

# Contents

05	Authors	25	Ilinois
06	Our Team	29	Maryland
08	Executive Summary	31	Massachusetts
II	California	37	New York
18	Delaware	42	Texas
20	Florida	46	Virginia

Georgia

23



# Smart In Your World

# **Safeguarding Your Critical Assets**

Trade secrets are often among a company's most valuable assets. From conducting trade secret audits and drafting trade secret policies and confidentiality agreements, to litigating misappropriation and non-compete cases in venues across the country, Arent Fox attorneys have the experience to help clients safeguard their critical assets.

# **Authors**



Linda M. Jackson

Partner, DC

202.775.5785

linda.jackson@arentfox.com



**Dana J. Finberg**Partner, SF
415.757.5897
dana.finberg@arentfox.com



Alexander H. Spiegler
Partner, NY
212.457.5454
alexander.spiegler@arentfox.com



Allan E. Anderson

Partner, LA

213.443.7683

allan.anderson@arentfox.com



Sara T. Schneider
Partner, LA
415.757.5911
sara.schneider@arentfox.com



Lauren C. Schaefer Associate, BOS 617.973.6120 lauren.schaefer@arentfox.com



Jake Christensen
Associate, SF
415.805.7998
jake.christensen@arentfox.com



Alexandra M. Romero
Associate, DC
202.828.3469
alexandra.romero@arentfox.com



Nadia Patel Associate, DC 202.775.5716 nadia.patel@arentfox.com



Morgan R. Pankow

Associate, DC
202.857.6495
morgan.pankow@arentfox.com



Natalie C. Kreeger Associate, LA 213.443.7693 natalie.kreeger@arentfox.com



**Tenese L. Lockhart**Associate, NY
212.457.5598
tenese.lockhart@arentfox.com

### **Our Team**

Linda M. Jackson

Partner, DC 202.775.5785 linda.jackson@arentfox.com

Michael L. Stevens

Labor & Employment
Practice Group Leader, DC
202.857.6382
michael.stevens@arentfox.com

**Jerrold Abeles** 

Partner, LA 213.629.7407 jerry.abeles@arentfox.com

**Craig Gelfound** 

Partner, LA 213.443.7604 craig.gelfound@arentfox.com

**Eric Roman** 

Counsel, NY 212.492.3283 eric.roman@arentfox.com

Samantha K. Collins

Associate, DC 202.857.6221 samantha.collins@arentfox.com

Alexandra M. Romero

Associate, DC 202.828.3469 alexandra.romero@arentfox.com Dana J. Finberg

Partner, SF 415.757.5897 dana.finberg@arentfox.com

Robert K. Carrol

Partner, SF 415.805.7973 robert.carrol@arentfox.com

Nicholas J. Nesgos

Partner, BOS 617.973.6168 nicholas.nesgos@arentfox.com

Peter R. Zeidenberg

Partner, DC 202.857.6139 peter.zeidenberg@arentfox.com

Roxanne M. Wilson

Counsel, LA 213.443.7515 roxanne.wilson@arentfox.com

Tenese L. Lockhart

Associate, NY 212.457.5598 tenese.lockhart@arentfox.com

Lauren C. Schaefer

Associate, BOS 617.973.6120 lauren.schaefer@arentfox.com Allan E. Anderson

Partner, LA 213.443.7683 allan.anderson@arentfox.com

Amal U. Dave

Partner, DC 202.857.6336 amal.dave@arentfox.com

Valerie C. Samuels

Partner, BOS 617.973.6248 valerie.samuels@arentfox.com

John Zaimes

Partner, LA 213.443.7543 john.zaimes@arentfox.com

Stefan Bogdanovich

Associate, LA 213.443.7637 stefan.bogdanovich@arentfox.com

Morgan R. Pankow

Associate, DC 202.857.6495 morgan.pankow@arentfox.com

**Anthony J. Orler** 

Attorney, LA 213. 443.7531 anthony.orler@arentfox.com Alexander H. Spiegler

Partner, NY 212.457.5454 alexander.spiegler@arentfox.com

**Darrell S. Gay** 

Partner, NY 212.457.5465 darrell.gay@arentfox.com

Sara T. Schneider

Partner, LA 415.757.5911 sara.schneider@arentfox.com

Stewart S. Manela

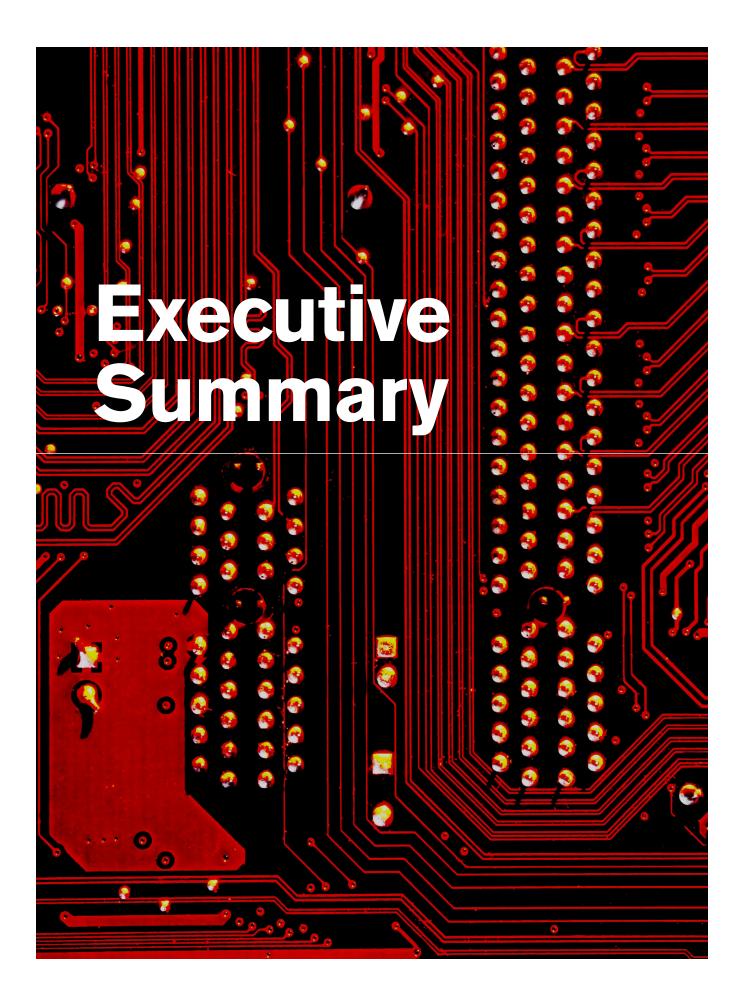
Counsel, DC 202.857.6364 stewart.manela@arentfox.com

**Jake Christensen** 

Associate, SF 415.805.7998 jake.christensen@arentfox.com

Nadia Patel

Associate, DC 202.775.5716 nadia.patel@arentfox.com



# **Trade Secret 2020 Whitepaper**

2020 was a unique year in many ways. Nevertheless, trade secrets remained a critical piece of intellectual property for companies of all sizes, in all industries, and in all geographies.

As increasing scrutiny was cast at the state and federal level on noncompetition agreements and other restrictive covenants, companies were forced to assess their ability to safeguard trade secret information. Not to mention the global pandemic, which changed the way many companies interact with their employees, and the way that employees, in turn, interact with company trade secrets. Despite the challenges, litigation in the trade secrets space stayed strong, with increasingly high damages awards and even the risk of criminal charges. This white paper will take a look at these and other issues in the trade secret space in 2020.

#### **FTC Public Workshop**

The year kicked off with a public workshop held by the Federal Trade Commission on January 9, 2020 to consider whether there was a sufficient legal basis for the FTC to issue a rule that would restrict or prohibit the use of non-competes in employment contracts. The FTC workshop reflected a growing attention to the use of non-compete agreements in today's labor markets and their associated impact on low-income workers and worker mobility. Among the takeaways from the workshop was a general agreement that there is little justification for the imposition of non-competes on low-wage workers, but that a wholesale ban on non-competes may not be the correct approach.

#### **State Level Non-compete Legislation**

This focus on the impact of non-competes on low-wage workers was also reflected in state-level legislation throughout 2020. For example, effective January I, 2020 in Washington state, noncompetition agreements are only enforceable against employees who earn more than \$100,000 per year and independent contractors who earn more than \$250,000 per year. The state also imposed additional limitations on the use of restrictive covenants, and critically, was retroactive in its application. Next, Rhode Island's Noncompetition Agreement Act, which prohibits non-compete agreements with nonexempt workers, interns and short-term student employees, anyone

younger than 19, and employees whose average annual earnings are less than 250% of the federal poverty levels, went into effect on January 15, 2020. Finally, in Virginia, effective July 1, 2020, non-competes with low-wage employees were prohibited.

Other states also tightened the reigns on the use of non-competes in other ways. For instance, in Oregon, new legislation requires that a signed, written copy of the terms of the noncompetition agreement be provided to the employee within 30 days after the date of the employee's termination.

#### **COVID-19 and Trade Secrets**

In early Spring 2020, much of the United States was subject to shelter in place orders as a result of the COVID-19 pandemic, with entire workforces transitioned to a remote work environment and layoffs across industries leading to record unemployment levels. This shift in the way that many companies worked brought with it new risks for protecting trade secrets and questions about what would qualify as reasonable measures. The use of Zoom, for example, highlighted issues of confidentiality and publication of information, which was analyzed in detail in the case of Smash Franchise Partners, LLC v. Kanda Holdings, a Delaware chancery court opinion that highlighted the importance of security measures in an increasingly remote work environment. These remote work issues are here to stay in 2021.

