurance Agency employees Jeffery Blanton and Danny Yates; or (c) any referral source on the ICL to the limited extent that such business is related to any customer listed on the ICL; and (3) breaching (or aiding the breach of) the non-disclosure and non-recruitment provisions of Marsha's employment agreement with plaintiff.

Federal Circuit

***Texas Advanced Optoelectronic Sols., Inc. v. Renesas Elecs. Am., Inc.*, 895 F.3d 1304 (Fed. Cir. 2018)**. The Federal Circuit held that the Seventh Amendment does not provide a right to a jury trial on the remedy of profit disgorgement for a trade secret claim. TAOS sued Renesas (formerly known as Intersil) for patent infringement, trade secret misappropriation, breach of contract, and tortious interference, alleging that after the parties' confidential merger negotiations, Intersil used TAOS's technical and financial data in Intersil's newly released ambient light sensors. A jury returned a verdict for TAOS, awarding damages for, *inter alia*, disgorgement of Intersil's profits and exemplary damages for trade secret misappropriation. On appeal, Intersil argued that the trial court should not have relied on the jury's verdict on disgorgement as a remedy for trade secret misappropriation because disgorgement is an equitable remedy to be determined by the court, requiring findings of fact and conclusions of law. This raised the question of whether the Seventh Amendment afforded TAOS the right to a jury determination on disgorgement. The Federal Circuit cited Supreme Court precedent stating that, in evaluating whether a right to a jury trial is afforded by the Seventh Amendment, the Court "first asks if the 'cause of action' was tried at law in 1791 or is 'analogous to one that was,' and then asks if the particular 'trial decision'—such as the 'remedy' determination after finding 'liability'—must be decided by the jury in order to preserve the jury-trial right on the cause of action as it existed in 1791." The question for the Federal Circuit was, therefore, "whether disgorgement of the defendant's profits . . . was available at law in 1791 for this sort of wrong." The answer, according to the Federal Circuit, is "no." The court found that patent, copyright, and trademark infringement were appropriate analogues of TAOS's trade secret claim, and that no disgorgement was available at law in 1791 for any of those claims. The court therefore concluded that TAOS had no Seventh Amendment right to a jury determination on disgorgement as a remedy for trade secret misappropriation and vacated the disgorgement award.

State Cases

New Hampshire

***Vention Med. Advanced Components, Inc. v. Pappas*, 188 A.3d 261 (N.H. 2018)**. Vention, a medical device components manufacturer, sued Pappas and Ascend Medical for misappropriation of trade secrets under the New Hampshire Uniform Trade Secrets Act ("UTSA"). Vention makes medical balloons, medical tubing, and heat shrink tubing ("HST"). Pappas worked for Vention for ten years. During his employment, where he signed a confidentiality agreement, Pappas was exposed to Vention's confidential HST technology and information. He also had knowledge of Vention's business and marketing information and strategies, including sales volumes for Vention's various products. Immediately after he left Vention, Pappas established Ascend and was

actively marketing his own design of HST. After examining Ascend's HST samples, Vention petitioned the trial court for injunctive and other relief under the UTSA. The trial court concluded that the defendants misappropriated Vention's trade secret, and issued five injunctions, including a perpetual ban for the production and marketing of HST made from polyester and another ten-year ban for HST made from other material, and for the destruction of all their equipment and designs. The Supreme Court of New Hampshire held that although the injunctions issued prohibited conduct that fell outside the scope of Vention's trade secrets, they did so only for the limited purpose of placing the burden on Pappas and Ascend to prove that they were not using Vention trade secret technology. The court also affirmed the perpetual and ten-year injunctions, given evidence that the product could not be reverse engineered, that plaintiff's process had not been duplicated by any competitor, and that to do so would take a company seeking to develop the trade secret technology at least four to five years to do so. The evidence was sufficient to support the trial court's ruling that Vention's trade secrets were unique and that Ascend's process for making HST was not based upon publicly available information or upon a former employee's industry knowledge and experience. Finally, the court held that, although defendants' machine was not identical to Vention's, it employed Vention's trade secrets, and it was thus proper to order the destruction of defendants' machine.

New York

***Brown & Brown, Inc. v Johnson*, 158 A.D.3d 1148 (N.Y. App. Div. 2018).** Plaintiffs terminated Johnson from her position and she was hired by Brown's competitor, Lawley. Plaintiffs brought causes of action alleging that Johnson breached their employment agreement, which contained a non-solicitation covenant. Plaintiffs also brought causes of action alleging that Johnson misappropriated confidential and proprietary information. The court refused to partially enforce the non-solicitation covenant because plaintiffs failed to show that the covenant was not a "use of dominant bargaining power … but ha[d] in good faith sought to protect a legitimate interest." *BDO Seidman v. Hirshberg*, 93 N.Y.2d 382, 394 (1999). The non-solicitation covenant had been imposed as a condition of employment after Johnson had left her prior employer and her position had been filled, indicating that plaintiffs held dominant bargaining power. In addition, plaintiffs imposed a non-solicitation covenant on all of its employees, undermining plaintiffs' contention that it was imposed with a legitimate business interest. The court also found that plaintiffs could not maintain a claim of misappropriation of confidential and proprietary information because the information at issue was readily ascertainable outside of plaintiffs' business.

