ABA Section of Intellectual Property Law, Trade Secrets and Interferences with Contracts Committee Annual Trade Secret Law Report 2016/2017

This 2017 edition contains contributions or assistance from the following lawyers: D. Joshua Salinas, Klaus H. Hamm, Robert Milligan, John F. Zabriskie, Jason Britt, Hayley Altabef, Kimberly F. Rich, Amanda Praestholm, Amy Abeloff, Jessica Mendelson, C. Todd Norris, Bart Quintans, Nathalie Knight, Kami LaBerge, Emily Erdman, Keia Atkinson, Anna Skaggs, Paul Holton, Lara A. Levine, Aaron Lubeley, Amanda Frey, Olivia J. Wada, Dena Sanders, Linda Ryan, MiRi Song, Caitlin Wang, Alexander Kargher, Emily Stover, Alex W. Dockery, Shannon Pierce, Veronica Peterson, Doug Thornley, Michael Cross, Anjuli Cargain, Shadee Navid, and Heather J. Zacharia.

1st Circuit

***Iconics, Inc. v. Massaro,* 266 F. Supp. 3d 461 (D. Mass. 2017)**. Iconics alleged that the defendants misappropriated its trade secrets in violation of Massachusetts trade secret law in developing their Energy Studio Pro product. The defendants moved for summary judgment arguing (a) they did not misappropriate the alleged trade secrets and (b) the alleged subjects were not trade secrets either because Iconics publicly disclosed them or because they involved the sort of public or general knowledge beyond trade secret protection. The court addressed three claimed trade secrets. It denied summary judgment as to Iconic's "core architecture" because (i) although it was disclosed publicly on April 9, 2009, Iconics was claiming misappropriation between January and April 2009 and (b) in light of its expert's testimony that an alleged 2008 disclosure did not disclose the trade secret, a reasonable jury could conclude that it disclosed only aspects, and not the full trade secret. As to Iconic's claimed "data intake" trade secret, the defendants "seem[ed]" to argue that Iconics failed to define the trade secret with adequate specificity, and that it altered the definition throughout the litigation. The court agreed that Iconics had failed at times to explain with precision what the trade secret was, but that any earlier difficulties had been addressed in response to the court's prior order in which Iconics defined the "'data intake' trade secret both with technical specificity and 'with clarity that can be understood by a lay person.'" [Citation omitted.] Drawing all inferences in Iconics' favor, including the conclusions of Iconics' expert report, the court concluded that a reasonable jury could conclude that the defendants had in fact misappropriated the trade secret. The court likewise rejected the defendants' contention that the trade secret was in the public domain, reasoning that "a trade secret can be based on elements 'each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret.'" [Citation omitted]. Finally, as to Iconics' claimed "Workflow" trade secret, the court concluded that drawing all inferences in Iconics' favor, a reasonable jury could conclude that the defendants used the workflow trade secret but failed to implement it in a way that realized one of its benefits. However, the failure to maximize its value did not mean there had been no misappropriation. The court rejected the defendants' assertion that the trade secret had been publicly disclosed because the defendants' argument was unresponsive and failed to address the true definition of the trade secret at issue.

***TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo,* 2017 U.S. Dist. LEXIS 49838 (D.C.P.R. 2017)**. TLS brought an action against the defendants alleging, among other things, violation of the Industrial and Trade Secret Protection Act of Puerto Rico (the "Act"). TLS stored information about its tax strategies, insurance strategies, customer lists, and other confidential information on an online business account at the domain name "Dropbox.com." The Dropbox was for the exclusive use of TLS employees and required a business account to be used in compliance with TLS's terms and policies. Defendant Rodriguez was hired by TLS after working for one of its subcontractors. Rodriguez resigned from TLS about two years later but not before forming his own company GOS, a competitor of TLS. Before resigning, Rodriguez transferred many confidential documents, including a template of TLS's operating agreement, from TLS's Dropbox into a "GOS" folder. Under the Act, if it is proven that a trade secret has been misappropriated, the court may issue a preliminary injunction without proof of irreparable damages. TLS proffered multiple examples of misappropriation, including conversations with TLS's clients in which Rodriguez referenced TLS's business methods and procedures and a TLS pricing formula. Defendants contended TLS was nonetheless not entitled to an injunction because there was no evidence that Rodriguez intercepted TLS's Dropbox without authorization. The court rejected that argument, noting that although unlawful interception or access is a linchpin of other statutes, it is not required under the Act in question. Rodriguez next argued he was permitted to use TLS's confidential information in advising clients who no longer wanted to use TLS's services. In rejecting that argument, the court reasoned, *inter alia,* that due to the copying mentioned above, there was a reasonable inference that GOS had obtained TLS's confidential information. Rodriguez further argued that he had kept some of TLS's confidential documents in case they were needed for a peer-review process. The court found that argument meritless because Rodriguez admitted he was not subject to the peer review program, and even if he were, it did not do away with all the communications he had had with third parties in which he disclosed information that was likely TLS's trade secrets. Next, Rodriguez argued an injunction should not issue because he had reported to the IRS unlawful conduct by TLS, but the court declared the injunction that would issue should not be interpreted to prohibit the defendants from participating in any proceedings before a government agency. Finally, the defendants argued the motion for a preliminary injunction was moot because Rodriguez no longer had any confidential documents. The court rejected that argument also because Rodriguez likely could recall confidential information and because voluntary cessation of allegedly unlawful conduct ordinarily does not suffice to moot a case. The injunction was granted.

<u>2nd Circuit</u>

***In re Document Techs. Litig*, 2017 U.S. Dist. LEXIS 104811 (S.D.N.Y. 2017)**. DTI, an e-discovery company, acquired another company, Epiq, which employed four salespeople as high level sales personnel. These salespeople had signed agreements containing restrictive covenants, including a one-year noncompete provision, a one-year nonsolicitation provision, a nondisclosure provision, and a covenant to return the company's confidential information upon termination of employment. DTI's competitor, LDiscovery, began recruiting the salespeople, and in May 2016, LDiscovery's CEO met with them to discuss a transition. In preparation for the meeting, the salespeople provided their DTI sales revenue and performance information to LDiscovery. In January 2017, the salespeople signed employment agreements with LDiscovery under which they agreed to resign from DTI by the end of the month and take a "sabbatical year" during which LDiscovery would not provide any work or information restricted by their agreements with Epiq. The agreements further provided that each salesperson would receive a sizable signing bonus to be paid throughout the sabbatical year and that DTI would indemnify them for attorneys' fees and damages relating to their transition from DTI to LDiscovery. The salespeople resigned from DTI in January 2017; although they returned their laptops and mobile devices, one salesman failed to return a thumb drive with a backup of his company laptop. Then, at the end of January, one salesman contacted DTI and asked for a list of invoices paid by his clients to confirm his commission check; DTI accidentally forwarded a list of all of the company's invoices for the entire month to him, and he forwarded that list to the other salesmen. In February 2017, the salesmen planned to meet to discuss their sales strategy at LDiscovery. This meeting never occurred because DTI sent a cease and desist letter then brought an injunctive relief action against LDiscovery, LDiscovery's CEO, and the salespeople. DTI moved for a preliminary injunction against LDiscovery and the salespeople.

With respect to LDiscovery, DTI contended that LDiscovery tortiously interfered with DTI's relationships with existing and prospective customers by intentionally inducing the four individuals to breach the restrictive covenants in their employment agreements. The court was not persuaded, finding that DTI had not shown a likelihood of success on the merits because LDiscovery's indemnification of and provision of a signing bonus to the salesmen was not sufficient to establish a tortious interference claim. The court also determined that DTI had not established a likelihood of succeeding in its trade secret misappropriation claim because the documents at issue—the salesmen's revenue and performance information—did not constitute trade secrets. With respect to the individual salesmen, the court held that DTI had not shown a likelihood of success on the merits on its breach of contract claims with respect to the restrictive covenants. The court found that one salesman's failure to return a thumb drive was not sufficient because it was inadvertent and a forensic analysis confirmed that he never accessed the drive. It further found that the salesman's decision to forward the invoice list to the other salesmen was not improper because he testified that he believed the other salesmen would want to confirm their own commissions. Accordingly, the court denied DTI's motion for a preliminary injunction.

In re Document Techs. Litig**, 2017 U.S. Dist. LEXIS 116369 (S.D.N.Y. 2017)**. DTI, an e-discovery company, brought a claim for injunctive relief against its former sales employees and its competitor, LDiscovery, and its CEO, alleging that the former employees conspired with LDiscovery to misappropriate its trade secrets (under the DTSA and New York trade secret law) and solicit their customers in violation of their employment agreements. The court dismissed the complaint for failure to state a claim and issued an order denying DTI's motion for a preliminary injunction. DTI filed an amended complaint, and LDiscovery and its CEO again moved to dismiss. DTI alleged that its former employees began accessing its customer relationship management software around the time of a meeting with LDiscovery's CEO and that at that time, LDiscovery incentivized the former employees to unlawfully access DTI's computer systems by offering and providing full commission credit three months later. The court found that a full commission credit offer three months after the employees' alleged conduct was not sufficient to constitute an incentive. DTI also alleged that LDiscovery misappropriated its trade secrets because its former employees emailed LDiscovery's CEO their historical sales revenue and performance with DTI. The court found that this allegation was not sufficient to establish a misappropriation claim because that revenue information is not protectable as a matter of law because it is industry practice for e-discovery providers to ask potential sales hires for their past revenue figures.

Next Communs., Inc. v. Viber Media, Inc., **2017 U.S. Dist. LEXIS 162405 (S.D.N.Y. 2017)**. The court dismissed a claim for trade secret misappropriation under New York state law on summary judgment where the plaintiff had named three specific components on summary judgment that were absent from its operative complaint, and those components in any event "merely consist[ed] of vague descriptions and rudimentary graphics and concepts" that the plaintiff could not sufficiently explain, beyond conclusory allegations, to be unique or secret.

ScentSational Techs. LLC v. PepsiCo Inc.**, 2017 U.S. Dist. LEXIS 162723 (S.D.N.Y 2017).** ScentSational Technologies, LLC ("Plaintiff") sued PepsiCo, Inc., Pepsi-Cola Technical Operations, Inc., The Quaker Oats Company, Stokely-Van Camp, Inc., and Tropicana Products, Inc. (collectively, "Defendants"), asserting claims for misappropriation of trade secrets (under New York state law), breach of contract, unfair competition, unjust enrichment, the imposition of a constructive trust, and the correction of inventorship of an issued patent. Over the course of an almost decade-long relationship, Plaintiff contended that it disclosed confidential and trade secret information relating to the development of aromatic food and beverage packaging to Defendants and that Defendants then misappropriated that information for their own benefit. Defendants moved for summary judgment because Plaintiff had not proffered evidence sufficient to support its claims. Defendants argued that Plaintiff's misappropriation of trade secrets claim should not proceed to trial because there was no evidence that Plaintiff ever possessed any of its 11 claimed trade secrets, that Defendants misappropriated those trade secrets, or that Plaintiff suffered damages as a result. The court granted summary judgment in favor of Defendants as to the damages aspect of Plaintiff's trade secret claim regarding a contemplated project with Coke, finding that there was no evidence that Plaintiff ever suffered damages as a result of the alleged misappropriation. The court denied summary judgment as to the issues of whether Plaintiff possessed a trade secret or Defendants misappropriated such trade secrets. The court explained that Defendants' focus on the lack of documented evidence of alleged trade secrets was misplaced because documentation is not a requirement, nor must a plaintiff demonstrate the economic value of the alleged trade secrets; rather, a plaintiff need only demonstrate "competitive advantage."