#### **Litigation Trends**

Despite the wide-ranging effects of the pandemic, litigation in the trade secret space was robust throughout 2020. Trade secrets are critical intellectual property for companies of all sizes, in all geographies, and across industries, and the litigation trends reflect this as well. For example, in the **cannabis industry**, the Northern District of Illinois issued a preliminary injunction for DTSA and CFAA claims in *GCM Partners*, *LLC v. Hipaaline*. The case involves a provider of telehealth services for medical cannabis

patients and its software platform provider. In fashion and retail, pending litigation in the East District of Pennsylvania between Le Tote, Inc. and Urban Outfitters, Inc. involves the alleged misappropriation of trade secrets after an anticipated acquisition fell through. In e-commerce, a business that boomed this year as consumers stayed home, the Northern District of California issued a decision that OSHA Form 300A data summarizing Amazon warehouse worker injuries and illnesses that were reported to the Department of Labor's Occupational Safety and Health Administration did not qualify as a privileged and confidential trade secret or confidential and financial information exempt from disclosure under Exemption 4 of the Freedom of Information Act, in the case of Center for Investigative Reporting v. United States Department of Labor. And, as for the **consumer products** space, let's not forget Peloton Interactive, Inc., whose earnings skyrocketed as consumers transitioned to at-home workouts, and who sought to protect its intellectual property by bringing suit in the District of Delaware against competitor ICON Health and Fitness (the maker of Nordic Track), which Peloton alleges sought "to improperly acquire Peloton's trade secret advertising plans."

2020 also continued to prove that the damages associated with trade secret misappropriation can be significant. In May, the Northern District of Illinois entered a judgment for over \$764 million in Motorola Solutions, Inc. v. Hytera Communications Corp. Ltd., a case brought on the basis of the extraterritorial application of the Defend Trade Secrets Act, with the misappropriation taking place in Malaysia. The award was cut by \$200 million in January 2021. In October 2020, in Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Grp., we saw an even larger damages award of over \$854 million, including \$569.7 million in punitive damages, come out of the Southern District of New York based on the misappropriation of over 100 TriZetto trade secrets and infringement of copyrights. Perhaps unsurprisingly, this damages award is currently being contested.

#### **Criminal Implications**

In addition to substantial civil damages, trade secret misappropriation can lead to criminal implications. In *United States v. Smith*, the Northern District of Florida upheld a guilty verdict against an individual who hacked into the a company's private computer system for computer fraud, theft of trade secrets, and extortion in relation to offshore fishing reef location coordinates. The case is currently on appeal. The Department of Justice also stepped into the ring in 2020 and issued its first indictments for use of naked no-poach agreements and wage fixing since issuing the Antitrust Guidance for Human Resources Professionals in 2016.

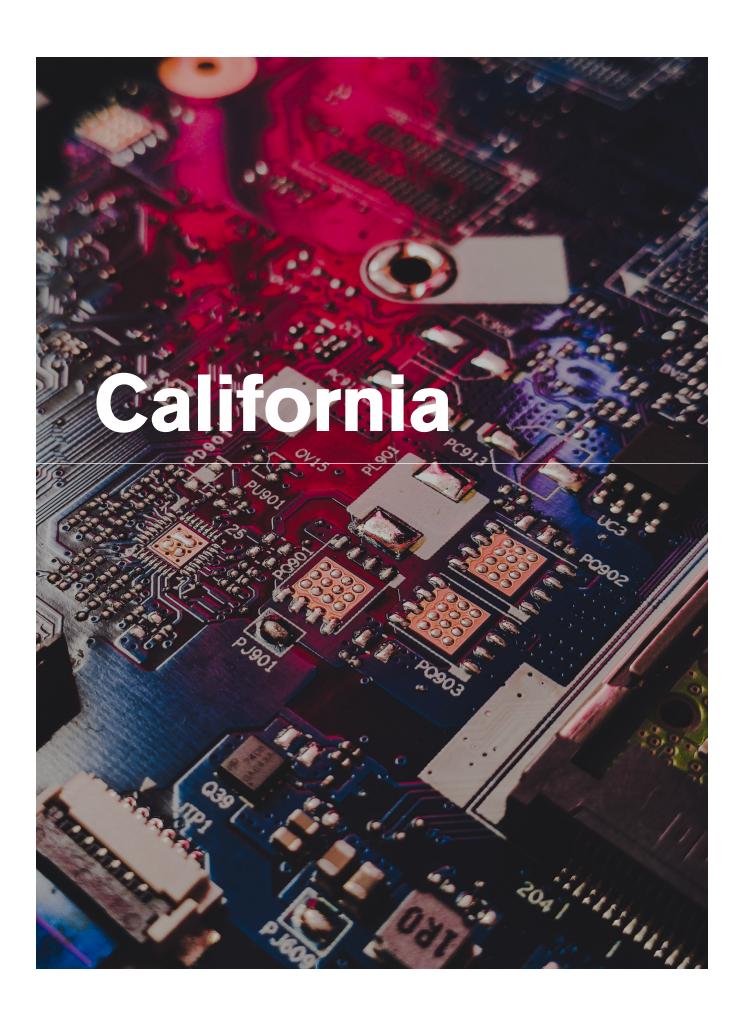
#### **Defend Trade Secrets Act**

As we approach five year anniversary of the passing of the Defend Trade Secrets Act ("DTSA"), now is a good opportunity to assess whether progress has been made toward the goal of uniformity in trade secret law. Certainly we have seen an increase in litigation in the federal courts since 2016, but the application of trade secret law has been somewhat jurisdiction specific. For example, the issue of preemption of state law tort claims premised on misappropriation of trade secrets by state UTSA corollaries has been decided differently in California (broad preemption), Massachusetts (no preemption), and Virginia (narrow preemption). Moreover, one of the most controversial and buzzworthy provisions of the DTSA – the remedy of ex parte seizure – has scarcely been granted at all.

#### 2021 and Beyond

As we make our way into 2021, it has become clear that the trends from 2020 are here to stay. In particular, President Biden has announced his intention to "Eliminate non-compete clauses and no-poaching agreements that hinder the ability of employees to seek higher wages, better benefits, and working conditions by changing employers." Soon after this announcement, on January II, 202I, DC's Mayor signed into law the Ban on Non-Compete Agreements Amendment Act of 2020, passed by the Council of the District of Columbia in December 2020. This law will serve as a near-total ban on the use of non-competes in DC.

In light of this movement away from the use of noncompetition agreements, and with an increasingly remote workforce with access to confidential and trade secret information, it is more critical than ever that businesses ensure that their confidential and trade secret information is protected. Companies should audit their trade secret information, and institute a series of safeguards to protect against misappropriation. In particular, companies should consider the use of nondisclosure agreements, non-solicitation and no-raid provisions, and alternative forms of noncompetes such as garden leave provisions or forfeiture for competition provisions. From a policy perspective, companies must institute clearly communicated information security procedures, rules regarding the use of company devices, and comply with exit interview procedures and reminders about ongoing confidentiality obligations. Through these avenues, trade secrets will continue to be a source of competitive advantage for companies who protect them correctly.



#### I. California

- a. Federal Court
  - i. Ninth Circuit
    - I. Prostar Wireless Grp., LLC v. Domino's Pizza, Inc., 815 F. App'x 117 (9th Cir. 2020)
      - a. **Issue:** Whether Domino's could be held liable for: (I) misappropriation of trade secrets; (2) breach of an implied contract or the covenant of fair dealing absent evidence showing the existence of an implied-in-fact contract with terms definite enough to be enforced; and (3) deceit, negligent misrepresentation, or unfair competition absent evidence that it was reasonable for group to believe company was committed to ultimately approving the system.
      - b. Holding: Affirmed that Domino's could not be liable for any of the above causes of action.
      - c. **Procedural Posture:** Appeal of grant of summary judgment in favor of Defendant.
      - d. **Relevant Background:** A wireless services group brought ten claims under California law against Domino's Pizza after Domino's declined to provide the approval necessary to enable the wireless services group to sell, for use in Domino's locations, a GPS-based driver-tracking solution that it had developed in collaboration with Domino's over the course of several years.

The court held that Domino's was not liable for misappropriation of trade secrets because there was no evidence that it ever had access to the algorithms, or that the algorithms were discernible from materials that the wireless services group shared with Domino's. The trade secret claim also failed because the wireless services group made insufficient efforts to keep the system architecture secret when it had shared conceptual design overviews and technical specification for the system with pizza and IT companies without nondisclosure agreements in place.

The court also held that Domino's could not be held liable under California law for breach of an implied contract or breach of the covenant of fair dealing arising out of its failure to approve the GPS system absent evidence showing the existence of an implied-in-fact contract with terms definite enough to be enforced. Although the wireless services group alleged that the parties engaged in a lengthy development project based on a mutual understanding that, if successful, the wireless services group would be allowed to market and sell the system to Domino's franchisees, the evidence supported only an inference that the company hoped enough progress would be made to allow the parties to reach an agreement in the future.

Finally, the court held that Domino's was not liable for deceit, negligent misrepresentation or unfair competition, because there was no evidence showing that it was reasonable for the wireless services group to believe that Domino's was committed to ultimately approving the system.

- e. **Takeaway:** To be a trade secret, the information must be maintained as a secret and derive value from the fact that it's a secret. Companies sharing trade secrets with outside parties should ensure appropriate safeguards are in place to ensure the trade secret is protected, including confidentiality agreements or NDAs.
- 2. *InteliClear, LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653, 655 (9th Cir. 2020)
  - a. **Issue:** Whether plaintiff identified a trade secret with sufficient particularity.
  - b. Holding: Triable issues of fact existed and reversal of grant of summary judgment for defendant.
  - c. Procedural Posture: Appeal of grant of summary judgment in favor of Defendant.
  - d. Relevant Background: InteliClear developed a comprehensive electronic system for managing stock brokerage firm accounting, securities clearance, and securities settlement services. ETC's predecessor and later subsidiary obtained a license of the InteliClear System from InteliClear and signed a Software License Agreement. The agreement acknowledged that all information InteliClear provided was confidential, proprietary, and copyrighted, and through the agreement, ETC agreed to maintain that information in confidence "during and after" the terms of the agreement. The rights, duties, and obligations under the License Agreement were assigned and delegated to Defendant ETC in 2012. ETC later terminated the agreement, and certified that it had destroyed all copies of InteliClear's system. But before

terminating the Software License Agreement, ETC had begun building its own securities clearing software. Shortly thereafter, ETC deployed its own new electronic trading system.