***E.J. Brooks Co. v. Cambridge Sec. Seals*, 31 N.Y.3d 441 (2018).** E.J. Brooks Company, doing business as TydenBrooks, is the largest manufacturer of plastic indicative security seals in the U.S. TydenBrooks brought an action in the United States District Court for the Southern District of New York against a rival manufacturer, Cambridge Security Seals (CSS). TydenBrooks alleged that its former employees misappropriated trade secrets of a process for manufacturing plastic indicative security seals when the employees defected to CSS. TydenBrooks asserted causes of action including common law misappropriation of trade secrets, unfair competition, and unjust enrichment, and sought damages based on defendant's avoided costs. Under the avoided cost theory, TydenBrooks sought monetary relief in an amount equal to the difference between the costs CSS actually incurred in developing and using TydenBrooks's manufacturing process and the costs that CSS would have incurred had it not misappropriated TydenBrooks's process. At trial, the jury found CSS liable for all three claims and awarded TydenBrooks a $3.9 million

judgment. On appeal, the Second Circuit certified a question to the Court of Appeals of New York to decide whether, under New York law, a plaintiff asserting claims of misappropriation of a trade secret, unfair competition, and unjust enrichment can recover damages measured by the costs the defendant avoided due to its unlawful activity. The New York Court answered the question in the negative, and held that for each of these claims, damages may not be measured by the defendant's avoided development costs. The court explained that while the defendant's gains may be evidence of the plaintiff's losses, they may not be taken as the actual measure of the plaintiff's losses.

Ohio

***Sheil v. Horton*, 117 N.E. 3d 194 (Ohio Ct. App. 2018).** In this case a television journalist (Sheil) made a public records request for an unredacted copy of a speaking engagement contract between a foundation connected with Cuyahoga Community College ("Tri-C Foundation") and a guest speaker, Octavia Spencer. One issue was whether the redacted portions of the contract with Spencer constituted trade secret information. The court noted that the Ohio Public Records Act excepted trade secrets from production. Tri-C Foundation asserted that the redacted terms of contract were trade secrets: "business information that (1) derives independent economic value and (2) is subject to efforts that are reasonable under the circumstances to maintain its secrecy." Yet Tri-C Foundation did not identify any contractual term with specificity, other than the fee paid to Spencer for the speaking engagement. The court noted that information about Spencer's similar contracts for speaking engagements, which revealed (amongst other information) Spencer's speaking fee, were publicly available. The court then held that the essence of the information redacted from the Spencer contract was known publicly and thus Tri-C Foundation had not established that the redacted portions of the Spencer contract derived independent economic value from not being readily ascertainable from other proper means. Finding that the redacted portions of the Spencer contract were not trade secrets, the court ordered production of the unredacted contract pursuant to the public records request.

***Boehm v. Black Diamond Casino Events, LLC*, 116 N.E. 3d 704 (Ohio Ct. App. 2018).** Black Diamond operates a casino-games-themed events business for corporate and private parties. Boehm, a former employee, approached the owners about buying two of the four-member interests in that company. In conjunction with due diligence, Boehm signed a nondisclosure agreement ("NDA") and obtained Black Diamond's customer information, tax returns, financial statements and vendor information. Boehm then elected to move forward to purchase the two interests, but the interest holders refused to sell. Boehm sued for breach of an oral contract to sell. Black Diamond intervened asserting, via counterclaim, Boehm's violation of the Ohio Uniform Trade Secrets Act ("Act"). The matter went to trial only as to Black Diamond's claim that Boehm violated the Act. The trial court found in favor of Boehm and Black Diamond appealed. The appeals court found that Black Diamond's client list, tax returns and financial statements qualified as trade secrets under the Act. The appeals court further found that to sustain a claim of misappropriation under the Act, proof of damages was not required. The appeals court also found that Boehm's retention of copies of the trade secret information beyond the time allowed under the NDA constituted a misappropriation and his sharing of the documents with his accountant, without having the accountant sign an NDA, was also a technical violation of the Act. The appeals court, however, upheld the trial court's ruling that Black Diamond was not entitled to injunctive relief under the Act because Boehm returned all the information back to Black Diamond as part of the litigation and had retrieved it from his accountant when the proposed purchase fell through.

The appeals court also affirmed that Black Diamond was not entitled to damages under the Act – no evidence presented demonstrating actual loss or unjust enrichment and insufficient evidence put forth to award a reasonable royalty.

Vermont

***Long v. City of Burlington*, 199 A.3d 542 (Vt. 2018)**. Codefendants City of Burlington and BTC Mall Associates ("BTC") entered into a predevelopment agreement for a public-private partnership in a $222 million redevelopment project in downtown Burlington. Pursuant to the agreement, the city required BTC to provide information regarding feasibility analysis and marketing studies. The agreement additionally stated that all parties would treat "proprietary and confidential information" appropriately. In due course, BTC provided the city and the public a copy of the marketing study, but with key financial data redacted. Plaintiffs Coalition for a Livable City and Long requested that the city release the unredacted study pursuant to Vermont's Public Records Act ("PRA"). The city attorney denied the request, stating the nondisclosure agreement and the PRA's trade secrets exemption prohibited disclosure. Plaintiffs filed suit against the city and BTC. The trial court dismissed plaintiffs' claims on summary judgment, stating the study was not a public record under the PRA, and additionally, the information was a trade secret and thereby exempt from disclosure. On appeal, plaintiffs claimed the study should be denied trade secret status as it contained financial estimates rather than BTC's trade information, and furthermore, BTC made insufficient efforts to maintain its secrecy. Assuming the documents to be public records for the purposes of its decision, the Supreme Court of Vermont nonetheless concluded that the information contained within the documents fell under the PRA exemption, as trade secrets need not be "in the nature of intellectual property." The exemptions under the statute clearly list "compilations of information" as exempt from disclosure. As such, "sensitive financial data that gives its possessor advantage over others" was exempt. The court reasoned that to find otherwise would cause contractors and service providers to decline to cooperate with the state in the bid process. The court further concluded that BTC had made reasonable efforts to keep the information secret.