<u>3rd Circuit</u>

Fres-co Systems USA, Inc. v. Hawkins**, 2017 WL 2376568 (3rd Cir. June 1, 2017)**. The Third Circuit Court of Appeals applied the inevitable disclosure doctrine to uphold a preliminary injunction order entered against the plaintiff's former employee. The plaintiff former employer brought an action against its competitor and a former employee, a sales representative who began working for the competitor, alleging misappropriation of trade secrets (under both the DTSA and Pennsylvania UTSA) and to enforce a non-competition agreement. The United States District Court for the Eastern District of Pennsylvania granted the former employer's motion for preliminary injunction to bar former employee from disclosing the former employer's confidential information and from soliciting 12 clients whom former employee had serviced while at former employer. On appeal, the Third Circuit upheld the preliminary injunction order and explained: "[g]iven the substantial overlap (if not identity) between Hawkins's work for Fres-co and his intended work for Transcontinental—same role, same industry, and same geographic region—the District

Court was well within its discretion to conclude Hawkins would likely use his confidential knowledge to Fres-co's detriment." The Third Circuit was not clear whether its application of the inevitable disclosure doctrine was based solely on the Pennsylvania UTSA, as opposed to the DTSA, although it appears to have been based on both.

***Advanced Fluid Sys. v. Huber*, 2017 U.S. Dist. LEXIS 86145 (M.D. Pa. 2017).** AFS distributes, manufactures, and installs hydraulic components for engineering projects. Huber was employed at AFS as a full-time sales engineer until he left his position to start his own firm. Prior to leaving AFS, Huber took affirmative steps to help competitors familiarize themselves with AFS's hydraulic systems. AFS asserted claims against Huber for misappropriation of trade secrets (under the Pennsylvania UTSA) and breach of the fiduciary duty of loyalty. Huber contended that AFS could not pursue a misappropriation claim because it was not the legal owner of all materials generated for the hydraulic system in question. The court concluded that ownership, in the traditional sense, was not a prerequisite to a misappropriation claim, and that one need only demonstrate lawful possession of a trade secret to maintain a claim. The court granted AFS's motion for summary judgment on its misappropriation claim against Huber, finding that Huber clandestinely downloaded hundreds of thousands of proprietary files from AFS's password-protected servers on the eve of his resignation, with knowledge that the documents were valuable trade secrets.

***Alpha Pro Tech, Inc. v. VWR Int'l, LLC*, 2017 U.S. Dist. LEXIS 135507 (E.D. Pa. 2017)**. The court granted summary judgment for the defendant on the plaintiff's trade secret misappropriation claim (under the Pennsylvania UTSA) because the defendant's reverse engineering argument foreclosed possibility that plaintiff protected its trade secret.

***Arkeyo, LLC v. Cummins Allison Corp.*, 2017 U.S. Dist. LEXIS 100605 (E.D. Pa. 2017)**. Arkeyo creates software that integrates with coin counting machines. Cummins manufactures and sells coin counting machines. Arkeyo and Cummins agreed that Arkeyo would purchase coin counting machines from Cummins, attach them to its custom computers, configure them with Arkeyo's software, and then Arkeyo would resell the machines for installation in banks. Prior to working together, the parties entered into a nondisclosure agreement to protect the disclosure of proprietary and confidential information regarding Arkeyo's software to third parties. Thereafter, Arkeyo collaborated with Cummins to create software compatible with Cummins's coin counting machine. Arkeyo alleged that Cummins misappropriated its trade secret software (in violation of the Pennsylvania UTSA) and thus sought a preliminary injunction to enjoin Cummins from selling its coin counting machines directly to any customer in circumstances where the machine is sold as part of a system that includes software derived in whole or in part from the Arkeyo software. The court denied Arkeyo's motion for a preliminary injunction because Arkeyo was unable to meet the threshold requirement of demonstrating a likelihood of success on the merits. The court found that Arkeyo's decision to make its software publicly available on the internet for 15 months without taking standard precautions to protect its confidentiality demonstrated that it did not take reasonable steps to protect its trade secrets. Arkeyo argued that it took reasonable measures to protect its trade secrets by executing nondisclosure agreements. However, the court found that the nondisclosure agreements became ineffectual once Arkeyo published its trade secrets on the internet because Arkeyo made its software publicly available to individuals who owed no duty of nondisclosure to Arkeyo.

***AutoTrakk, LLC v. Auto. Leasing Specialists, Inc.*, 2017 U.S. Dist. LEXIS 106188 (M.D. Pa. 2017)**. Plaintiff AutoTrakk, LLC filed suit against two former employees, Michael Caffrey (president) and George Stauffer (vice president of sales) and their new employer, Ambassador Dealer Funding. Each signed forms acknowledging they had received AutoTrakk's policy manual that notified employees of the "duty not to disclose proprietary trade secrets or confidential information obtained during the course of employment," and Stauffer also signed a confidentiality agreement. Caffrey resigned from AutoTrakk, began working for Ambassador, and allegedly sent emails to Stauffer seeking specific information concerning AutoTrakk's computer program. Stauffer allegedly received an offer of employment from Ambassador in exchange for this information, which he accepted. AutoTrakk alleged that Caffrey and Stauffer misappropriated some of AutoTrakk's proprietary information for Ambassador's benefit in violation of the DTSA and Pennsylvania UTSA. The court granted Ambassador's motion to dismiss this claim without prejudice on the ground that the information Ambassador allegedly took from AutoTrakk to create its own program was publicly available on AutoTrakk's own website and well known in the automotive financing industry. The court, however, recognized that a trade secret claim may exist where there have been post-patent or otherwise secret refinements. It noted that the Third Circuit had alluded to the existence of these claims, but the district court clarified that this type of claim is indeed cognizable. Because the claim was cognizable and the complaint failed to allege sufficient facts to state a plausible claim for misappropriation of trade secrets, the court gave AutoTrakk leave to amend and indicated that it would be willing to allow AutoTrakk to plead facts under seal demonstrating that its program contained secret advances surpassing common knowledge.

***Astor Chocolate Corp. v. McCall*, 2017 U.S. Dist. LEXIS 82567 (D.N.J. 2017)**. The court denied the defendant's motion to dismiss the plaintiff's misappropriation of confidential information claim because the record was insufficient as to where and when confidential information was allegedly disclosed. The court also concluded that it was unable to make a determination as to whether New Jersey or New Hampshire law applied at the pleading stage based on the lack of sufficient evidence.

***Brand Energy & Infrastructure Servs. v. Irex Contr. Grp.*, 2017 U.S. Dist. LEXIS 43497 (E.D. Pa. 2017)**. Construction Company Brand Energy & Infrastructure Services provides scaffolding, industrial coatings, and other construction-related services. Brand alleged that several of its former employees stole its trade secrets and equipment, and misappropriated its proprietary business information. Brand alleged that these former employees left Brand and joined Irex Corporation, one of Brand's competitors, to benefit Irex and poach business from Brand. Irex brought a motion to dismiss these claims, including a DTSA claim, alleging that the DTSA does not apply because it was enacted after the allegedly unlawful acts took place. The court denied the motion to dismiss, holding that the DTSA applied to misappropriations that occurred after the enactment of the DTSA, or even those that continued to occur after the enactment. Through the proposition that the DTSA applies to misappropriations that began prior to the enactment date so long as the misappropriation continued to occur after the enactment date, the court specifically rejected Irex's constitutional challenged based on the prohibition against ex post facto law.

***Chubb INA Holdings, Inc. v. Chang*, 2017 U.S. Dist. LEXIS 16744 (D.N.J. 2017)**. The court denied a competitor insurance company's motion to dismiss the plaintiff insurance company's DTSA claim where factual allegations that the plaintiff's former employee worked in concert with the defendant competitor to recruit other employees who had sent confidential information to personal email accounts and data storage devices, supported an inference that the defendant competitor had used misappropriated trade secrets.

***Gov't Emps. Ins. Co. v. Nealey*, 2017 U.S. Dist. LEXIS 91219 (E.D. Pa. 2017)**. The plaintiff insurance company brought action alleging that a Washington attorney and California attorney representing plaintiffs in class actions against insurer in Washington misappropriated trade secrets by sharing insurer's employee's affidavit with their expert witness, and that in so doing, attorneys violated the DTSA. The defendant attorneys moved to dismiss for lack of personal jurisdiction and for failure to state a claim. The court found that since the plaintiff insurance company took steps (including filing a protective order and submitting affidavits and public filings) to protect its alleged trade secrets, consisting of customer claims data, the court could determine whether the company took reasonable measures to protect trade secrets in ruling on whether to dismiss DTSA claim. The court rejected the plaintiff's contention that the reasonable measures determination was a question of fact that could not be made at the pleadings stage. The court dismissed the DTSA claim without prejudice after finding that the insurance company had not taken reasonable measures because it relied on what it alleged were trade secrets to argue that the amount in controversy was met in its notice of removal, and in entering into a protective order, failed to label the supporting affidavit as confidential as required.

***High 5 Games, LLC v. Marks*, 2017 U.S. Dist. LEXIS 9302 (D.N.J. 2017)**. The court granted the plaintiff's motion to amend its complaint in order to bring a claim under the DTSA even though the alleged conduct at issue occurred prior to the enactment of the DTSA. The court acknowledged that other courts have considered continuing post-enactment conduct and that deeming the DTSA claim as futile on a motion for leave to amend would be premature. The court further explained that to the extent the DTSA claim is viable would depend on the adequacy and specificity of the allegations in the pleading, which is more appropriate for a Rule 12(b) (6) motion instead of a Rule 15 motion to amend.

***Marimar Textiles, Inc. v. Jude Clothing & Accessories Corp.*, 2017 U.S. Dist. LEXIS 163458 (D.N.J. 2017)**. The court held that the DTSA is not retroactive while recognizing that allegations of pre-enactment acquisition of a trade secret, coupled with post-enactment continued use, are sufficient to sustain a claim under the DTSA at the motion to dismiss phase.

***Mifflinburg Tel., Inc. v. Criswell*, 2017 U.S. Dist. LEXIS 164273 (M.D. Pa. 2017)**. The court granted summary judgment on the plaintiff publishing company's Pennsylvania

UTSA claim against its former employee who had taken the plaintiff's customer lists for use at competing company she had started.

4th Circuit

***AirFacts, Inc. v. de Amezaga*, 2017 U.S. Dist. LEXIS 133483 (D. Md. 2017)**. The court held that the plaintiff employer failed to prove that the defendant employee misappropriated trade secrets (under the Maryland UTSA) when the defendant employee emailed work related documents to his personal email prior to his last day of work. The court highlighted that the employee was instructed to and did continue to work on an assigned project through his last day. The court noted that the defendant emailed the documents to himself at his personal email address as he had previously done in order to work remotely. The court further noted that his may not have been an explicitly authorized practice, but other employees also used personal email accounts for plaintiff's business or worked on home computers. Forensic evidence also showed the information was not accessed after the end of the defendant's employment.

***CSS, Inc. v. Herrington*, 2017 U.S. Dist. LEXIS 120396 (S.D.W.V. 2017)**. The court denied the plaintiff company's motion for preliminary injunction because the misappropriation of trade secrets claim (under the West Virginia UTSA) was not likely to succeed on merits. The court reasoned that the alleged trade secret source code was available for some time on county servers and was not password-protected or encrypted, the alleged trade secret client list was publicly available information, alleged trade secret pricing methodology was not unique, and alleged trade secret plans of expansion and customer preferences were not kept confidential.

***Integrated Glob. Servs. v. Mayo*, 2017 U.S. Dist. LEXIS 148355 (E.D. Va. 2017)**. The court granted the plaintiff company's motion for preliminary injunction for alleged trade secret misappropriation (under the DTSA and Virginia UTSA) because the defendant employee took one month to return his work computer to employer; forensics showed that several documents had been accessed, downloaded, and deleted after his employment was terminated; the defendant should have known this was not permitted; and the defendant secured employment with a direct competitor.

***PC Connection, Inc. v. Mereos*, 2017 U.S. Dist. LEXIS 41012 (D. Md. 2017)**. Applying New Hampshire law, the court granted a preliminary injunction against the defendant former employee for breach of his nondisclosure agreement because the agreement was sufficiently narrowly tailored, the plaintiff company showed that the defendant likely violated it by forwarding company information to a nonsecured, external email address, and the plaintiff would suffer irreparable harm because the information at issue provided a roadmap for stealing plaintiff's business.