The court held that, to show existence of a trade secret protected by the Defense of Trade Secrets Act (DTSA), a plaintiff should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons skilled in the trade, and may not simply rely upon catchall phrases or identify categories of trade secrets they intend to pursue at trial. It is inadequate for plaintiffs to cite and incorporate by reference hundreds of documents that purportedly reference or reflect the trade secret information.

InteliClear described its trade secrets as "the InteliClear System's unique design and concepts and the unique software, formulas, processes, programs, tools, techniques, tables, fields, functionality, and logic by which its components interrelate and process data," and produced two declarations expanding on and describing specific features of the System as trade secrets. The declarations outlined the specific tables, table columns, account identifiers, codes, and methodologies InteliClear claimed as trade secrets. The court held that there was a genuine issue of material fact as to whether InteliClear identified its trade secrets with sufficient particularity, because a reasonable jury could conclude that the uniquely designed tables, columns, account number structures, methods of populating table data, and combination or interrelation thereof, are protectable trade secrets. InteliClear identified aspects of its database logic and architecture with enough specificity to create a triable issue of fact.

The court noted that defendant moved for summary judgment immediately after discovery opened and stated, "[a]t this stage, particularly where no discovery whatsoever had occurred, it is not fatal to InteliClear's claim that its hedging language left open the possibility of expanding its identifications later. InteliClear's burden is only to identify at least one trade secret with sufficient particularity to create a triable issue." The court concluded that its decision balanced two competing interests: "Refining trade secret identifications through discovery makes good sense. The process acknowledges the inherent tension between a party's desire to protect legitimate intellectual property claims and the need for intellectual property law to prevent unnecessary obstacles to useful competition."

- e. **Takeaway:** It is unwise to move for summary judgment on the particularity of trade secrets before the parties have had an opportunity to conduct discovery. Nevertheless, Plaintiffs should identify trade secrets with as much particularity as possible at the outset of the case, and should use declarations (filed under seal) to identify the specific trade secrets at issue.
- 3. *Attia v. Google LLC*, 983 F.3d 420 (9th Cir. 2020)
  - a. **Issues:** Whether: (i) the disclosure of a trade secret prior to the enactment of the Defend Trade Secrets Act (DTSA) forecloses the possibility of a DTSA claim arising from the continued use of the trade secret post-enactment; and (ii) disclosure of alleged trade secret information in patent applications destroys trade secret status.
  - b. **Holding:** Misappropriation prior to the enactment of the DTSA does not preclude a claim arising from post-enactment misappropriation or continued use of the same trade secret; however, filing such trade secret information in a patent application eliminates any trade secrecy and invalidates a claim of misappropriation.
  - c. Procedural Posture: Appeal of grant of motion to dismiss.
  - d. **Factual Background:** Attia developed a new architecture technology and partnered with Google to further develop the technology and monetize it. To that end, Attia disclosed his trade secrets to Google in 2010. Google applied for patent applications in 2012 incorporating Attia's trade secrets. Google then allegedly excluded Attia from the project and used Attia's trade secrets to create a new venture.

Attia sued Google in 2014 for state law trade secret and contract claims. Following the enactment of the DTSA in 2016, Attia amended his complaint to include DTSA and RICO claims.

The Court noted that, unlike the Uniform Trade Secrets Act (UTSA), which contains an

anti-continued use provision, the DTSA does not, suggesting that the DTSA is not limited to misappropriation that began after enactment of the DTSA. Because Congress was aware of the UTSA at the time it passed the DTSA, this omission is significant, and the Court held that misappropriation prior to the enactment of the DTSA does not preclude a claim arising from post-enactment misappropriation or continued use of the same trade secret.

However, the Court also noted that Google had disclosed the trade secrets in patent applications and to investors in 2012, and Attia was aware of such disclosures. It is well-settled that publication of information in a patent application eliminates its trade secrecy. Attia's alleged trade secrets were completely parallel to what was disclosed in the published patent applications. As a result, the trade secret status was extinguished.

e. **Takeaway:** Claims under the DTSA for continued misappropriation may be successful, but trade secrets owners must still protect the secrecy of their information in order to state such a claim.

#### ii. District Court

- I. *Albert's Organics, Inc. v. Holzman*, 445 F. Supp. 3d 463, 469 (N.D. Cal. 2020).
  - a. **Issue:** Whether a specialty produce company-employer alleged sufficient facts to demonstrate that its claimed confidential and trade secret information qualified as a trade secret under the Defend Trade Secrets Act ("DTSA") and California Uniform Trade Secrets Act ("CUTSA"), and whether the CUTSA preempted the employer's claims for tortious interference with business relationship, violations of California's Unfair Competition Law, and interference with prospective economic advantage.
  - b. **Holding:** While allegations related to certain categories of alleged protected information lacked particularity sufficient to put the former employee-defendants on notice as to the specific alleged trade secrets, the employer sufficiently alleged claims for misappropriation of trade secrets under the DTSA and CUTSA as to its customer information list because the employer alleged that it developed, maintained, and safeguarded its customer information at great expense and that former employees were trained on the importance of maintaining confidentiality of the employer's customer list. Further, the CUTSA preempted the employer's claims for tortious interference with business relationship, violations of California's Unfair Competition Law, and interference with prospective economic advantage.
  - c. Procedural Posture: Motion to Dismiss.
  - d. Relevant Background: A specialty produce company purchased a produce broker and distributor, and, as a condition of the purchase agreement, hired the broker/distributor's two former owners. The former owners signed employment agreements with the company restricting their use of the company's confidential and proprietary information and trade secrets to the company's legitimate business purposes. The company and former owners also agreed that, should the former owners wish to work at a competing business while employed by the company, the former employees would first seek permission from the company. The former owners also agreed to return all confidential and proprietary company information and trade secrets to the company upon their termination.
    - Years later, one of the former owners was terminated and almost immediately engaged with the company's competitors, business partners, and investors to form a new, competing company. To recruit company customers, suppliers, and key employees to launch the new company, the former owner further disclosed the names of the company's customers and suppliers, employees, pricing and financing resources, potential venture partners, and key confidential business relationships, as well as key business information (the company's plans to expand into certain markets, investment commitments and profitability, business model, product sources, and import volumes). The former owner also enlisted the other former owner, who was still working at the company, to recruit other company employees to work for their new competing business.
  - e. **Takeaway:** Where a company has spent considerable time, effort, and resources developing its customer information lists and the company made reasonable efforts to maintain the secrecy of the list, the list most likely constitutes a protectable trade secret. Further, trade secret claims must be alleged with particularity sufficient to put the opposing party on notice as to the specific trade secret at issue. Finally, the CUTSA displaces common law claims that are rooted in the

same nucleus of operative facts as a claim based on the misappropriation of trade secrets.

- 2. Erhart v. Bofl Holding, Inc., No. 15-civ-02287, 2020 WL 1550207 (S.D. Cal. Mar. 31, 2020).
  - a. **Issue:** Whether an employer can enforce an employee's confidentiality agreement as to confidential employer documents disclosed to regulators as part of a whistleblower complaint, and whether the California Uniform Trade Secrets Act ("CUTSA") displaces common law claims of fraud, conversion, and breach of the duty of loyalty that are rooted in the same nucleus of operative facts as a claim based on the misappropriation of trade secrets.
  - b. **Holding:** Summary judgment granted in favor of employer on majority of former employee's whistleblower claims, which did not fit within narrow scope of protected activity under the Sarbanes-Oxley and Dodd-Frank Acts. Summary judgment granted in favor of former employee on the majority of employer's misappropriation of confidential business information claims related to confidential documents taken by the former employee and that were pleaded under common law tort rather than as trade secrets, and were preempted by the CUTSA as a result. (Court also previously ruled that employer-internet bank could not enforce former employee-auditor's confidentiality agreement regarding confidential documents tied to his whistleblowing activity.)
  - c. Procedural Posture: Cross Motions for Summary Judgment.
  - d. Relevant Background: Internal company auditor filed a whistleblower lawsuit against former bank-employer under Sarbanes-Oxley and Dodd-Frank Acts, claiming he had been retaliated against for reporting illegal conduct at the bank. Bank alleged numerous tort claims including fraud, negligence, conversion, and breach of duty related to the employee's liability for "misappropriat[ing]" confidential and proprietary business documents, but did not allege a misappropriation of trade secrets claim. The court reasoned that CUTSA displaced the Bank's claims that were "based on the same nucleus of facts as the misappropriation of trade secrets claim for relief" and were "premised on the wrongful taking and use of confidential business and proprietary information," even though "that information does not meet the statutory definition of a trade secret." By not pleading a trade secrets misappropriation claim, the court found that the Bank sidestepped CUTSA's requirements, including proving that the information rose to the level of a protectable trade secret, which the Bank likely would not have been able to achieve.
  - e. Takeaway: Employers should rigorously enforce security measures needed to claim trade secret protection, including marking documents as confidential, limiting internal distribution and access, maintaining and enforcing confidentiality agreements, and ensuring that confidential information is protected by established information security best practices. Doing so will increase employers' ability to establish that the documents or information are protectable trade secrets should the need arise.
- 3. *Navigation Holdings, LLC v. Molavi*, 445 F. Supp. 3d 69 (N.D. Cal. 2020)
  - a. **Issue:** Whether trade secrets were identified with sufficient particularity.
  - b. Holding: Plaintiff identified trade secrets with sufficient particularity.
  - c. Procedural Posture: Motion to Dismiss.
  - d. **Relevant Background:** Plaintiffs supply high-quality aluminum alloy products. Defendant was a Vice President of plaintiffs, and eventually served as President. He was charged with negotiating agreements with customers and generating new business. Plaintiffs allege that while still employed with plaintiffs, defendant began to siphon business away to a competing company that he created. Defendant allegedly secured business based upon confidential information and trade secrets that he took from plaintiffs.

The court explained that to defeat a motion to dismiss, the plaintiff must "describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies." Vendavo, Inc. v. Price f(x) AG, No. 17-CV-06930-RS, 2018 WL 1456697, at \*4 (N.D. Cal. Mar. 23, 2018). However, "a plaintiff need not 'spell out the details of the trade secret.' Autodesk, Inc. v. ZWCAD Software Co., No. 5:14-CV-01409-EJD, 2015 WL 2265479, at \*5 (N.D. Cal. May 13, 2015).

Plaintiffs are not required to distinguish the alleged trade secrets from the "more nebulous, larger bucket of confidential information." Plaintiffs asserted two categories of trade secrets: I) client information; and 2) a "specialized process for anodizing unfinished alloy tubes, before machining, for the aerospace industry," and plaintiffs spelled out both in detail, rather than merely setting forth a broad category.

- e. **Takeaway:** Although plaintiffs should identify trade secrets in as much detail as possible in a complaint rather than simply alleging broad categories of confidential information, there is not a "heightened" pleading standard for identifying trade secrets under the DTSA.
- 4. *Snapkeys*, *Ltd. v. Google LLC*, 442 F. Supp. 3d 1196 (N.D. Cal. 2020)
  - a. Issue: Whether fraud claim was superseded by the CUTSA.
  - b. Holding: Fraud claim was superseded by the CUTSA.
  - c. Procedural Posture: Motion to Dismiss.
  - d. Relevant Background: Snapkeys is a "software development company that specializes in creating smartphone and smartwatch keyboard technology." The parties were engaged in discussions to promote Snapkeys' "iType" technology on Google's smartwatches pursuant to an NDA. Snapkeys alleges that, over the course of a year and a half, Google made a number of fraudulent and misleading promises that it would work with Snapkeys and promote Snapkeys' iType keyboard technology, and induced Snapkeys into providing prototypes of the technology. Ultimately Google declined to work with Snapkeys and instead went with a competitor of Snapkeys to develop similar technology. Snapkeys original complaint alleged a misappropriation of trade secrets claim, but its amended complaint did not (because the alleged secrets had been made public).

The court concluded that Snapkeys' fraud claim was superseded by the CUTSA. Specifically, "[t]o survive preemption, [a claim] must 'allege wrongdoing that is materially distinct from the wrongdoing alleged in a CUTSA claim.' "Prostar, 360 F. Supp. 3d at 1006 (quoting SunPower, 2012 WL 6160472, at \*9).

Snapkeys alleges that Google misrepresented that Google "would engage in an agreement and business relationship" with Snapkeys, even though "Google's true intent was to ... misappropriate Plaintiff's technology into its own smartwatch keyboard, and/or provide that technology to Plaintiff's competitors." Snapkeys argued that its fraud claim did not depend on the existence of any trade secret, and that Google's representations were fraudulent with or without any confidential information actually being exchanged.

The court disagreed because the subject of the misrepresentations are of no moment to the CUTSA supersession analysis, which instead asks whether, "stripped of facts supporting trade secret misappropriation, the remaining factual allegations can be reassembled to independently support other causes of action."

e. Takeaway: Be careful of presenting a misappropriation claim as a fraud claim in California.

#### b. State Court

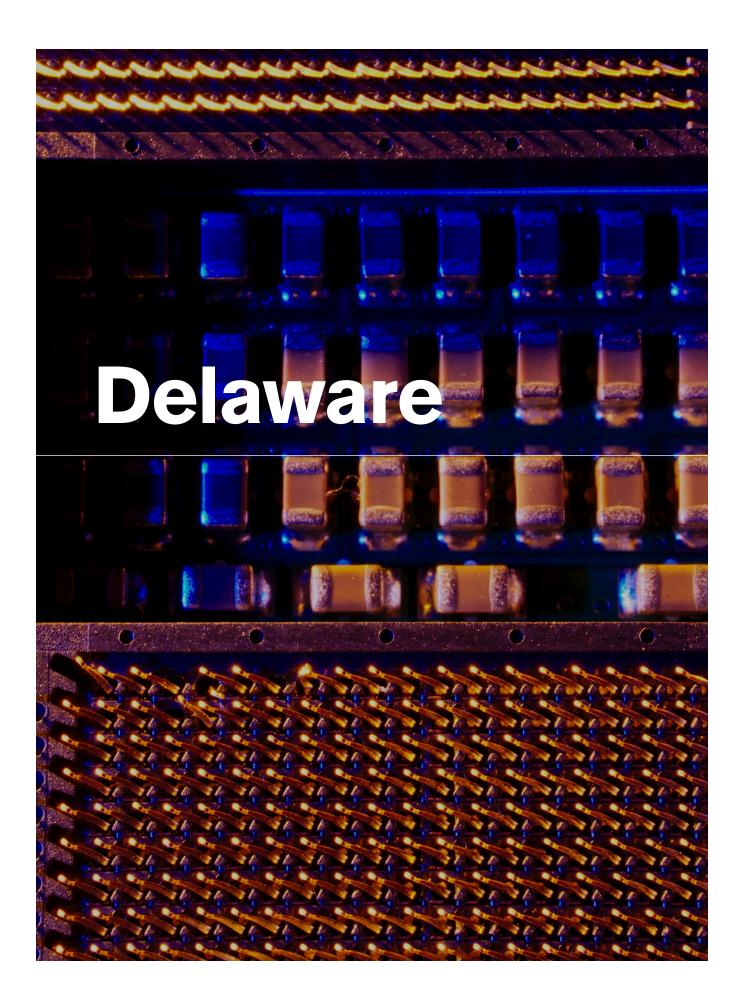
- i. Appellate Court
  - I. Amgen Inc. v. Health Care Servs., 260 Cal. Rptr. 3d 873 (Cal. Ct. App. 2020), review denied (Aug. 26, 2020).
    - a. **Issue:** Whether a pharmaceutical manufacturer's drug price increase notice was a trade secret and therefore exempt from disclosure under the California Public Records Act (CPRA).
    - b. **Holding:** The court of appeals reversed the trial court's order granting a preliminary injunction in favor of a pharmaceutical manufacturer because the company failed to demonstrate how its price increase notice was a trade secret.
    - c. **Procedural Posture:** Appeal of Grant of Motion for Preliminary Injunction, Demurrer to Complaint, and Petition for Writ of Mandate.
    - d. **Relevant Background:** A pharmaceutical manufacturer was statutorily compelled to disclose its drug price increase notice to more than 170 registered purchasers, which were also required by

statute to disclose to their large contracting public and private purchasers. The pharmaceutical manufacturer imposed no obligation to maintain confidentiality on the recipients of the drug price increase notice. A news organization thereafter made a CPRA request for the drug price increase notice after the pharmaceutical manufacturer provided it to the California Correctional Health Care Services (CCHCS). The pharmaceutical manufacturer filed a complaint and petition for writ of mandate, seeking declaratory and injunctive relief to prevent the disclosure of the drug price increase notice. The trial court granted a preliminary injunction, which CCHCS appealed.

- e. **Takeaway:** Documents or information disclosed as part of mandatory government reporting and that are not required to be treated confidentially by the recipients are likely not eligible for an exemption from required disclosure under the California Public Records Act.
- 2. *Hooked Media Grp., Inc. v. Apple Inc.*, 55 Cal. App. 5th 323, 269 Cal. Rptr. 3d 406, reh'g denied (Cal. Ct. App. June 19, 2020), publication ordered (Sept. 30, 2020), review filed (Nov. 6, 2020), review granted and cause transferred sub nom. Hooked Media Grp. v. Apple, 472 P.3d 1064 (Cal. 2020)
  - a. **Issue:** Whether plaintiff established misappropriation of trade secrets.
  - b. Holding: Apple did not improperly use or acquire trade secrets.
  - c. **Procedural Posture:** Trial court granted summary judgment in favor of Defendant.
  - d. Relevant Background: Hooked Media Group is a startup company that Apple expressed interest in acquiring. Representatives from each company met to explore a possible acquisition but Apple ultimately passed. Then, three of Hooked's most important employees left to work for Apple. Hooked sued for fraud; misappropriation of trade secrets; interference with contract and prospective economic advantage; aiding and abetting breach of fiduciary duty; unfair business practices; and unjust enrichment.

The court held that the misappropriation of trade secrets claim failed because there was no evidence that Apple improperly used or acquired the alleged trade secrets. Hooked argued that its former employees were assigned to tasks at Apple similar to the work they did at Hooked and within weeks one of them produced a detailed plan for a recommendations system much like Hooked's version. Further, an expert opined that the source code for Apple's recommendations system was similar to the source code for Hooked's. The court agreed the evidence suggested that the engineers drew on knowledge and skills they gained from Hooked to develop a product for their new employer, but that California's policy favoring free mobility for employees specifically allows that. "Allowing an action for trade secret misappropriation against a former employee for using his or her own knowledge to benefit a new employer is impermissible because it would be equivalent to retroactively imposing on the employee a covenant not to compete."

e. **Takeaway:** Employers should ensure they implement appropriate safeguards to protect trade secrets, including ensuring employees know what information is confidential and return trade secret information upon departure. Employers should also take steps to prohibit new employees from using a former employer's trade secrets.