***Tucker Auto-Mation of N.C., LLC v. Rutledge*, 2017 U.S. Dist. LEXIS 105890 (M.D.N.C. 2017)**. The court found that the plaintiff company sufficiently alleged misappropriation of trade secrets claim under North Carolina Trade Secrets Protection

Act because the list of confidential financial, customer, and other business information at issue was specific enough to survive a motion to dismiss and the plaintiff had sufficiently alleged that defendant, the plaintiff's former president, took files upon leaving and used confidential information to start a competing company.

5th Circuit

***Quantlab Techs., Ltd (BVI) v. Kuharsky*, 2017 U.S. App. LEXIS 11136 (5th Cir. 2017)**. Kuharsky and Mamalakis worked for Quantlab, a quantitative financial research firm that applies proprietary computer analytics to identify profitable trading opportunities. Quantlab fired Kuharsky and Mamalakis in 2007, and, in response, both men threatened to use Quantlab's information for their own benefit. Kuharsky not only failed to return Quantlab's confidential information after he was terminated, but he also copied large amounts of Quantlab's source code and other proprietary information. In 2009, Quantlab sued Kuharsky and Mamalakis for misappropriation of trade secrets (under Texas state law) and conspiracy, among other claims. Prior to trial, the parties argued over Quantlab's damages theories. The court entered a finding of liability against Kuharsky, based on Kuharsky's wide-ranging destruction of evidence and imposed damages against Kuharsky in the amounts of $1,800,000 for misappropriation and $5,400,000 for conspiracy to misappropriate; and against Mamalakis in the amounts of $1,000,000 for direct misappropriation and $4,000,000 for conspiracy to misappropriate. Both men appealed on various grounds. Kuharsky's appeal attacked the award of damages, arguing that it was improper to instruct the jury to determine damages based on "the value Quantlab's trade secrets." The Fifth Circuit affirmed the award. Kuharsky failed to point to a single example of evidence referencing the trade secret's "value to Quantlab." Before trial, Quantlab unambiguously asserted that the only measure of damages it sought were based on defendants' avoided costs and profits. During the trial, Kuharsky objected to damages testimony supposedly referencing the value of Quantlab's trade secrets. Although one of the jury instructions referenced the value Quantlab's trade secrets, the record shows that the jury never heard any amount of damages other than the development costs or the profits defendants earned. Thus, the jury could not have based its damages award on anything else.

***N. Am. Deer Registry, Inc. v. DNA Solutions, Inc.*, 2017 U.S. Dist. LEXIS 84867 (E.D. Tex. 2017)**. The court found that a database of deer genetic information and deer lineages was a trade secret (under the DTSA and Oklahoma UTSA) where the plaintiff "expended significant time and effort in creating" database, so defendant's failure to return information from database constituted misappropriation.

6th Circuit

***Am. Furukawa, Inc. v. Hossain*, 201 U.S. Dist. LEXIS 161650 (E.D. Mich. 2017).** Senior product manager Hossain worked for American Furukawa, Inc. ("AF"), a distributor of automotive and electrical components. Hossain did not sign a restrictive covenant agreement. Hossain, while still employed by AF began actively working for AF's direct competitor, Huatong, which did not have a Michigan presence until its hire of Hossain. During the period of time Hossain was in fact employed by both companies, he collected short term disability benefits from AF, in which he claimed he needed time off to recover from an injury. To collect these benefits, he represented he was not working during his recovery period. Following his return from leave, he announced his resignation. At the time of his resignation, he refused to sign an Employment Certification and Agreement on termination in which he would have affirmed that he had returned all property belonging to AF and that he had complied with and would continue to abide by the Invention Assignment and Secrecy Agreement, which prohibited the disclosure of confidential information and trade secrets. Within three weeks of Hossain's departure, AF learned that Hossain was using its pricing template and formulas to solicit business. Subsequent forensic analysis confirmed that Hossain had copied and accessed confidential information. AF sued, in pertinent part for breach of fiduciary duties. The court found that Hossain had breached his fiduciary duty when he commenced working for Huatong, not when he entered into an employment agreement with Huatong. Notably, the court found that AF's claims for fraud related to Hossain's undisputed misrepresentations were not viable following AF's knowledge of Hossain's actions. The court held that Hossain's refusal to sign the Employee Certification and Agreement upon termination precluded any reliance on his representations that he had returned all property and would continue to comply with the Invention Assignment and Secrecy Agreement. AF had learned of Hossain's employment with Huatong within three weeks of his resignation; therefore, because they could not offer evidence of loss within that finite period of time, and because Hossain's refusal to sign the relevant agreement precluded any reliance on his admittedly false previous representations that he was not working for another entity and had not used AF's information, AF's claim was not viable.

***Xoran Holdings LLC v. David Zurich and Tungsten Med.,* 2017 U.S. Dist. LEXIS 147868 (E.D. Mich 2017)**. Defendant Zurich was the director in sales for plaintiff Xoran, which developed, patented and sold CT scanners for medical use in offices and operating rooms. Zurich was subject to both nondisclosure and noncompetition provisions contained in his employment agreement. Zurich's employment with Xoran ended in 2016 and Xoran later discovered he had formed a new entity, Tungsten Medical Network, LLC. Xoran concluded that Zurich was violating his obligations after a Xoran employee saw him at a trade show. Subsequently, plaintiffs filed suit alleging misappropriation under the DTSA and Michigan state law, breach of contract and tortious interference with a contractual relationship. Plaintiffs sought exemplary damages and attorneys' fees under DTSA. Defendants argued that plaintiffs were not entitled to exemplary damages and attorneys' fees under the DTSA for two reasons: first, plaintiff failed to plead any facts to support their claim that defendant Zurich's conduct constituted on intentional and malicious breach of his confidentiality and noncompete agreements. Second, the agreement did not provide notice of employee whistleblowing immunity provisions governing the use of trade secrets. The court denied defendants' motion to dismiss on this basis holding that there was no heightened pleading standard referenced by the

DTSA. The court did, however, hold that the absence of the required notice of whistleblower immunity precluded recovery of attorneys' fees and exemplary damages under the DTSA. Plaintiffs also moved to dismiss defendant Zurich's counterclaim for wrongful discharge. Plaintiffs argued that this claim was subject to an arbitration agreement governing the parties' employment relationship. Ultimately, the court agreed that arbitration was the appropriate forum for defendant's claims, but found merit in defendants' argument that if the court granted this motion, any claim for monetary damages asserted by plaintiff should also be decided in arbitration. The court declined to issue an order because defendants had not presented this argument in a motion, but held that it would dismiss all such claims to binding arbitration once upon proper motion

7th Circuit

***Chatterplug, Inc. v. Digital Intent, LLC*, 2016 WL 6395409 (N.D. Ill. 2016)**. Plaintiff, a healthcare management technology company, sued Defendants, a technology consulting company and a physical therapy company, after they announced an app for rehabilitating patients that Plaintiff alleged contained trade secrets it had disclosed in confidence to the consulting company. Plaintiff's first amended complaint was ninety-six pages long and alleged twenty-nine counts, including claims for misappropriation of trade secrets under the DTSA and the Illinois Trade Secrets Act ("ITSA"). Defendants filed a motion to dismiss, arguing that Plaintiff's trade secret misappropriation claims failed to state a claim on which relief could be granted.

The court denied Defendants' motion without prejudice, but also dismissed Plaintiff's first amended complaint without prejudice and with leave to amend. The court found that the complaint's ninety-six pages contained repetitive allegations that violated Federal Rule of Civil Procedure 8's "short and plain statement" standard. At the same time, notwithstanding the pleading's length, the court also found that its description of the allegedly misappropriated trade secrets was too short and did not give Defendants adequate notice of what trade secrets were at issue. Plaintiff claimed trade secrets in three of its products, but failed to adequately describe any of the products themselves or the "general contours" of the alleged trade secrets in them. Instead, Plaintiff alleged only the current product names, which were different than the names when Plaintiff allegedly disclosed its trade secrets to the consulting company.

***Cortz, Inc. v. Doheny Enterprises, Inc.*, 2017 WL 2958071 (N.D. Ill. 2017)**. Plaintiff fired one of its employees after he refused to sign a non-compete agreement. The employee then joined a competing company that had considered acquiring Plaintiff. Plaintiff then sued its former employee and the competing company for, among other claims, misappropriation of trade secrets in violation of the DTSA and ITSA. Plaintiff moved for a preliminary injunction, and after a two-day evidentiary hearing, the court denied the motion. Initially, Plaintiff failed to demonstrate that its vendor pricing was a trade secret because it put in no evidence as to the time and effort in creating it or the difficulty in duplicating it. The court also rejected Plaintiff's actual misappropriation contention in light of conflicting testimony over whether a key telephone call occurred and the court's crediting of Defendant's witness's innocent explanation of its vendor price reductions. The court further noted that the individual Defendant only had a few of Plaintiff's vendor pricing records on his personal computer, and that those older records were likely irrelevant to current vendor prices. The court similarly rejected Plaintiff's inevitable disclosure contention. The court evaluated inevitable disclosure under both the DTSA and ITSA claims with the same analysis, concluding that the individual Defendant was not at risk of inevitably disclosing vendor pricing because he neither negotiated nor discussed vendor pricing at his new job.

***Matrix Basement Sys., Inc. v. Drake,* 2017 IL App (1st) 151831-U, ¶ 1, *appeal denied,* 89 N.E.3d 756 (Ill. 2017)**. Plaintiff corporation filed a complaint alleging that the defendant, plaintiff's former contractor, gave the plaintiff's trade secrets to a competitor, also a defendant, in violation of the Illinois Trade Secrets Act ("the ITSA"), among other claims. The plaintiff later filed an amended complaint, dropping the ITSA claim but continuing to assert that the alleged trade secret misappropriation violated the former contractor's contractual obligations to Plaintiff. After the defendant's counsel showed that the plaintiff's misappropriation claims were unfounded, the plaintiff filed a motion to voluntarily dismiss the amended complaint without prejudice. In response, the former contractor sought sanctions on multiple grounds, including under Section 5(i) of ITSA, which authorizes a discretionary award of reasonable attorney's fees to the prevailing party if a claim for misappropriation is made in bad faith. The trial court denied sanctions, and the appellate court affirmed. As to Section 5(i) of ITSA, the appellate court rejected the defendant's contention that it was the "prevailing party" in light of the plaintiff's voluntary dismissal. In the absence of controlling Illinois authority construing ITSA, the appellate court looked to Illinois cases construing analogous statutory provisions and ruled that, to be a prevailing party, a litigant must either receive a judgment on the merits or a judicially-enforceable settlement agreement. In addition, the appellate court noted that there was no finding or evidence of bad faith within the meaning of Section 5(i), since the plaintiff had reason to believe the defendant had stolen trade secrets when it filed its original complaint.

***Maxtech Consumer Prod., Ltd. v. Robert Bosch Tool Corp.*, 255 F. Supp. 3d 833 (N.D. Ill. 2017)**. Two power tool companies, Maxtech and Bosch, signed a non-disclosure agreement to explore a potential business arrangement involving three products. The discussions were unsuccessful, and Maxtech filed suit against Bosch alleging, among other things, claims under ITSA that Bosch misappropriated Maxtech trade secrets in each of the three products. Bosch moved for summary judgment on all trade secrets claims. The court granted Bosch summary judgment on its misappropriation claim as to the first product. First, the court concluded that Maxtech's claim was barred by ITSA's five-year statute of limitations, under which a misappropriation claim accrues when a plaintiff has actual or constructive notice of the alleged misappropriation. In this case, the court found that a Bosch patent application published six years before Maxtech's suit put Maxtech on constructive notice of the misappropriation. While filing a patent application does not always create constructive notice, the court found that, since Maxtech was pursuing a similar invention and knew Bosch was a competitor in this area, it was reasonable to conclude that Maxtech was monitoring Bosch's patent filings. The court also rejected Maxtech's contention that the statute of limitations should be equitably tolled due to fraudulent concealment because Maxtech's complaint did not allege fraudulent concealment at the outset. Second, the court found no misappropriation because Maxtech defined its trade secret as the "idea" of the product, rather than the physical "making" of it, and Bosch had shown that it independent thought of the same invention before Maxtech disclosed this trade secret to it.

The court also granted Bosch's summary judgment as to second product, finding that Maxtech did not identify its trade secret with sufficient particularity. Maxtech claimed trade secrets in thirteen elements, but conceded that none alone was a trade secret and failed to identify which specific combinations were a trade secret. There court also noted that there were significant differences in the two companies' products with respect to the technology at issue. But the court denied Bosch's summary judgment motion as to trade secrets in the third product because Plaintiff pointed to specific overlap in technology and identified in interrogatory answers how this technology was disclosed to Bosch. The court also found there was sufficient evidence from which a jury could infer that Maxtech's claimed trade secrets were at least the jumping off point for Bosch's technology, even if Bosch did not use all aspects of Maxtech's technology.

***Mickey's Linen v. Fischer*, 2017 WL 3970593 (N.D. Ill. 2017)**. Plaintiff sued its former employee for misappropriation of trade secrets under the DTSA and the ITSA, and for violation of his non-compete agreement. Plaintiff alleged that Defendant divulged Plaintiff's confidential information to his new employer, a direct competitor of Plaintiff's in the linen service business. Plaintiff moved for a preliminary injunction. After an evidentiary hearing, the court issued a preliminary injunction based, in part, on the DTSA and ITSA claims. The court found that customer identities were a trade secret even though a customer's linen provider might be knowable from markings on the linen, that customer information such as pricing terms were trade secrets even though the customers were free to divulge them, and that financial information of Plaintiff's easily qualified as a trade secret. Regarding proof of misappropriation, the court relied on circumstantial evidence such as Defendant's wiping of his company-issued phone before returning it and unreliable testimony from Defendant about why he returned to the Plaintiff far fewer documents than he had removed. Apart from circumstantial evidence, the court also found that evidence showed threatened misappropriation through inevitable disclosure. After weighing the credibility of the testimony of each side's witnesses regarding the comparability of Defendant's positions at Plaintiff and his new employer and the new employer's preventive measures, the court concluded that Defendant would inevitably disclose Plaintiff's trade secrets, especially given Defendant's "history of deceit." The court used the same inevitable disclosure analysis to find "threatened misappropriation" under both the ITSA and the DTSA. The court also found the non-compete agreement to be enforceable.

***Miller UK Ltd. v. Caterpillar Inc.*, 2017 WL 1196963 (N.D. Ill. 2017)**. Defendant, a manufacturer of earthmoving equipment, terminated a supply agreement with the plaintiff corporation for a coupler attachment that Defendant would sell under its own name. After Defendant began selling a coupler of its own that was similar to Plaintiff's, Plaintiff sued, alleging, among other claims, misappropriation of trade secrets in violation of ITSA and breach of the supply agreement's confidentiality provision. Following an eight week trial, a jury awarded Plaintiff compensatory damages of $24.9 million and exemplary damages of $49.7 million on the misappropriation claim, and $16 million on the breach of contract claim.

In denying Defendant's post-trial motion for judgment as a matter of law, the trial court rejected arguments that Plaintiff's models of the coupler needed to be specifically marked as confidential to qualify as "trade secrets" under the ITSA or be covered under the agreement. Testimony indicated that the parties had discussed and agreed to the confidentiality of information shared under the agreement, and this was enforceable under Illinois law notwithstanding a prior written contract setting forth the specific information that would be deemed confidential. The trial court also held that a combination of elements could be protected as confidential, even if some were public, and rejected Defendant's contention that the jury should have been instructed that published or readily ascertained information does not qualify as a trade secret. Further, the court held that there was sufficient evidence that Plaintiff had taken reasonable steps to protect the confidentiality of the information, such as the use of confidentiality agreements. The trial court also denied Defendant's motions directed at the damages awards, holding that the evidence—including an internal email saying that Defendant wanted its coupler to look "identical" to Plaintiff's—supported a finding that defendant knowingly used Plaintiff's confidential information, and exemplary damages were therefore properly awarded under the ITSA. The court also upheld the amount of the exemplary damages, holding that in light of the statutory exemplary damages cap of two times compensatory damages, an award at the amount of the cap was not per se excessive. Finally, the trial court rejected Defendant's contention that the ITSA should not be applied extraterritorially to award damages to a non-Illinois plaintiff based on conduct by Defendant's employees that largely occurred outside of Illinois.

***Molon Motor & Coil Corp. v. Nidec Motor Corp.*, 2017 WL 1954531 (N.D. Ill. 2017)**. Plaintiff, a manufacturer of electric motors, filed suit against a competitor that had hired one of plaintiff's high-ranking employees, who had allegedly copied plaintiff's confidential information (including engineering data, quality control testing data, and customer communications) onto a thumb drive and taken the data to Defendant. Defendant moved to dismiss Plaintiff's ITSA and DTSA claims, arguing that Plaintiff had failed to allege adequately "misappropriation" because the downloading occurred while the former employee was still employed by Plaintiff and there was no plausible way that Defendant had used the trade secrets.

The court denied the motion to dismiss. As a threshold matter, the court found that Plaintiff had adequately described the alleged trade secrets in the copied data, observing that Defendant could obtain additional specificity as the case progressed through interrogatories. Regarding "misappropriation," the court first held that the federal and Illinois claims could be discussed together as the pertinent definitions of the two acts are similar. The court then held that, at the pleading stage, the allegations were sufficient to satisfy the statutes' definitions of acquiring trade secrets by "improper means." In this regard, the court found that Plaintiff's employment agreement with the defecting employee put the employee on notice that he could not use Plaintiff's confidential information for any purpose other than his employment, and that retrieving this information for his own use fell outside of the normal course of his employment. Plaintiff also had sufficiently alleged that it had policies and procedures protecting its trade secrets, which its employee had circumvented to download the confidential information at issue.

As to the allegations that Defendant acquired the trade secrets from the defecting employee or used the trade secrets, the court held that the inevitable disclosure doctrine applied for both the ITSA and DTSA claims. At the pleading stage, Plaintiff had alleged facts sufficient to support an inference that Plaintiff and Defendant were direct competitors, and that the employee's responsibilities with Defendant were similar to his responsibilities with Plaintiff. The court further held that the risk of inevitable disclosure remained as of the effective date of the DTSA, even if the employee had obtained the information in question and switched employers prior to the effective date of the DTSA. The court also noted, however, that Plaintiff will bear the burden of ultimately proving, not just alleging, enough facts such that disclosure is not premised on a mere unsubstantiated fear. Injunctive relief was not at issue, and the decision did not address the DTSA's language regarding injunctions that prohibits an injunction impacting employment that is based merely on information the person knows. *See* 18 U.S.C. § 1836(b)(3)(A)(i)(I).

***Kuryakyn Holdings, LLC v. Ciro, LLC*, 242 F. Supp. 3d 789 (W.D. Wis. 2017)**. Plaintiff, a designer of aftermarket motorcycle parts, filed suit against a competing business and its founders (former officers of Plaintiff), as well as several individual employees allegedly poached from Plaintiff by the competing business. Plaintiff alleged, among other claims, misappropriation of trade secrets in violation of the Wisconsin Uniform Trade Secrets and DTSA. Applying the same analysis to the state and federal claims, the court granted Defendants summary judgment because Plaintiff had failed to sufficiently define its trade secrets to survive summary judgment, instead giving vague descriptions, such as "information about the manufacturing skill, reliability, resources, capacity, technical knowledge, costs of manufacture, component costs, and expertise specific to the development and production of motorcycle parts and accessories." The court further held that, to the extent Plaintiff had provided any level of specificity, Plaintiff failed to establish that such information could not be legitimately learned via other means (such as simply asking a third-party supplier), or reverse-engineered from the product in question.

<u>8th Circuit</u>

***Aggreko, LLC v. Barreto*, 2017 U.S. Dist. LEXIS 35573 (D.N.D. 2017)**. The court denied the defendant's motion to dismiss claims for misappropriation of trade secrets (under the DTSA and North Dakota UTSA), breach of contract, and conversion because plaintiff's pleadings were adequate and supported by sufficient evidence that defendant had access to a substantial amount of plaintiff's confidential and proprietary information and trade secrets relating to operations, customers, business proposals, pricing strategy, client preferences, and proprietary pricing models.

***Deluxe Fin. Servs., LLC v. Shaw*, 2017 U.S. Dist. LEXIS 122795 (D. Minn. 2017).** The court denied the defendant executive employee's motion to dismiss trade secret misappropriation claims (under the DTSA and Ohio UTSA) because the plaintiff check printing company sufficiently pleaded that it undertook efforts to maintain secrecy of the alleged trade secrets, that the information would have significant value to its competitors, and defendant had access to confidential sales information including detailed customer pricing and data, sales analysis, and strategies.

***Express Scripts, Inc. v. Lavin*, 2017 U.S. Dist. LEXIS 105006 (E.D. Mo. 2017)**. The court granted the plaintiff pharmacy services corporation's motion for a temporary restraining order to: (1) prevent its former national sales director from joining competing company and from disclosing confidential information to a competing company; and (2) prevent a competing company from employing plaintiff's former sales director or using any of the plaintiff's confidential information. The court found that the information possessed by the former sales director constituted trade secrets as defined by both the DTSA and the Missouri UTSA. The court further applied the inevitable disclosure in finding that the plaintiff suffered and would continue to suffer irreparable harm if not granted injunctive relief.

***Flowshare, LLC v. TNS, US, LLC*, 2017 US. Dist. LEXIS 116778 (E.D. Mo. 2017)**. Plaintiff Flowshare, LLC, doing business as ShareTracker, is a telecom research company and defendant TNS was one of its distributors. ShareTracker alleged that it had entered into an oral license agreement allowing TNS to sell or grant limited, nonexclusive, nontransferable sublicenses for a fee to use ShareTracker products to three authorized customers or sublicensees. In exchange, ShareTracker provided updated or refreshed databases and data fields to TNS to support licensed ShareTracker products. ShareTracker alleged that in 2015, it acquired GeoResults, Inc., another telecom research company, primarily due to its relationship with a key customer, one of the largest telecom companies in the U.S. market. Shortly after the acquisition, the customer ended its decades-long business relationship with GeoResults. ShareTracker alleged that TNS encouraged the customer to end its relationship with GeoResults and deal directly or indirectly with TNS. ShareTracker also alleged that TNS misappropriated and converted some or all of ShareTracker's confidential information without authorization. ShareTracker claimed TNS improperly used its license to ShareTracker's database products by distributing, directly or indirectly, those products to the customer without ShareTracker's authorization and obtaining payment directly from the Customer. The court characterized the plaintiff's claim as broad and general, but viable enough to survive a motion to dismiss under both the DTSA and Missouri UTSA because the plaintiff maintained proprietary, network-based technology that used the largest sample sizes in the industry and is highly accurate, and because its products were the result of a significant expenditure of time, effort, and expense.

***Mid-Am. Bus. Sys. v. Sanderson*, 2017 U.S. Dist. LEXIS 166463 (D. Minn. 2017)**. The court denied the plaintiff storage company's motion for a temporary restraining order against its former service technician and his new employer to prevent both from misappropriating the plaintiff's trade secrets under the DTSA and Minnesota UTSA. The court held that the storage company failed to sufficiently demonstrate that the misappropriation of what it alleged were trade secrets occurred or was likely to occur.

***Porters Bldg. Ctrs., Inc. v. Sprint Lumber*, 2017 U.S. Dist. LEXIS 162139 (W.D. Mo. 2017)**. The court denied in part and granted in part the defendant's motion for summary judgment as to the misappropriation of trade secrets (under the Missouri UTSA) by applying a factors test to determine whether information was a trade secret; denying as to top customer data compilations, financial data, market share, inventory turnover, materials lists, and internal operating procedures, and granting as to compensation information because plaintiff failed to establish that compensation information was not readily ascertainable by proper means.