#### II. Delaware

#### a. State

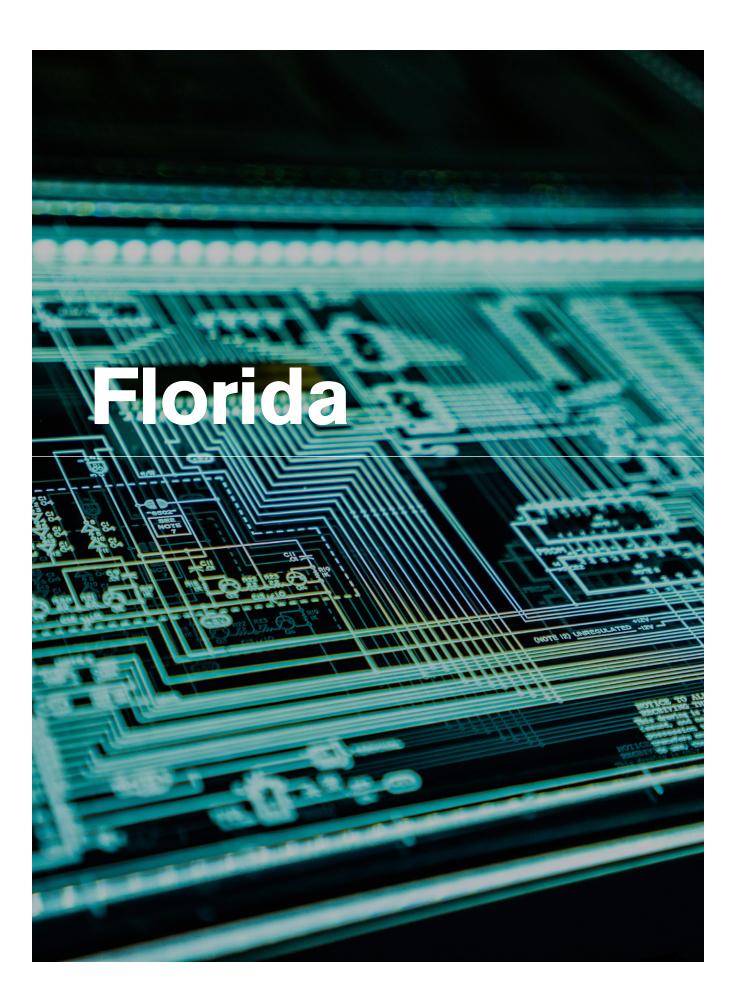
- i. Chancery Court
  - I. Smash Franchises Partners LLC and Smash My Trash LLC v. Kanda Holdings, Inc., et al., No. CV 2020-0302-JTL, 2020 WL 4692287 (Del. Ch. Aug. 13, 2020), modified, (Del. Ch. 2020), and vacated in part, (Del. Ch. 2020).
    - a. **Issue:** Whether information was adequately protected as a trade secret to prove a likelihood of success on the merits on a motion for preliminary injunction.
    - b. **Holding:** Because information was not adequately protected, it could not be classified as confidential or trade secret information as required to support a claim for misappropriation or unjust enrichment.
    - c. **Procedural Posture:** Motion for preliminary injunction.
    - d. **Factual Background:** Plaintiffs operated a mobile trash compaction business on a franchise model. Defendant expressed interest in operating a franchise. However, he soon concluded that he could be more successful if he simply created his own competing business. Despite reaching this conclusion, defendant continued to feign interest in a franchise so that he could gather information from Plaintiffs that would assist him in forming his own new venture.

Upon learning of the new business, plaintiffs moved for a preliminary injunction against defendant. However, the Court determined that the record did not support an injunction because there was no likelihood of success on the merits. All of the information that defendant received was publicly available, freely shared, or provided by Plaintiffs to defendant without taking adequate precautions to protect its confidentiality.

Plaintiff contended that Defendants received Confidential Information by participating in the initial calls about starting a franchise (Franchisee Forum Calls and Founder Calls). However, none of this information qualified as confidential. In particular, Plaintiffs provided information to anyone who expressed interest in operating a franchise, without requiring a signed non-disclosure agreement. Moreover, Plaintiffs invited potential franchisees to engage in video conferences with current franchisees, who were carved out of the scope of any applicable non-disclosure agreement. Finally, Plaintiffs failed to control who attended zoom meetings, and didn't use passwords, new meeting links, or take attendance.

Likewise, Plaintiff did not demonstrate a reasonable probability of success on a claim for unjust enrichment because the information that the defendants acquired was not confidential. It was information that Smash provided freely in its Disclosure Documents, its pitch deck, its introductory calls, and its Franchisee Forum Calls.

e. Takeaway: Although defendants in this case engaged in "disingenuous and underhanded" actions, this fact alone could not support an injunction against them. The burden remains on the trade secret owner to keep its information confidential and protect it appropriately. In an increasingly remote setting, such protections may require a creative mix of non-disclosure agreements, coupled with new technology, like password-protected video conference calls.



#### III. Florida

#### a. Federal Court

- i. District Court
  - I. *United States v. Smith*, 469 F. Supp. 3d 1249 (N.D. Fla. 2020)
    - a. **Issue:** Whether there was sufficient evidence to establish each element of a claim for theft of trade secrets pursuant to 18 U.S.C. § 1832? Specifically, did defendant have the intent to convert a trade secret to benefit someone beyond StrikeLines Pensacola, LLC and StrikeLines Tampa, LLC (together "StrikeLines") and did StrikeLines' fishing coordinates constitute a trade secret given defendant's argument that the coordinates are readily ascertainable?
    - b. Holding: Defendant's post-verdict motion for judgment of acquittal was denied.
    - c. **Procedural Posture:** Post-verdict motion for judgment of acquittal, or alternatively, motion for new trial pursuant to Federal Rules of Criminal Procedure 29 and 33. This case has since been appealed.
    - d. Relevant Background: StrikeLines sold coordinates for private artificial fishing reefs on its website for \$190-\$199. Each set of coordinates was sold only once to one customer and never again. In May 2018, StrikeLines received information that defendant had obtained the coordinates due to a "vulnerability" in its computer system. Defendant confirmed that he was able to and did retrieve the coordinates. Evidence showed defendant thereafter used, or intended to use, the coordinates himself and shared them with friends without permission. In June 2018, after StrikeLines increased its security measures, defendant admitted that he was still able to access the information but denied sharing it at that time. He offered to delete Facebook posts discussing the coordinates if StrikeLines gave him additional information about the coordinates. StrikeLines agreed and then defendant backed out of the deal. To prove defendant violated 8 U.S.C. § 1832(a)(1), the government had to prove: "(I) that the defendant intended to convert proprietary information to the economic benefit of anyone other than the owner; (2) that the proprietary information was a trade secret; (3) that the defendant knowingly stole [or appropriated, took, or carried away without authorization] trade secret information; (4) that the defendant intended or knew the offense would injure the owner of the trade secret; and (5) that the trade secret was included in a product that is placed in interstate commerce." As to the first element, and given the evidence showing defendant used, or intended to use, the fishing coordinates and gave them to several of his friends, the Court found there was sufficient evidence to show defendant intended to convert a trade secret. It also found StrikeLines' coordinates constituted trade secrets because a majority of the reefs were located only through using sonar equipment and were naturally occurring, which a reasonable juror could thus infer was not publicly available. Additionally, defendant, himself, referred to the locations as "private spots" and defendants conversations with his friends made it appear that the coordinates were not generally ascertainable. As to defendant's argument that StrikeLines did not take reasonable measures to secure its information, there was evidence showing a web developer secured the data on multiple occasions, and defendant admitted that the security used would "deter 99.9% of users." Lastly, as to the harm element, defendant's texts and Facebook messages showed that he was boasting about his access to the coordinates and offered them to friends despite knowing StrikeLines was trying to sell them.
    - e. **Takeaway:** Trade secrets are handled similarly in the civil and criminal contexts with regard to what constitutes a trade secret. Additionally, it is important to show that the holder of a trade secret(s) has taken reasonable measures to secure the secret in both civil and criminal cases.
  - 2. For Life Products, LLC v. Rust-Oleum Corp., 440 F.Supp.3d 1364 (S.D. Fla. 2020).
    - a. **Issue:** Whether a covenant not to compete is sufficient to establish personal jurisdiction under Florida's long-arm statute.
    - b. **Holding**: The Florida long-arm statute was insufficient to establish jurisdiction over defendant. Case transferred to Northern District of Illinois.
    - c. **Procedural Posture:** Motion to Dismiss for Lack of Subject Matter and Personal Jurisdiction and/ or Motion to Transfer Venue

- d. Relevant Background: The parties executed a license agreement to create a business partnership, which contained a covenant not to complete prohibiting the defendant from competing with Plaintiff's product line for three years. Plaintiff later filed suit against defendant, alleging that defendant was violating the covenant by distributing a competing product. Defendant moved to dismiss the case on the grounds that the covenant not to compete was insufficient to establish jurisdiction under the Florida long-arm statute. The court agreed, reasoning that the covenant did not require defendant to actually perform any specific act within Florida, and that contractual duties to merely perform for Florida residents are insufficient under the statute.
- e. **Takeaway:** Parties expecting to rely upon a state's long-arm statute to establish jurisdiction, which are often broadly construed and sometimes thought of as "catch-alls," must be aware of narrower interpretations as occurred here and should endeavor to include specific language in covenants, when possible.

#### b. State Court

- i. Court of Appeals
  - I. *Digiport, Inc. v. Foram Dev. BFC, LLC*, No. 3D18-1651, 2020 WL 7379128 (Fla. Dist. Ct. App. Dec. 16, 2020)
    - a. **Issue:** Whether: (i) a proposed data center design qualified for trade secret protection; (ii) trade secret misappropriation claim was preempted by misappropriation of a business idea claim brought under FUTSA; and (iii) plaintiff incurred actual damages resulting from defendant's alleged misappropriation.
    - b. **Holding:** The Court of Appeals held that a factual issue remained related to the FUTSA claim and affirmed the trial court's summary judgment of the remaining claims.
    - c. Procedural Posture: Appeal of Summary Judgment Rulings.
    - d. Relevant Factual Background: Digiport's alleged trade secret was its proposed design of a collocation center for computer hardware located inside Brickell Financial Centre, in which the building's tenants could rent space for their computer hardware, or use cloud computing and management services provided by Digiport. Digiport further contemplated offering other services, such as wiring the building for data and telecom and providing 24/7 on-site technical support. Digiport allegedly presented this proposal to Foram Group's agents in confidence, in 2008 when the building was under construction. After it acquired the technical information required to provide a specifically tailored proposal, it met with Foram Group's engineers to discuss the incorporation of the data center. The parties then explored the overall structure and design of the data center.

Ultimately, Foram Group's agents hired another company to design and install a data center in the building. The building is now connected to Terremark's Network Access Point of the Americas, and its tenants are being offered many of the services Digiport had offered to provide. Digiport sought to recover lost profits suffered as a result of the missed opportunity to earn what it estimated was up to \$18,000 revenue annually per tenant that may have contracted to use its data center, but for the alleged misappropriation. Foram Group argued (r) the proposal for the building was not a trade secret under FUTSA because it was based on overall, general design features of a colocation center, which were well-known in the data center provider industry prior to 2008 and (2) the concept at issue lacked the "genuine novelty" element required to prevail on a claim for misappropriation of an idea. While the Court of Appeals explained that a trade secret can exist in a unique compilation of public information, a question of fact remained regarding whether the compilation had independent economic value and offered a competitive advantage to competitors. The Court also held that to avoid preemption under the FUTSA, a claim for misappropriation of business ideas must contain material variations from the trade secrets claim.

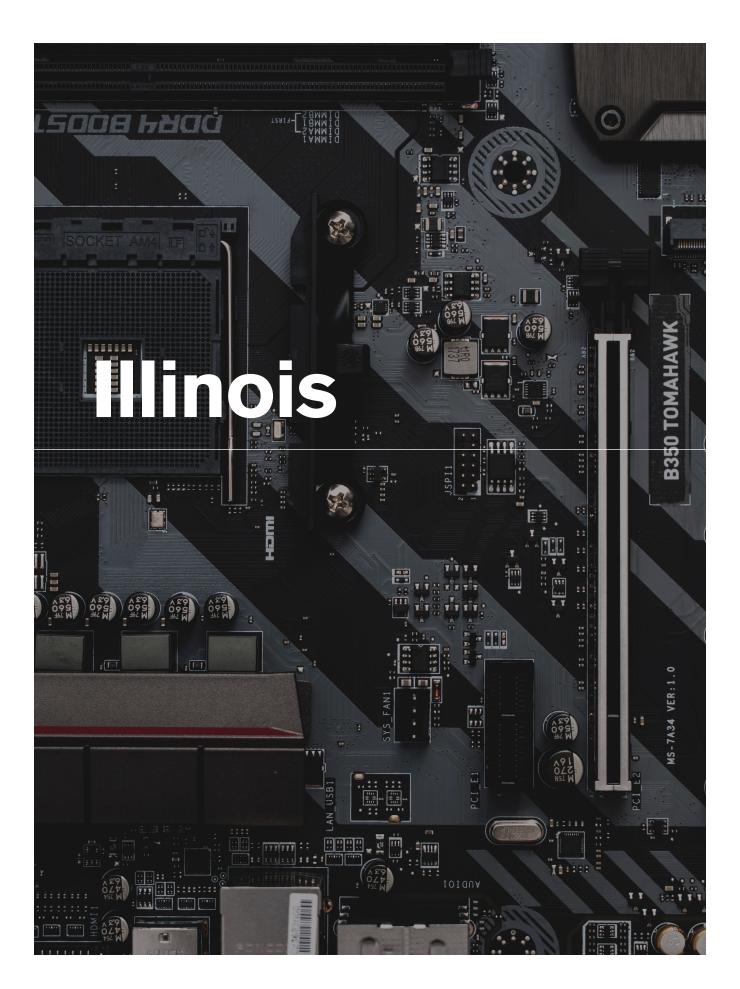
e. **Takeaway:** In order to prevail on an action for misappropriation of a compilation trade secret, a plaintiff must establish how the compilation meets the statutory definition of a trade secret.

```
port content="width=device-width, initial-scale=1 * magazinin-scale=2 *
        tcut icon" href="/favicon.ico" type='image/x-icon'>
          | href="/favicon.ico" type="image/x-icon"
  viesneet href="/css/animate ss | Constant ansammer | No. | N
                                                                                                                                         "stylesheet" href="css/materialize.min.css member
     tylesheet" href="css/theme.css">
href " class="brand-logo hide-on-med-and-up" class="brand-logo" class=
                                                                                                                                                                                                                                                                                                                                                                                  till network and merkspace that for huma
                                                                                                                                                                                                                                                                                                           oht: 400">starter()sparassam styles
                                                                                                                                                                                                                                 m8 18 hide-on-small-only'>
                                                     ss "container"
```

#### IV. Georgia

#### a. Federal Court

- i. District Court
  - I. Global Payments Inc. v. Green, Case No. 4:20-CV-185 (CDL), 2020 WL 5166041 (M.D. Ga. Aug. 31, 2020)
    - a. **Issue:** Whether a covenant not to compete, which geographically spanned four continents and effectively precluded defendant from employment, was reasonable in scope.
    - b. **Holding:** Covenant not to compete was reasonable in geographic scope, time, and restriction. Injunction granted.
    - c. **Procedural Posture:** Motion for Preliminary Injunction against defendant.
    - d. Relevant Background: Plaintiff is a global provider of certain payment technology services involving e-commerce, integrated payment systems, and other software, allowing merchants to accept electronic payments for commercial services across the world. Plaintiff operates services in North American, Europe, Latin America, and Asia. Defendant was a former vice president for plaintiff and was heavily involved in the company's international strategies. As part of employment, defendant entered into a covenant not to compete should his employment be terminated, which spanned "the geographic area in which [plaintiff] conducts business." Defendant was terminated due to company downsizing and three months later, began working for another company in the electronic payment market, which provided services in North American and Europe. Plaintiff moved to enjoin defendant from that employment under the covenant. Defendant argued that the covenant's geographic scope, spanning North America, Europe, Latin America, and Asia, was unreasonable because it would grossly limit his ability to obtain employment. The court disagreed, ruling that defendant's previous role in developing the company's international strategy rendered the area reasonable because his expertise was especially broad.
    - e. **Takeaway:** Employers and employees alike should be cognizant that the geographic scope of their businesses can potentially be construed as global and that courts may not hesitate to enforce such a multi-continent covenant.



#### V. Illinois

#### a. Federal Court

- i. 7th Circuit
  - I. Epic Systems Corp. v. Tata Consultancy Services, Ltd., Nos. 19-1528 & 19-1613 (7th Cir., Aug. 20, 2020)
    - a. **Issue:** Whether sufficient evidence was introduced to support jury's verdict award of \$140 million in "head start" damages.
    - b. **Holding:** A jury could award "head start" damages based on avoided research and development costs under an unjust enrichment theory.
    - c. Procedural Posture: On Appeal; Motion for Judgment as a Matter of Law (JMOL)/Directed Verdict
    - d. Factual Background: From 2012 to 2014, Tata Consultant Services ("TCS") unlawfully downloaded thousands of documents containing Epic Systems' ("Epic") confidential information and trade secrets. TCS used some of this information to enter the United States health record market and steal Epic's clients. Epic sued TCS, alleging that TCS unlawfully accessed and used Epic's confidential information and trade secrets. Epic sought unjust enrichment damages, and based this theory on a calculation of "the value TCS received by avoiding research and development costs they would have incurred without the stolen information." The jury then awarded \$140 million in compensatory damages, for the value of the "head start" obtained by TCS from the misappropriation.
    - e. **Takeaway:** Given the significant investments that companies make in research and development, the availability of substantial "head start" damages in trade secret cases can serve as a powerful deterrent to misappropriation. However, this deterrent is only available if companies carefully guard their trade secret information through the adoption of policies and procedures designed to protect the information from unauthorized acquisition, disclosure, or use.

#### ii. District Court

- I. *Motorola Sols., Inc. v. Hytera Commc'ns Corp.*, No. 1:17-CV-1973, 2020 WL 6554645 (N.D. Ill. Oct. 19, 2020)
  - a. **Issue:** Whether sufficient evidence existed to support jury verdict in favor of manufacturer on its claim for misappropriation of trade secrets.
  - b. **Holding:** Motorola provided sufficient facts to allow the misappropriation of trade secret question to go to the jury, and the jury was well informed of both party's arguments and found that it believed Hytera had concealed the theft. The legal instruction on this issue was correct, and Hytera failed to show that no reasonable jury could find for Motorola.
  - c. **Procedural Posture:** Motion for Judgment as a Matter of Law (JMOL)/Directed Verdict; Motion for New Trial: Motion for Remittitur.
  - d. Relevant Factual Background: Motorola developed technology to create certain specific digital radios. In June 2007, the president of Hytera, Chen, reached out to Motorola engineer G.S. Kok, who worked for Motorola in Malaysia. Hytera's president told Kok that he was looking to set up a potential research and development center for Hytera in Malaysia. Shortly thereafter, Chen and Kok negotiated Kok's departure from Motorola for Hytera. Hytera hired two additional Motorola Malaysia engineers. Evidence at trial showed that these two engineers downloaded more than 10,000 technical documents from Motorola's secure database and brought them to Hytera. At the time of trial, Motorola argued that more than 1,600 of those documents were still within Hytera's databases—among the files taken were Motorola's source code for the DMR radio project. Segments of Motorola's source code were also directly inserted into Hytera's product. Hytera developed a radio that was functionally indistinguishable from the DMR radio developed by Motorola. Motorola alleges that Hytera sold that radio for years and, continued selling the misappropriated trade secrets and infringing products to this day. After the jury was presented with detailed evidence regarding the trade secrets contained in the technical documents and the time and effort that went into developing that information, the jury returned a \$345 million verdict in favor of Motorola.