***Search Partners, Inc. v. MyAlerts, Inc.*, 2017 U.S. Dist. LEXIS 102577 (D. Minn. 2017)**. The court dismissed the plaintiff's DTSA claim with prejudice for failure to state a claim on the ground that the DTSA does not apply to acts occurring before its effective date of May 11, 2016.

***Sharp Med. Solutions, LLC v. Stobbe*, 2017 U.S. Dist. LEXIS 113918 (D. Neb. 2017)**. The court granted the plaintiff medical supply company's motion for a TRO enjoining the defendant former employees from violating their employment agreements and from using plaintiff's proprietary information because defendants were subject to non-compete agreements, took confidential and trade secret documents belonging to former employer prior to termination, and used that information in an effort to establish a competing business.

***Sys. Spray-Cooled, Inc. v. FCH Tech, LLC*, 2017 U.S. Dist. LEXIS 73909 (W.D. Ark. 2017)**. Prior to the formation of Defendant FCH Tech, Plaintiff Systems was the only provider of low pressure, spray cooling equipment in the steel industry. William Henry and J. Michael Campbell, former Systems employees, formed FCH with the intent to directly compete with Systems. Henry and Campbell signed agreements with Systems prohibiting the taking, disclosure, or use of Systems's trade secrets and confidential information. Systems alleged that Henry and Campbell breached the agreements by taking and possessing Systems's trade secrets and confidential information in violation of the DTSA, and also asserted claims for breach of employment agreement, breach of fiduciary duty, and tortious interference. Systems sought to enjoin the defendants from further misappropriation, disclosure, and use of Systems's trade secrets and confidential information until a final determination on the merits of the pending litigation had been made. In addition, Systems sought to enjoin defendants from directly or indirectly designing or supplying low pressure spray-cooling equipment for the steel industry for a three-year period. In analyzing Systems's likelihood of success on the merits, the court examined whether its design drawings, pricing information, customer lists, revenue forecasts and financial statements qualified as trade secrets. The court concluded that Systems offered sufficient evidence that its design drawings and pricing information qualified as trade secrets, but was unpersuaded with respect to Systems's customer lists, revenue forecasts and financial statements. Further, the court held the defendants' misappropriation of Systems's trade secrets could not be measured in money damages and, thus, created a presumption of irreparable harm. The court also found that Systems suffered irreparable harm due to the possible loss of its largest, most important customer. The court further found that the public interest in preserving fair competition and protecting trade secrets weighed in favor of granting injunctive relief. Thus, after analyzing Systems's success on the merits, the threat of irreparable harm, and the public interest, the court granted Systems's preliminary injunction.

9th Circuit

***United States v. Liew*, 856 F.3d 585 (9th Cir. 2017)**. Defendant and his company were convicted under the (pre-DTSA) Economic Espionage Act ("EEA") for conspiracy and attempt to commit economic espionage and theft of trade secrets, possession of misappropriated trade secrets, and conveying trade secrets, among other crimes. The trade secret at issue concerned methods of producing titanium dioxide ("TiO2"). DuPont had been a leader in TiO2 production since the 1940s, when it became more efficient to produce TiO2 through a chloride-based process. DuPont opened chloride plants around the US, including one in Antioch, California and one in Ashtabula, Ohio. The Ashtabula plant was built for Sherwin-Williams, subject to a fifteen-year confidentiality agreement effective through the plant's sale in the 1970s. The plant was sold multiple times thereafter and was ultimately acquired by a competitor of DuPont who was not bound by any nondisclosure or confidentiality obligations to the company. DuPont improved its TiO2 manufacturing process and began incorporating the newer technology into new plants, including a facility in Taiwan. Unlike the Antioch and Ashtabula plants, the new Kuan Yin plant was equipped to extract titanium from lower-grade ore, making DuPont's the most competitive chloride process. The Chinese government sought to license DuPont's TiO2 technology but ultimately chose a more cost-effective molten-salt option from the former Soviet Union. The Chinese government then tasked Walter Liew, a businessman and US citizen, with bringing chloride TiO2 production to China. Liew hired two former DuPont employees with TiO2 experience and with their help, went about securing business, which eventually brought them to their various convictions under the EEA. Liew and the other defendants appealed their convictions to the Ninth Circuit.

One of the defendants' many arguments on appeal was that the technology at issue was not trade secret material because DuPont sold the Ashtabula plant and, thus, did not take reasonable measures to guard its technology. The Court rejected defendants' arguments and held that it was not plain error for the district court not to instruct the jury that disclosure "'to even a single recipient who is not legally bound to maintain [a trade secret's] secrecy' destroys trade secret protection." The Ninth Circuit explained that there was no clear or controlling authority addressing whether disclosure to one competitor makes information "generally known" or "readily ascertainable" by "the public" under the EEA's then-definition of trade secrets. The Court further stated that the government was not required to prove no disclosures of DuPont's technology occurred; only that DuPont took reasonable measures to guard its technology. The Court found DuPont's selectiveness in employing contractors and use of confidentiality agreements to be reasonable measures. The sale of a plant or information in a recipient or competitor's hands is not the end of the reasonable measures inquiry, particularly if the information disclosed is not part of the trade secret(s) at issue. As a result, the Ninth Circuit upheld criminal convictions under the (pre-DTSA) Economic Espionage Act for trade secret misappropriation despite a third-party competitor (who was not bound by any confidentiality obligations) acquiring the trade secret.

AccentCare Home Health of Rogue Valley, LLC v. Bliss**, 2017 U.S. Dist. LEXIS 88125 (D. Or. 2017)**. The court held that a plaintiff in a claim of trade secret misappropriation may maintain both a state court action against in-state defendants and a federal court diversity action against out-of-state defendants. The court reasoned that in an action for trade secret misappropriation under Oregon law, the acquirer of the trade secrets may be sued separately from the person who disclosed the trade secrets if the person who acquired the information knew or should have known that the trade secrets were improperly acquired.

AllCells, LLC v. Zhai, **2017 U.S. Dist. LEXIS 47062 (N.D. Cal. 2017)**. Biotechnology Company AllCells alleged that prior to their departures, two former employees misappropriated the plaintiff's trade secrets by copying to external storage devices data related to AllCells's standard operating procedures, internal operations, customer identities, needs and preferences, key contacts, pricing, and sales forecasts and projections. Issuing a preliminary injunction prohibiting any use or disclosure of the alleged trade secrets, the court noted that while the record was not sufficiently developed to show otherwise at that point in the litigation, AllCells's allegations of trade secret misappropriation "raised serious questions" going to the merits of the case. The court then held that injunctive relief should issue on the basis that the potential for the defendants to cause harm to the plaintiff through use or disclosure of the alleged trade secrets during the pendency of the action outweighed any harm that the defendants would suffer through issuance of the injunction, especially in light of the defendants' representations to the court that the alleged trade secrets were of little to no value to the defendants.

Avago Techs. United States Inc. v. NanoPrecision Prods., **2017 U.S. Dist. LEXIS 13484 (N.D. Cal. 2017)**. The court dismissed a claim of conversion based on UTSA preemption because the only basis for the property right at issue in this claim was trade secret law. The court further dismissed the counterclaimant's claim of misappropriation of trade secrets under the DTSA on the grounds that the DTSA does not allow for a misappropriation claim to be asserted based on the continued use of information that was improperly disclosed prior to the effective date of the statute. However, the court granted leave to amend to include allegations of misappropriation after the effective date of DTSA.

Contemporary Servs. Corp. v. Landmark Event Staffing Servs., Inc., **677 F. App'x 314 (9th Cir. 2017)*****, as amended on denial of reh'g*** **(Mar. 30, 2017)**. The court reversed an order granting summary judgment on a claim of misappropriation of trade secrets (under the California UTSA) because the plaintiff raised triable issues of fact related to: (1) whether its customer lists, deployment workbook, and a document containing financial information qualified as trade secrets and (2) whether the defendant had unlawfully ratified its employee's misappropriation of this data by failing to ease the use or otherwise disavow the employee's conduct after it learned of the misappropriation.

***Gatan, Inc. v. Nion Co.*, 2017 U.S. Dist. LEXIS 49751 (N.D. Cal. 2017)**. The court denied a motion to dismiss a claim of trade secret misappropriation (under the California UTSA) because (1) the plaintiff manufacturer of electron microscope components satisfied the requirement to identify its trade secrets with reasonable particularity by identifying its trade secrets as the recipes by which it constructed magnetic optics, the shape of its electron trajectories, the number and location of various electron-optical crossovers, and the exact way it corrected the many electron optical aberrations; (2) the identified trade secrets derived economic value from not being generally known since the defendant, who worked with plaintiff on a collaborative project, used its trade secret information to bypass years of costly research, win a million dollar grant, and compete in the market; (3) the plaintiff took reasonable efforts to maintain the secrecy of its trade secrets by requiring defendant to sign a nondisclosure agreement; and (4) there was evidence of misappropriation because defendant allegedly disclosed plaintiff's trade secrets to the government and used it to develop its own spectrometer product.

***GTAT Corp. v. Fero*, 2017 U.S. Dist. LEXIS 80511 (D. Mont. 2017)**. GTAT, a technology company operating heavily in the solar industry, invested significant research and development to create a proprietary process for producing polysilicon. After its former engineer and director, Fero, left GTAT, began operating a competing polysilicon technology business, and offered to sell essentially the same technology at a lower price to a Chinese company that had engaged in extensive negotiations with GTAT, GTAT asserted claims for the misappropriation of trade secrets under the DTSA and Montana UTSA. Denying GTAT's application for preliminary injunction, the court first held that GTAT could not demonstrate a likelihood of success on the merits because it had not established that its polysilicon process arose to the level of a trade secret since, per GTAT's admission, much of the polysilicon process was generally known. The court also noted the lack of evidence of misappropriation of the alleged trade secrets. While GTAT had proffered evidence that Fero failed to return his work laptop after his resignation and established a DropBox account and deleted it shortly after he left, GTAT failed to demonstrate what, if any, GTAT information was taken by either means. While GTAT also argued that Fero's offer to the Chinese company inherently demonstrated the misappropriation of trade secrets since Fero offered essentially the same technology at a lower price, the court rejected this argument and credited Fero's evidence indicating that he used the knowledge he gained from nearly 20 years in the industry to prepare the offer at issue. Finally, the court noted that GTAT's failure to enforce the physical and electronic security measures that, per GTAT, constituted the reasonable measures it took to protect its trade secrets may also impact GTAT's likelihood of proving that the information at issue arises to the level of a trade secret, although the court did not reach a conclusion on this point since it held that GTAT failed to demonstrate a likelihood of success on the merits in other respects.

***IA Technologies, Inc. v. ASUS Computer International*, 2017 WL 491172 (N.D. Cal. 2017)**. The court allowed the plaintiff to amend its complaint to add a DTSA claim after discovery revealed alleged continued misappropriation.

***KCG Ams. LLC v. Zhengquan Zhang*, 2017 U.S. Dist. LEXIS 54746 (N.D. Cal. 2017)**. The court held that a securities trading company's allegations against its former employee that he "wiped" his work computer and could disclose information and may destroy evidence were entirely speculative and not supported by evidence. Accordingly, the court found there was no demonstration of likely irreparable harm and denied the plaintiff's application for a temporary restraining order brought for alleged violations of the DTSA.

***Mfg. Automation & Software Sys. v. Hughes*, 2017 U.S. Dist. LEXIS 72203 (C.D. Cal 2017)**. The court found that the plaintiff's allegations under the California UTSA that its trade secrets were comprised of "the procedures, processes, systems, methods of operation for [its] software products, costumer identifications, private phone numbers and email addresses, individual customer product needs and specifications, market studies, special business practices and private bank account information" identified the alleged trade secrets with sufficient particularity so as to overcome motion to dismiss and permit discovery to commence.

***Octaform Sys. v. Johnston*, 2017 LEXIS 90330 (D. Nev. 2017)**. The court granted a motion to dismiss claims of conversion, tortious interference, unjust enrichment, and civil conspiracy due to preemption under the Nevada UTSA. However, the court rejected defendants' argument that the case should be dismissed under Fed.R.Civ.P. 19 due to failure to name a necessary party, noting that entities are not necessary parties merely because they are joint tortfeasors.