- e. **Takeaway:** It is important to present detailed evidence at trial regarding the information a plaintiff alleges to be trade secret and its value, especially if unjust enrichment/head start damages are sought.
- 2. *GCM Partners, LLC v. Hipaaline Ltd.*, Civ. No. 20 C 6401, 2020 WL 6867207 (N.D. Ill. Nov. 23, 2020)
  - a. **Issue:** Whether a party was entitled to preliminary injunctive relief for misappropriation of trade secrets under the Defend Trade Secrets Act where the party agreed to share its confidential information with another party pursuant to a written agreement.
  - b. **Holding:** A party cannot show misappropriation of trade secrets where it expressly agreed to share its confidential information with another party as part of a written agreement. Additionally, the failure to return or destroy confidential information does not constitute misappropriation standing alone, even where the party had a contractual obligation to do so, and temporary injunctive relief based on the party's failure to return or destroy confidential information is not appropriate absent evidence that the party would inevitably use or disclose the confidential information at issue.
  - c. Procedural Posture: GCM Partners, LLC ("GCM") sought a temporary restraining order to prevent Hipaaline Ltd. ("Hipaaline") and its Chief Executive Officer ("CEO"), defendants, from disabling or suspending GCM's access to its software platform and related confidential information and trade secrets, and replacing GCM's third-party payment processor with their own payment processor. GCM also sought a temporary restraining order requiring defendants to comply with the parties' agreement for GCM to use Hipaaline's Leafwell software platform for its telehealth services for medical cannabis patients. Once the parties agreed to a standstill arrangement pending the Court's decision, the Court converted GCM's motion for a temporary restraining order for a motion for preliminary injunctive relief.
  - d. Relevant Factual Background: GCM was founded by two partners, a pharmacist and a doctor of osteopathy, to expand their brick-and-mortar clinic providing treatment to medical cannabis patients in Illinois to serve patients in Maryland, Ohio, and Pennsylvania. GCM entered into an informal agreement with Hipaaline to operate telehealth clinics with medical cannabis programs, where Hipaaline agreed to provide GCM with marketing efforts and technological infrastructure through Hipaaline's Leafwell software platform. The Leafwell platform allowed prospective patients to submit the necessary documentation to obtain a medical cannabis card to be approved by a GCM medical provider through a virtual appointment. GCM's medical providers operated as independent contractors. If the patient was approved for a medical cannabis certification, GCM would charge the patient using its third-party payment processor, Bluepay. Pursuant to Leafwell's terms of service, users agree that any information submitted through the platform is provided on a non-proprietary and non-confidential basis, and patients grant Hipaaline a non-exclusive and perpetual license to use, modify, display, or publish any such information.

GCM and Hipaaline memorialized their business relationship in a written agreement approximately two years later. The agreement stated that it could be terminated by either party prior to the expiration of the five-year term only upon a material breach of the agreement by the other party. The agreement also stated that GCM and Hipaaline had an exclusive relationship whereby Hipaaline would be the sole provider of marketing and consulting services to GCM and only GCM providers would conduct appointments with patients through the Leafwell platform. To facilitate the agreement, Hipaaline provided GCM with a license to use the Leafwell platform and permitted GCM to use the Leafwell name for any legitimate business purpose during the term of the agreement. The agreement stated that all patient payments received through the Leafwell program would be solely collected by GCM, but that GCM would pay Hipaaline a fee per hour worked in exchange for the marketing services provided. GCM represented that it operated its clinics in compliance with all applicable laws regarding the practice of medicine.

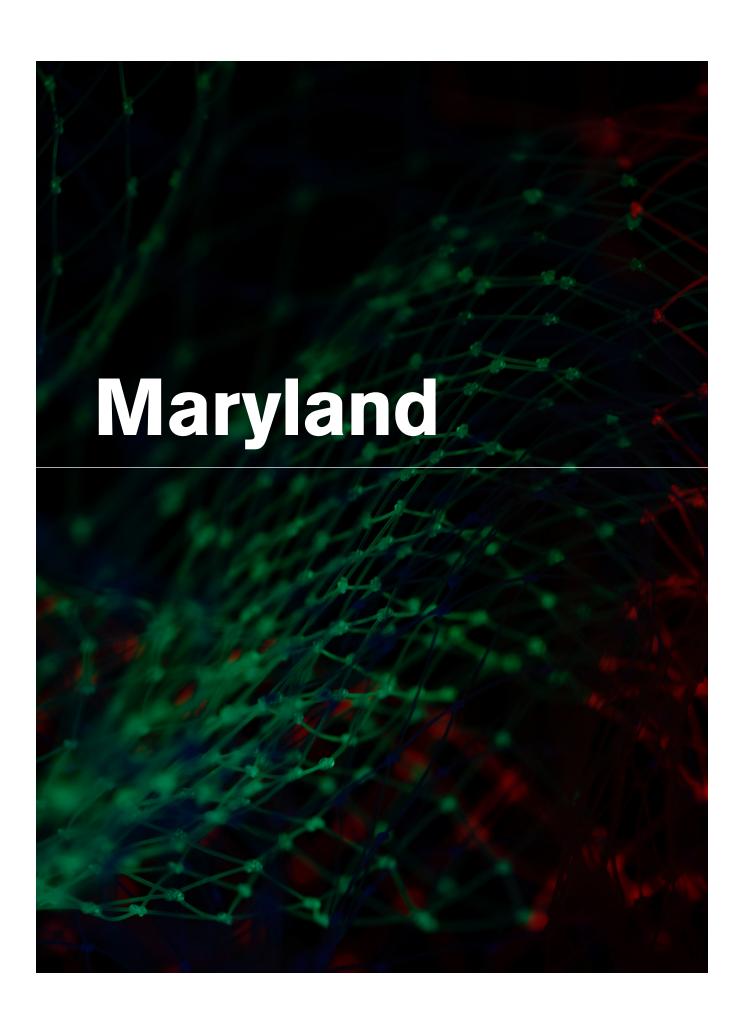
Approximately one year after execution of the agreement between GCM and Hipaaline, Hipaaline's CEO and one of GCM's founders arranged for one of GCM's independent contractor physicians to evaluate patients using both the Leafwell platform and another platform operated by a Hipaaline competitor. GCM, Hipaaline, and the physician shared the resulting fees in certain percentages they did not memorialize in a written agreement.

Several months later, Hipaaline's CEO sought to terminate the agreement with GCM, alleging that GCM had engaged in material breach of the agreement by engaging a direct competitor of Hipaaline to provide substantially similar services to those it agreed to provide Hipaaline on an exclusive basis, and violating corporate practice of medicine rules by improperly splitting fees with its independent contractor physician. GCM sought a temporary restraining order to block Hipaaline's anticipatory repudiation of the agreement by disabling GCM's access to the Leafwell platform and replacing GCM's payment processor with its own.

The court granted GCM's request for preliminary injunctive relief on the basis that Hipaaline had improperly engaged in anticipatory repudiation of its agreement with GCM. First, the court held that GCM did not breach the agreement's exclusivity provision by arranging for one of its independent contractor physicians to provide services on a competing software platform, given that Hipaaline's CEO had not only been aware of the arrangement, but facilitated it. Second, although the court found that GCM and its physicians had likely violated Illinois rules regarding the practice of medicine, the court held that this did not give Hipaaline a basis to anticipatorily repudiate the agreement because Hipaaline "entered into the Agreement with eyes wide open" and was in fact instrumental in developing GCM's operational model. Moreover, the court held that GCM's apparent violation of the rules governing the practice of medicine were curable, and that Hipaaline's efforts to terminate the agreement were a bad-faith effort to find a pretextual basis to get out of an agreement with which it was no longer happy.

Finally, the court rejected GCM's claim against Hipaaline for attempted misappropriation of GCM's trade secrets in violation of the federal Defend Trade Secrets Act. The court held that even if GCM's allegedly confidential information merited trade secret protection, it could not argue that Hipaaline had acquired it by improper means given that GCM specifically agreed to share its trade secrets with Hipaaline in their agreement. The court also rejected GCM's argument that Hipaaline engaged in misappropriation by failing to return or destroy GCM's allegedly confidential information, even though Hipaaline was required to do so pursuant to the agreement. Finally, the court held that temporary injunctive relief based on Hipaaline's failure to return or destroy GCM's information was not warranted because GCM failed to provide evidence that Hipaaline would inevitably use or disclose the information at issue.

e. **Takeaway:** Misappropriation under the Defend Trade Secrets Act does not occur where one party obtains the confidential information of another party pursuant to the terms of a contract between them. Further, where a party has a contractual obligation to return or destroy another party's confidential information, the failure to do so does not constitute misappropriation absent a showing that the party will inevitably use or disclose such information.



#### VI. Maryland

- a. Federal
  - i. Fourth Circuit
  - ii. District Court
    - I. Brightview Group, LP v. Teeters, 441 F.Supp.3d 115 (D.Md., 2020)
      - a. **Issue:** Whether information related to senior living homes be considered trade secrets?
      - b. **Holding:** Plaintiffs established likelihood of success on merits of claims for misappropriation of trade secrets under DTSA and MUTSA, as well as a likelihood of success on merits of unfair competition claim.
      - c. Procedural Posture: Motion for Preliminary Injunction
      - d. **Relevant Background:** Brightview is a developer and operator of approximately thirty senior living communities along the Mid-Atlantic coast. Carliner was the Executive Vice President of Brightview. Defendants Andrew Teeters and Ross Dingman were former Brightview employees. Teeter was the Senior Vice President for Development. In this position, Teeters oversaw the site selection and development of Brightview communities.