***Oakiwear Outdoor, LLC v. Timbee, LLC*, 2017 U.S. Dist. LEXIS 137023 (W.D. Wash. 2017)**. In an action for misappropriation of trade secrets under the DTSA and Washington UTSA, the parties stipulated to a preliminary injunction precluding the defendants from contacting Oakiwear's existing or prospective customers and from using a particular Chinese manufacturing company to produce the defendants' goods. Oakiwear later moved to amend the injunction to add two retailers, Zulily and Kid to Kid, and two additional Chinese manufacturers to the list of companies not to be contacted or utilized by the defendants. According to Oakiwear, Timbee's contacting the retailers and manufacturers at issue constituted a misappropriation of trade secrets. The court denied Oakiwear's motion on the grounds that (1) the existence of large retailers and ordinarily known manufacturers is not a trade secret and (2) the balance of harms tipped in favor of the defendants, who would be put out of business by the proposed amendment (whereas Oakiwear could be made whole with a damages award).

***Peo Experts CA, Inc. v. Engstrom,* 2017 U.S. Dist. LEXIS (E.D. Cal. 2017)**. Plaintiff (dba Bixby) sought a preliminary injunction against its former sales manager and two former sales agents based on alleged misappropriation of trade secrets (under the DTSA and California UTSA) consisting of customer identities and contact information, customer pricing information, prior purchase history, specifications, and habits, and other forms of customer goodwill. Granting an injunction against the sales manager, the court first held that the information at issue was a trade secret in part because Bixby devoted considerable time and resources developing the information. While Bixby failed to require its employees to sign nondisclosure agreements, the court found that its other security measures, such as encrypting confidential information, password protecting its Google drive, and providing confidential information to employees only on an as-needed basis, were sufficient to satisfy the California UTSA's requirement that the alleged trade secrets be subject to reasonable measures to safeguard the information. The court further held that the sales manager's acts of proposing specific services to customers based on his memory of the services he had developed at Bixby constituted improper use arising to the level of misappropriation of trade secrets even if the sales manager did not access Bixby files containing this information. The court declined, however, to issue a preliminary injunction against the sales agents, noting that the fact that Bixby had repeatedly told these agents that they were responsible for expanding their own books of business and would receive residual commissions if they continued to manage the accounts after their departures, combined with the fact that these agents invested personal funds to develop these client relationship, gave the agents a proprietary interest in the customer data at issue, thereby undercutting any claim that their use of this information was improper.

***OOO Brunswick Rail Mgmt. V. Sultanov*, 2017 U.S. Dist. LEXIS 2343 (N.D. Cal. 2017)**. The court found that the plaintiff satisfied the requirements for a TRO brought for alleged violations of the DTSA and California UTSA because (1) the evidence showed the former employees disseminated protectable trade secrets by emailing documents to their personal accounts and then sending the information to third parties, (2) the plaintiff would suffer irreparable harm if such information was disseminated to its creditors, competitors, and adverse parties in arbitration, and (3) a TRO would serve the public interest.

***Physician's Surrogacy, Inc. v. German*, 2017 U.S. Dist. LEXIS 135325 (S.D. Cal. 2017)**. The court dismissed a claim under the DTSA because the alleged improper acquisition of the trade secrets occurred prior to the effective date of the UTSA, and because the complaint failed to adequately allege other trade secret misappropriation, such as improper use of the trade secrets.

***Prot. Techs., Inc. v. Ribler*, 2017 U.S. Dist. LEXIS 33200 (D. Nev. 2017)**. The court found that a customer list containing information concerning customers' product preferences, buying patterns, credit profiles, customer invoices and pricing, customer practices, margins and profit variances, and transaction details arose to the level of a trade secret under the DTSA and Nevada UTSA. The court further held that the act of downloading company data immediately after termination, coupled with attempts to hide these acts, indicates an intent to use this data against the company's interests.

***Sec. Alarm Fin. Enters., L.P. v. Alder Holdings, LLC*, 2017 U.S. Dist. LEXIS 17536 (D. Alaska 2017)**. The court denied a motion for summary judgment as to a home security company's claim that theft of a customer list constituted misappropriation of trade secrets under the Alaska UTSA. The court noted that while the security company's customers could arguably be ascertained by observing yard signs identifying locations where the company provided services, there was a triable issue of fact as to whether the customer list constituted a protectable trade secrets since the customer list contained non-public information pertaining to the equipment being used, contract terms, and customer contact information.

***Select Timber Prods. LLC v. Resch*, 2017 U.S. Dist. LEXIS 137860 (D. Or. 2017)**. The plaintiffs claimed that the defendants violated the DTSA and Oregon UTSA by misappropriating the plaintiffs' proprietary process for producing specialized wood products as well as other trade secrets including pricing information, customer lists, and information about customer and employee relationships. The court denied the defendants' motion to dismiss the trade secret misappropriation claims. The court found evidence that the president of a company paid a competitor's former employee to replicate technology that gave the competitor an advantage in the marketplace, and then paid another of the competitor's former employees to train the company's employees as to use the competitor's machine and duplicate the competitor's confidential processes. The court deemed this evidence sufficient to satisfy the requirement that the plaintiff allege that the trade secret was acquired with knowledge of the theft or improper use.

***Sleekez, LLC v. Horton*, 2017 U.S. Dist. LEXIS 71410 (D. Mont. 2017)**. After Horton's employment with Sleekez, a custom horse grooming tool manufacturer, was terminated, Horton began selling knockoffs of Sleekez's products. Sleekez filed a motion to amend its complaint to assert a cause of action for misappropriation of trade secrets under the DTSA. Sleekez alleged Horton misappropriated its confidential and proprietary information, including the components of its tools, identified manufacturers, marketing information and strategies, and business strategies. Opposing Sleekez's motion, Horton argued that the amendment would be futile because there were insufficient allegations to show that Sleekez took reasonable efforts to maintain the secrecy of the alleged trade secrets. The court disagreed and permitted the amendment, noting that Sleekez's allegations that it did not publicly disclose the trade secrets, only disclosed select portions of the data (and customer account information) to employees on a need-to-know basis, instructed employees to maintain the information as confidential, and password-protected its business accounts were sufficient. The court further rejected Horton's argument that Sleekez had failed to assert that Horton owed a duty to maintain the secrecy of the information at issue, since Sleekez's proposed amended complaint alleged that Horton knew of his obligation to maintain in confidence the business methods, strategies and other confidential information to which he had access in connection with his longstanding employment with Sleekez.

***SolarCity Corp. v. SunPower Corp*., U.S. Dist. 2017 LEXIS 68639 (N.D. Cal. 2017)**. The court dismissed a claim for declaratory relief as being duplicative of causes of action, including cause of action for violation of the DTSA.

***Space Data Corp. v. X*, 2017 U.S. Dist. LEXIS (N.D. Cal 2017)**. The court granted a motion to dismiss on the basis that conclusory allegations that use of trade secret information exceeded what was permitted under a nondisclosure agreement, without specifying how the alleged conduct exceeded permissible use, were insufficient to allege misappropriation of trade secrets (under the DTSA and California UTSA).

***Synthes, Inc. v. Knapp*, 250 F. Supp. 3d 644 (E.D. Cal. 2017)**. Applying Pennsylvania law, the court granted a motion to dismiss due to the lack of sufficient evidence demonstrating that knowledge obtained by a former spine implant salesman regarding various doctors' personal preferences constituted trade secrets that were distinguishable from “subjective knowledge obtained in the course of employment”, which, under Pennsylvania law, does not qualify as a trade secret.

***UCAR Tech. (USA) Inc. v. Yan Li*, 2017 U.S. Dist. LEXIS 59965 (N.D. Cal. 2017)**. UCAR, one of the largest ride sharing providers in China, sought a preliminary injunction against four former employees based on alleged misappropriation of trade secrets under the DTSA. On application for preliminary injunction, UCAR asserted that the defendants reformatted their company issued laptops, effectively deleting data and information previously stored thereon, and accessed, downloaded and retained UCAR’s trade secrets on personal devices. UCAR further argued that (1) defendants’ act of destroying company property demonstrated a risk of evidence destruction and (2) defendants’ act of downloading UCAR trade secrets to personal devices demonstrated that defendants planned to disclose UCAR confidential information a competing company, thereby destroying UCAR’s competitive edge. Denying the motion for preliminary injunction, the court noted that UCAR had failed to demonstrate that the reformatting of company computers caused irreparable harm, since there was no evidence that actual loss of data resulted from these actions. The court further held that notwithstanding the evidence that (1) one defendant downloaded UCAR files from the UCAR server after his employment with UCAR ended and (2) the other defendants also retained UCAR data after resigning their employment with UCAR to join a competitor, the defendants’ declarations stating under oath that they did not intend to use UCAR’s data were sufficient to defeat the plaintiff’s argument that the defendants’ theft of the data demonstrated an immediate threat of use or disclosure.

***Veronica Foods Co. v. Ecklin*, 2017 U.S. Dist. LEXIS 101325 (N.D. Cal. 2017)**. Between 2004 and 2015, Ecklin worked in a sales capacity for Veronica Foods (VF), an importer of specialty food products. During his employment, Ecklin had regular contact with VF’s customers and acquired detailed knowledge of VF’s customer list, supplier list, the name and contact information for the person at each VF customer store responsible for purchasing, the ordering history of each customer store, information relating to particular needs and preferences of each customer, billing and payment information, product information, and cost and pricing information, including profit margins. After he resigned, Ecklin began working for MillPress. VF later asserted claims of misappropriation of trade secrets (under the DTSA and California UTSA) against Ecklin and MillPress, alleging that the defendants solicited business from VF’s customers through the use of VF’s trade secrets. Dismissing VF’s complaint without prejudice, the court first held that while certain aspects of the customer list may constitute trade secrets, VF’s full customer list did not constitute a trade secret because VF publicly disclosed that it maintained relationships with specific customers identified in the customer list at issue. The court further held that VF had failed to sufficiently allege that the defendants had misappropriated the alleged trade secrets at issue. While VF alleged that Ecklin possessed specialized knowledge of the particular stores to which VF sold its products, VF failed to allege that Ecklin acquired this knowledge by working with those particular stores (as opposed to observing public information that would demonstrate that VF, a dominant retailer in the industry, had products placed in those stores). The court further noted that VF’s conclusory allegations that the defendants made “improper and unauthorized use of the alleged trade secrets" failed to sufficiently identify what acts by defendants constituted the alleged misappropriation.

Waymo LLC v. Uber Techs., Inc., **2017 U.S. Dist. LEXIS 73843 (N.D. Cal. 2017)**. Waymo sued its former employee (Levandowski) and Uber (Levandowski's employer) alleging claims including misappropriation of trade secrets under the DTSA and California UTSA. Waymo alleged that Levandowski misappropriated more than 14,000 files containing Waymo's trade secret information related to the development of LiDAR systems (a critically important technology in the nascent autonomous vehicle industry). In issuing an injunction prohibiting Levandowski from contributing to Uber's development of LiDAR technology, the court held that while not all of the information taken by Levandowski constituted a trade secret, (1) the court believed that the evidence would likely show that at least some of the information taken by Levandowski constitutes trade secrets (or else, according to the court, Levandowski would not have taken it), (2) Uber hired Levandowski knowing that he possessed files likely to contain Waymo's intellectual property, and (3) at least some of the information in question had "seeped" into Uber's own efforts to develop a LiDAR system. The court also held that since the record indicated that Levandowski remained in possession of Waymo's misappropriated data, Waymo had demonstrated a likelihood of irreparable harm, in that there was a continuing danger of misuse that could not be unwound nor adequately compensated for with monetary damages. The court further explained that the public interest was served by, and the balance of harms weighed in favor of, precluding Levandowski's participation in the development of Uber's LiDAR, since the public interest in protecting trade secrets outweighed Uber's interest in utilizing an engineer who may have misappropriated the proprietary information of a competitor, and since the injunction was not so broad as to prohibit Uber from developing its own LiDAR technology through lawful means. The court declined, however, to enjoin Uber from using any of the alleged Waymo trade secrets at issue based on the court's belief that Waymo had significantly overstated its interests in the disputed information and had included within its alleged trade secrets "[g]eneral approaches dictated by well-known principles of physics" (which would not arise to the level of constituting trade secrets). The court further ordered Uber to use the full extent of its authority over Levandowski to cause the return of the misappropriated information.

Following this order, Uber successfully moved for summary judgment on Waymo's Business and Professions Code Section 17200 claim, on the basis of CUTSA preemption. Later, Uber again moved successfully for summary judgment, seeking to dismiss one of Waymo's trade secret claims on the basis of Waymo's failure to properly identify the trade secret. Uber claimed that Waymo's repeated reframing of the scope of the trade secret in question confirmed that it was not properly identified. Further, Uber argued that Waymo did not assert misappropriation of the specific parameters in the files, but instead focused on a general concept that Waymo argued is reflected in the trade secret files. After the court ordered Uber to assist Waymo in recovering the information Levandowski misappropriated, Uber claimed it urged Levandowski to cooperate and to turn over any evidence. When Levandowski failed to meet an internal deadline to produce materials, Uber terminated him.

United States District Court Judge Alsup previously referred the case to prosecutors to investigate potential criminal behavior, and federal prosecutors on November 22, 2017 sent a sealed letter to the trial court about the investigation. Accusations that Uber concealed evidence included claims that Uber provided employees with computers that were not licensed directly to the company or connected to its server, used vanishing message services, and invoked false attorney-client privilege designations. Finally, Uber was accused of creating a marketplace analytics team for the express purpose of acquiring trade secrets, code base and competitive intelligence.

***Waymo LLC v. Uber Techs., Inc.,* 2017 U.S. Dist. LEXIS 89174 (N.D. Cal. 2017)**. The court granted a motion to dismiss a claim of unfair competition under Business & Professions Code section 17200 due to UTSA preemption. The court noted that Waymo's blanket accusations of misappropriation of "confidential information," in conjunction with its failure to distinguish trade secrets from non-trade secret confidential information in the complaint, supported the conclusion that the claims were "either based upon misappropriation of a trade secret or… based on no legally significant events at all".

***Waymo LLC v. Uber Techs., Inc.,* 2017 U.S. Dist. LEXIS 132721 (N.D. Cal. 2017)**. The court quashed subpoenas that Uber issued to third party competitors seeking to obtain the nonparty competitors' trade secret LiDAR technology. In holding that Uber had failed to demonstrate a substantial need compelling disclosure, the court rejected Uber's arguments that obtaining the competitors' trade secrets would enable it to compare the plaintiff's alleged trade secrets to the nonparty's trade secrets in order to demonstrate that the plaintiff's alleged trade secrets were "not so secret". The court instead held that Uber's subpoenas would allow competitors to institute litigation against one defendant as a means to secure the trade secrets of all of its other competitors);

10th Circuit

***Johns Manville Corp. v. Knauf Insulation, LLC*, 2017 U.S. Dist. LEXIS 155206 (D. Colo. 2017)**. The court held that the statute of limitations on a misappropriation of trade secrets claim under the Colorado UTSA is not triggered by threatened misappropriations of trade secrets. A cause of action does not accrue until the plaintiff knows or should with reasonable diligence know that the defendant has used the plaintiff's trade secrets, even when the plaintiff previously knows that the defendant possessed and likely would use its trade secrets.

11th Circuit

***TransUnion Risk & Alternative Data Sols., Inc. v. Challa,* 676 F. App'x 822 (11th Cir. 2017)**. The Eleventh Circuit Court of Appeals affirmed the denial of the plaintiff employer's preliminary injunction where the defendant employee established that the possibility he would pass on his former employer's proprietary information was remote, thus discounting any presumption of irreparable harm. In particular, the employee stated that he had not and would not use or disclose any of employer's proprietary information while working for competitor, since he had no need for such information in his position at competitor given that his position there was substantially different from is former position with employer, and employer and competitor were both in the data fusion industry, which was rapidly evolving, minimizing the usefulness of proprietary knowledge that was at least 14 months old.

Coll Builders Supply, Inc. v. Velez **2017 U.S. Dist. LEXIS 151257 (M. D. Fla. Aug. 31, 2017)**. The court denied the individual defendant's motion to dismiss the plaintiff's claim for violation of Computer Fraud and Abuse Act where the plaintiff alleged sufficient facts to demonstrate defendant accessed plaintiff's computer system after her termination for the purpose of compromising plaintiff's data.

Digital Assur. Certification, LLC v. Pendolino **2017 U.S. Dist. LEXIS 8807 (Md. Fla. 2017)**. The court held that an employer's customer list was not a trade secret (under the DTSA and Florida UTSA) warranting protection for an order to seal because--despite efforts to protect the list from disclosure by password protecting its computer systems and requiring that employees routinely generate new complex passwords, restricting remote access to servers absent extraordinary circumstances, and requiring employees to sign confidentiality agreements providing for the non-disclosure of customer lists--the employer failed to explain the method by which the list was created or otherwise shown that the information is not readily available from a public source.

HCC Ins. Holdings, Inc. v. Flowers **237 F. Supp. 3d 1341 (N.D. Ga. 2017)**. The court held that more than 500 spreadsheets containing existing and prospective customers (hot sheets) were not protected trade secrets (under the Georgia UTSA) because the employer did not label the files as "confidential," direct employees to maintain the secrecy of the files other than through a general confidentiality agreement, or track the use of the hot sheets, and the former employee's transfer of the hot sheets within the employer's computer system using a computer that she returned upon termination of her employment, while suspicious, did not demonstrate a misappropriation.

Heralds of the Gospel Found. Inc. v. Varela **2017 U.S. Dist. LEXIS 98513 (S.D. Fla. 2017)**. The court held that audiovisuals that were broadcasted on the internet showing private, confidential meetings and discussions among an internal committee of priests regarding their observations and experiences with extraordinary cases of spiritual and possible mental illnesses in furtherance of developing protocols for treating these cases by healing prayers, constituted protected trade secret information under both the DTSA and Florida UTSA, warranting the imposition of an temporary restraining order.

***Pals Grp. v. Quiskeya Trading Corp*. 2017 U.S. Dist. LEXIS 18567 (S.D. Fla. 2017)**. The court denied the plaintiff's motion for preliminary injunction where plaintiff failed to establish that its customer list, which was easily ascertainable, was a trade secret under Florida state law.

Pinch A Penny, Inc. v. SR & JG, Inc. **2017 U.S. Dist. LEXIS 153178 (S.D. Fla. 2017)**. The court entered judgment in favor of the plaintiff and held that the defendants, purchasers of a pool supply business operating as the plaintiff Pinch A Penny, Inc. (PAP) franchise, misappropriated PAP's confidential customer data in violation of Florida state trade secret law, including customer's name, address, telephone number, each customer's pool size, and the number of store visits and purchase history of each customer.

***Sunil Gupta, M.D., LLC v. Franklin* 2017 U.S. Dist. LEXIS 185626 (S.D. Al. Nov. 9, 2017)**. The court denied the dismissal of an employer's claim for violation of Computer Fraud and Abuse Act where the employer had a policy that authorized access to its computerized records only for limited purposes and employees' use of computer for downloading confidential patient data to take to future employer exceeded that purpose.

***TMX Fin. Holdings, Inc. v. Drummond Fin. Servc., LLC*, 300 Ga. 835 (2017).** TMX Finance Holdings, Inc. dba TitleMax and Drummond Financial Services, LLC are competing automobile title loan companies in Georgia. Drummond, and several of its affiliated companies, filed suit against TitleMax, and several of its affiliated companies, alleging that TitleMax was "engaged in a nationwide campaign to systematically and illegally steal [Drummond's] customers." Drummond alleged that TitleMax was compensating Drummond employees to refer customers to TitleMax, entering onto Drummond's property to gather information about Drummond's customers, and using motor vehicle records to identify and solicit those customers in violation of the Driver's Privacy Protection Act. Based on these allegations, Drummond asserted claims against TitleMax for trespass, misappropriation of trade secrets (under the Georgia UTSA), tortious interference with contracts, and unfair competition. Drummond also filed a motion for a nationwide interlocutory injunction to prevent TitleMax from engaging in allegedly unlawful activities. Following a hearing, the trial court granted the injunction in its entirety. TitleMax appealed on the ground that the trial court erred when it found that there was a substantial likelihood that Drummond would prevail on the merits at trial as to each of its claims, and that the injunction was too broad.

After analyzing the merits of each cause of action, the Georgia Supreme Court affirmed the nationwide injunction to the extent it prohibits TitleMax employees and agents from going into Drummond stores for certain purposes, and to the extent that it prohibits TitleMax from offering compensation to Drummond employees for customer referrals. However, as to those aspects of the injunction based on the claims for trespass and misappropriation of trade secrets, the Supreme Court determined that the scope of the injunction was not supported. First, even assuming that Drummond held sufficient ownership in the in each property it sought to exclude TitleMax employees, it could not show that it had similar rights to the parking lots that it shares with other businesses to succeed on the merits of a trespass claim. Second, since Drummond claimed that TitleMax searched databases of motor vehicles to determine which vehicles had liens held by Drummond, and did not claim that TitleMax had taken a tangible customer list, while TitleMax's activity may have violated the Driver's Protection Act, the activity did not constitute a misappropriation of trade secrets in Georgia. Accordingly, the Supreme Court vacated the injunction in certain respects, and remanded the case to the trial court to reconsider the scope of the injunction.

Federal Circuit

CardiAQ Valve Techs., Inc. v. Neovasc Inc., 2017 U.S. App. LEXIS 16856 (Fed. Cir. 2017). CardiAQ Valve Technologies (CardiAQ), Neovasc Inc. and Neovasc Tiara Inc. (collectively Neovasc) both appealed the District Court for the District of Massachusetts's rulings in an action for misappropriation of trade secrets in violation of Massachusetts law. CardiAQ was formed in 2006 with the goal of developing a mitral-valve implant that could be delivered to the heart by catheter rather than open-heart surgery—a transcatheter mitral valve implant, or "TMVI." After developing several prototypes, CardiAQ engaged Neovasc to help with assembly of an aspect of the device. Their work together came to an end after about one year, but during that year, Neovasc secretly launched and ultimately patented its own TMVI projec. CardiAQ sued Neovasc in the District of Massachusetts, alleging that Neovasc had misappropriated several of CardiAQ's trade secrets. At trial, the parties grouped CardiAQ's allegedly misappropriated trade secrets into six agreed-upon categories. The district court found that Neovasc had misappropriated trade secrets described in three of the six categories and awarded CardiAQ $91 million in damages, subsequently denying Neovasc's motion for a new trial as to those three categories and related damages.

On appeal, Neovasc argued that none of the three trade secrets of which it was found liable for misappropriation were deserving of protection. First, Neovasc argued that Trade Secret 4 was neither a secret nor a unified process on the grounds that its description was insufficiently specific to identify a protectable trade secret and that the combination of known elements cannot be a protectable trade secret. The Federal Circuit rejected both arguments, holding respectively that the collection of sixty-one separate specific devices does not preclude a jury finding of specificity and that the presence of some known features similarly does not preclude a jury finding of secrecy. Second, Neovasc argued that Trade Secret 5 was not entitled to protection because CardiAQ disclosed the tool described therein in a published patent application before Neovasc used the tool to ultimately create the device described in its '964 patent. The court rejected this argument based on its finding that the patent did not disclose certain precise dimensions, manufacturing details, and materials. Finally, Neovasc argued that the jury could not find that Trade Secret 6—the developmental history of CardiAQ's product—meets the requirement of continued use, insofar as it was merely "negative know-how" or knowledge of what *not* to do. The court rejected this argument as well, agreeing with the district court's assessment that CardiAQ continues to use its past discoveries about what works and what does not as it further develops its TVMI device and works towards FDA approval. Notably, the court abstained from deciding whether a pure "negative know-how" trade secret would be unprotectable under Massachusetts law.

Organik Kimya, San. ve Tic. A.S. v. ITC, 848 F.3d 994 (Fed. Cir. 2017). Respondents appealed from the International Trade Commission's decision imposing a twenty-five-year limited exclusion order for development of opaque polymers. Organik Kimya and Dow Chemical Company both manufacture opaque polymers, which are used as paint additives to increase the paint's opacity. Dow filed a complaint with the ITC in May 2013 alleging patent infringement and trade secret misappropriation by Organic Kimya. In reviewing the Administrative Law Judge's findings, the ITC determined that the evidence demonstrated that it would have taken Organic Kimya twenty-five years to develop a commercial opaque polymer comparable to Dow's without using Dow's trade secrets. Thus, the Commission imposed a twenty-five-year limited exclusion order with a narrowing provision allowing Organik Kimya to seek an opinion from the Commission that would allow it to import products that it shows were developed without using Dow's misappropriated trade secrets.

On appeal, Organik Kimya argued that the twenty-five-year period was excessive, pointing to various cases to support its assertion that exclusion orders typically last five to ten years. However, the court affirmed the Commission's decision, stating that the Commission bases the time period of a limited exclusion order on a "reasonable research and development period" or an "independent development time" for the trade secrets at issue. The length of the exclusion order therefore depends on the trade secrets at issue and evidence in the record, not the particular length of exclusion orders in other cases. Because the record stated that it would take Organik Kimya fifteen to twenty-five years to develop opaque polymers independently, the Federal Circuit affirmed the order.

State Cases

Illinois

***Better Gov't Ass'n v. Village of Rosemont*, 2017 IL App (1st) 161957**. The plaintiff filed an Illinois Freedom of Information Act (FOIA) request for contracts between the Village of Rosemont and certain privately-owned entertainment venues. Rosemont redacted portions of the contracts it claimed contained trade secrets under the Illinois Trade Secrets Act (ITSA), citing exemptions in FOIA for trade secret information "obtained from a person or business," and for information that is "specifically prohibited from disclosure by federal or State law." The appellate court ruled that the redacted information was not exempt from disclosure, and must be released. The appellate court held that pricing terms in the contracts were not "information obtained from" the private contractor, but instead reflected Rosemont's own standard venue rental rates. In this regard, the court also cited case law holding that negotiated pricing terms are not "obtained from" any private contractual counter-party, and so would not qualify for the trade secret exemption in FOIA. The appellate court also held that the ITSA did not qualify for the "federal or State law" exemption in FOIA. While the ITSA provided that misappropriation (or threatened misappropriation) of a trade secret may be enjoined, it did not "specifically prohibit any disclosures," as required by FOIA. The court further reasoned that the "federal or State law" exemption was likely not intended by the legislature to act as a second exemption for trade secrets, given that an express trade secret exemption already exists in FOIA.

***Tate & Lyle Ingredients Americas LLC v. Craig*, 2017 IL App (4th) 160886-U**. Plaintiff, an industrial starch manufacturer, sued its former employee for trade secret misappropriation under ITSA after the employee emailed, downloaded and printed confidential information before resigning to join a competing company. Plaintiff secured an *ex parte* temporary restraining order prohibiting Defendant from working for his new employer or any other competitor of Plaintiff in any job involving industrial starch, and following an evidentiary hearing, a preliminary injunction with the same prohibitions. The court of appeals affirmed entry of the preliminary injunction. First, the court concluded that there was a fair question—the standard for reviewing a preliminary injunction—that the materials Defendant downloaded and copied qualified as trade secrets. Second, Plaintiff had sufficiently demonstrated "misappropriation" based on a theory of inevitable disclosure. In this regard, the court noted that the two companies were direct competitors, Defendant had expressed a desire to improve his new employer's systems by using strategies from his old company, and Defendant only sent, downloaded, and printed Plaintiff's confidential information *after* securing a job at the new company, suggesting that Plaintiff likely took these steps in anticipation of the new job. The court held that this inference overcame the new employer's efforts to prevent Defendant from using Plaintiff's materials and Defendant's testimony that he returned the materials in question to Plaintiff. The court acknowledged the breadth of the order in prohibiting Defendant from working for any of Plaintiff's competitors for an indefinite time, but still upheld it. In this regard, the court relied on witness testimony explaining that the documents Defendant took, including Plaintiff's strategic plan, would give a competitive advantage to any other starch manufacturer and would remain relevant for at least two to five years. Finally, the appellate court noted that the trial court had found Defendant's testimony not credible with respect to downloading files onto thumb drives, making it difficult to the limit the scope of the injunction based on believing Defendant's statements that he would not use Plaintiff's trade secrets in his new job.

Indiana

***Magnesita Refractories Co. v. Mishra*, 2017 WL 365619 (N.D. Ind. 2017) and 2017 WL 655860 (N.D. Ind. 2017)**. The plaintiff corporation sought and was granted an *ex parte* temporary restraining order under FRCP 65 authorizing the seizure of the laptop of Defendant, a former employee of Plaintiff. The TRO was based on evidence that Defendant was about to misappropriate trade secrets housed on the laptop and provide them to a competing company. In the initial opinion, the court rejected Defendant's argument that FRCP 64(a), and not FRCP 65, should determine whether the court could seize his computer. Under FRCP 64(a), state law governs all seizures meant to satisfy judgments unless a federal statute applies. Defendant argued that the then recently-enacted DTSA was such a federal statute. The court disagreed, holding that not all seizure orders in the trade secrets context had to be pursued under the DTSA. FRCP 64(a), by its own terms, applied to securing property to satisfy a potential judgment, not preserve evidence. Moreover, even if FRCP 64(a) applied, the DTSA still permitted seizures under FRCP 65 as its seizure provision cannot be invoked unless an order under FRCP 65 would be inadequate. *See* 18 U.S.C. § 1836(b)(2)(ii)(I). In the second opinion, the court denied Defendant's motion to dissolve the *ex parte* TRO. The court held that the requirements of FRCP 65(b) for issuing a TRO without notice were satisfied because Plaintiff had presented evidence that Defendant's laptop contained Plaintiff's trade secrets, Defendant was having on-going meetings with a company that competes against

Plaintiff, and there was reason to believe Defendant would delete or modify the evidence on his laptop if given notice. The court also rejected Defendant's contention that the *ex parte* TRO was overbroad; instead, it merely required seizure of the laptop, which was then left in the secure custody of the court. Finally, the court refused to dissolve the TRO, as Defendant's explanation that his assistance to the competing company was only to facilitate a work permit for a founder did not excuse that behavior.

***McFreen v. Alcatel-Lucent USA Inc.,* 2017 WL 1091215, (S.D. Ind. 2017)**. Plaintiff, an individual inventor, sued Defendant, a telecommunications technology company, alleging violation of the parties' mutual nondisclosure agreement and the California UTSA. Plaintiff alleged that Defendant used his alleged trade secret—a concept of an Internet-based system for accessing video, audio, and the Internet from a single portal. Defendant sought partial summary judgment on the issue of whether it (or a predecessor company) had given Plaintiff's confidential information to a third party, which eventually came out with a successful product with an underlying "concept" similar to Plaintiff's. The court granted Defendant's motion. First, there was unrebutted evidence that the third party had begun exploring the "concept" before the earliest date Defendant allegedly passed the confidential "concept" to the third party. Second, Plaintiff argued that Defendant had held merger discussions with the third party that Plaintiff contended likely included conversations about Plaintiff's trade secrets. The court disagreed, holding that it was unreasonable to assume the parties shared Plaintiff's confidential information simply because they considered merging. Third, the court also rejected Plaintiff's contention that the former company gave the third party other confidential information directly during previous business deals, concluding that two large companies doing some business together, without more, was not evidence of exchanging confidential information on other types of business. The court noted that Plaintiff was unable to point to any overlap of personnel on those deals with Defendant's personnel who would have had knowledge of Plaintiff's confidential concept.

<u>Massachusetts</u>

***Gillette Company v. Provost,* 91 Mass. App. Ct. 133, 74 N.E.3d 275 (2017)**. In Gillette's action against former employees and their new employer ShaveLogic, alleging misappropriation of trade secrets and confidential information, the trial court denied Gillette's motion to dismiss ShaveLogic's counterclaim, alleging Gillette's claims were brought in bad faith. The trial court concluded Gillette's lawsuit was not petitioning activity protected under the anti-SLAPP statute because the claims for misappropriation were devoid of any reasonable factual support and had caused ShaveLogic an actual injury such as loss of potential investors and marketing partners. The gravamen of Gillette's complaint was that defendants had allegedly "used Gillette confidential information and trade secrets to design . . . magnetic attachment and elastomeric pivot concepts." In affirming the trial court's order denying Gillette's motion to dismiss, the Court of Appeal noted that ShaveLogic's evidence showed the general concept of using magnetic attachments in razors was in the public domain as early as 1919, and the concept of using elastomeric pivots in razors was publicly known before the former employees joined ShaveLogic. According to the court of appeal, at the hearing on the motion, Gillette admitted the concepts were not trade secrets or protectable intellectual property. ShaveLogic also submitted detailed declarations from the individual defendants, all of whom denied working on any projects at Gillette involving magnetic attachments or elastomeric returns like those developed years later at ShaveLogic. By contrast, Gillette submitted a single declaration in which its counsel asserted that Gillette sent its prelitigation letters and filed the lawsuit for a legitimate good faith purpose, to protect its intellectual property and its investment in its confidential product development. The court of appeal concluded that given this record, the trial judge was within her discretion to find by a preponderance of the evidence that Gillette's complaint lacked any reasonable factual basis.

Texas

***Elite Auto Body LLC v. Autocraft Bodywerks, Inc.*, 520 S.W.3d 191 (Tex. App. 2017)**. Auto-repair shop Autocraft brought an action against former employees and members of a competing business (Elite) alleging trade-secret misappropriation, violation of the Texas UTSA, unfair competition, breach of fiduciary duty, and civil conspiracy. Elite moved for dismissal under the Texas Citizens Participation Act (TCPA) alleging that Autocraft's lawsuit constituted an improper legal action based upon or in response to Elite's exercise of free association and exercise of free speech. The trial court denied Elite's motion to dismiss. On appeal, the Court of Appeals of Texas held that the TCPA protections were not limited to public communications. That communications among the Elite employees through which they allegedly shared or used Autocraft's confidential, proprietary, and trade secret information – including client forms, technical service bulletins and salary information-constituted protected "communications" under the TCPA. The court further held that the use of this information by Elite to lure Autocraft employees and further Elite's competitive position satisfied the TCPA's definition of the "exercise of the right of association" and so Autocraft's lawsuit was "based on, related to, or was in response to" Elite's exercise of the right of association and the trial court should have granted Elite's motion to dismiss.

Wisconsin

***North Highland Inc. v. Jefferson Machine & Tool Inc.*, 898 N.W.2d 741 (Wis. 2017)**. The defendant created a business with the plaintiff corporation's employee that competed with the plaintiff even while the employee, who did not have a non-compete, still worked for the plaintiff. The employee worked on a bid for a project for both the plaintiff and the competing business. After the competing business won the bid, the plaintiff sued alleging, among other things, misappropriation of its trade secrets—namely, its bid amount—in violation of the Wisconsin UTSA. The appellate court had affirmed summary judgment for the defendant because the amount of a confidential bid was not "information" for the purposes of the definition of trade secret under the Wisconsin UTSA. In a 4-3 decision, the Wisconsin Supreme Court affirmed on an alternative basis, holding that the plaintiff had failed to establish that the individual defendant knew that his business partner (plaintiff's employee) had knowledge of the trade secret at issue, as would be required to hold that defendant liable for misappropriation. The dissent, looking to law from other jurisdictions, argued that the amount of a confidential bid should be a protectable trade secret under the Wisconsin UTSA, and further believed there were fact issues precluding summary judgment on the basis chosen by the majority.