Teeters left Brightview at the end of July, 2019. The year prior to Teeters's departure from Brightview, Teeters led a year-long, internal interdisciplinary group focused on analyzing future development opportunities both within Brightview's current markets, and within new, undeveloped markets. The product of that effort was a presentation that compiled publicly-available census data, plus the locations of current and in-development Brightview communities, to identify viable submarkets. To do so, the intradisciplinary group established certain adult-child income and population density benchmarks, and applied those benchmarks to the relevant market areas. Carliner testified that while other companies likely perform similar demographic analyses, the benchmarks Brightview established were its own, developed through its years of experience.

At some point in 2018, Teeters and Dingman (while still employed with Brightview) began collaborating with Glynn on starting their own senior living venture. Throughout 2018, and into 2019, Teeters and Dingman made several efforts to attract investors to their new business.

Brightview claimed that its benchmarks are trade secrets. Those benchmarks are not disseminated outside of Brightview, and only 125 of Brightview's 4,300 employees have access to the underwritings. Brightview has also shown that the underwritings are highly valuable to competitors. If a competitor had access to the proprietary formulas and data compiled in Brightview's underwritings, the competitor could improve its own underwriting tool and better predict the financial success of potential senior living community sites. The competitor could also gain an inside view into Brightview's financials, enabling the competitor to outprice Brightview in a particular market.

Based on the value of this information to Brightview and to other competitors, and the reasonable security measures taken to ensure this information's secrecy, the court held that Brightview is likely to succeed in demonstrating that their cross-property operating reports are trade secrets. The court also held that Brightview is therefore likely to succeed in showing that Dingman misappropriated Brightview's cross-property operating reports by downloading them for future personal use, without any legitimate Brightview business purpose.

e. **Takeaway:** Demographic information and benchmarks related to senior living communities can constitute trade secrets supporting preliminary injunction.

```
port content="width=device-width, initial-scale=1 * magazinin-scale=2 *
tcut icon" href="/favicon.ico" type='image/x-icon'>
 | href="/favicon.ico" type="image/x-icon"
                stvlesheet" href="css/materialize.min.css" medi
Vesheet href="/css/animate.css" Chusetts
tylesheet" href="css/theme.css">
href. " class "brand-logo hide-on-med-and-up vell-sum implies the mediane
                                       till network and mericance has for fair
                               oht: 400">starter ( spar) com style
                       m8 18 hide-on-small-only'>
     ss *container*
```

#### VII. Massachusetts

#### a. Federal

- i. First Circuit
  - I. Russomano v. Novo Nordisk Inc., 960 F.3d 48 (1st Cir. 2020)
    - a. **Issue:** When does the non-compete restriction period begin to run for purposes of enforcement, where the employee was laid off and then re-hired into a new position but without a new non-compete.
    - b. **Holding:** The one-year non-compete period began to run on the effective termination date specified in the company's letter to employee eliminating his position, regardless of the fact that the company subsequently re-hired him.
    - c. **Procedural Posture:** Appeal of denial of preliminary injunction.
    - d. **Relevant Background:** Novo Nordisk Inc., a pharmaceuticals company, sought to enforce the terms of a confidentiality and non-compete agreement signed by a former employee, Russomano.

The lower court denied the motion for preliminary injunction because it found Novo Nordisk did not show a likelihood of success on the merits. In particular, the court found that the one-year noncompete expired before the employee started work for his new employer. Russomano had been laid off in 2018 by a letter that specified an August 5, 2018 termination date, and encouraged him to apply for open positions. Russomano did apply to open positions and was rehired into a different role starting August 6, 2018. He was not required to sign a new non-compete. Russomano resigned from the new role in January 2020, and began work for a new employer shortly thereafter.

Novo Nordisk argued that Russomano was not laid off, but was instead transferred to a new role beginning the Monday after his termination date the Friday before.

In affirming the lower court's decision, the First Circuit noted that the language in the termination letter was unambiguous – Russomano's employment in the role to which the non-compete was subject ended. As such, the non-compete restriction began to run on the date employment in that role terminated.

- e. **Takeaway:** Employers should take care to ensure that changes in employment status are correctly characterized. If any question exists, best practice is to have employees sign new agreements or acknowledge the continuing nature of existing agreements.
- 2. TLS Mgmt. & Mktg. Servs., LLC v. Rodriguez-Toledo, 966 F.3d 46 (1st Cir. 2020)
  - a. **Issue:** Whether TLS established trade secrets for the purpose of its misappropriation claim, and whether the non-disclosure agreement (NDA) was too broad to be enforced.
  - b. **Holding:** TLS failed to satisfy its burden of proving that capital preservation reports and tax advice strategies constituted trade secrets, and the NDA was overbroad and unenforceable as a matter of public policy.
  - c. **Procedural Posture:** Appeal of summary judgment on the NDA claim, and appeal of a bench trial verdict on the misappropriation claim.
  - d. Relevant Background: TLS was a tax planning and consulting firm based in Puerto Rico that provided clients with advice to enable them to minimize tax liabilities in Puerto Rico and the United States. Rodriguez was the founder of ASG, a subcontractor for TLS, and also worked as the Managing Director for TLS. In connection with his role as a subcontractor and as managing director, he signed two NDAs. Rodriguez and ASG's relationship with TLS terminated in 2015, after which time Rodriguez began providing tax services in competition with TLS. TLS argues that Rodriguez misappropriated TLS trade secrets in the provision of those tax services, in violation of the NDAs.

Two alleged trade secrets were at issue. The first was a capital preservation report ("CPR"), which provided tax recommendations specific to each client based on an analysis of tax statutes and regulations. TLS argued that the portion of the report not specific to an individual client was a trade secret. The second was a tax arbitrage strategy by which TLS took advantage of lower tax rates in Puerto Rico to shield clients from higher tax rates in the US.

The lower court granted summary judgement to TLS on the breach of contract claims, finding that Rodriguez had waived his arguments regarding the unenforceability of the

agreements. It held a non-jury trial and found that Rodriguez had misappropriated the capital preservation report and the tax arbitration strategy belonging to TLS.

On appeal, Rodrigues argued that TLS had failed to establish that it had trade secrets. In addressing this argument, the First Circuit noted that trade secrets, unlike other forms of intellectual property, do not have a requirement of registration and, by definition, there is no public knowledge of the trade secret in advance of litigation. As a result, there is a possibility that a trade secret owner could tailor the scope of the trade secret to conform to litigation strategy. Here, TLS did not disclose the alleged trade secrets until the eve of trial, and neither truly qualifies as a trade secret under the statutory definition provided by the Puerto Rico Trade Secret Act.

In particular, the First Circuit found that the capital preservation report did not qualify as a trade secret because TLS could not articulate which aspects of the report in particular were trade secrets. Rather, TLS referred to the report generally. Moreover, TLS did not separate the purported trade secrets from the other information that was generally known in the trade. Next, the tax arbitrage strategy did not qualify as a trade secret because to a large extent, it consisted of public knowledge. Indeed, TLS's principals testified that components of the strategy were standard and common. Although TLS attempted to argue that one portion of the strategy – the use of promissory notes and security agreements to enable client to access distributed profits – was not publicly known, they did not establish that it was not readily ascertainable from public sources. As such, they failed to establish that trade secret protection applied.

The First Circuit further determined that the defendant's had not waived their unenforceability argument as to the NDAs, and held that the NDAs were in fact unenforceable as a matter of public policy. Relying on precedential case law regarding non-compete agreements, the court noted that overly broad nondisclosure agreements, while not specifically prohibiting an employee from entering into competition with the former employer, raise the same policy concerns about restraining competition as non-compete clauses when they have the effect of preventing the defendant from competing with the plaintiff. A non-disclosure agreement may be overly broad if it restricts the use of general knowledge acquired by an employee, if it prohibits disclosure of information that is not actually confidential because it is public knowledge, or if it extends to information properly provided to the defendant by third party sources. The First Circuit determined that all of these factors existed in the NDAs at issue. As a result of this over breadth, the NDAs were held to be void as against public policy.

e. **Takeaway:** To qualify for protection, a company must be able to articulate with specificity the trade secrets at issue and distinguish them from information generally known in an industry or readily ascertainable from public sources. Moreover, non-disclosure agreements that have the effect of preventing competition will be examined under non-compete standards and as such they (like non-competes) should be narrowly drafted to protect only that information that is truly confidential.

#### ii. District Court

- I. Neural Magic v. Facebook, No. 1:20-cv-1044-DJC, Memorandum and Order, at 9 (D. Mass, May 29, 2020) (Casper, J.).
  - a. **Issue:** Whether the recently enacted Massachusetts Uniform Trade Secrets Act (MUTSA) preempts claims based on confidential or proprietary information that does not necessarily rise to the level of a trade secret.
  - b. **Holding:** Relying on the text of the MUTSA, the legislative history, and the guidance of courts in other jurisdictions that had considered the issue in the context of the Uniform Trade Secrets Act, the Court held that the MUTSA did not, in fact, preempt such claims.
  - c. Procedural Posture: Motion to dismiss.
  - d. **Factual Background:** Neural Magic, a deep learning company, filed suit against Facebook and Dr. Aleksandar Zlateski, a former Neural Magic employee, asserting claims for misappropriation of trade secrets under the MUTSA and the Defend Trade Secrets Act, unfair competition, unjust enrichment, tortious interference and other state law claims.

Defendants argued that the MUTSA was adopted after years of interpretation of the UTSA in other states, and that the majority position at the time of adoption was that the preemption provision displaces any claim regarding theft or misuse of confidential proprietary, or otherwise secret information falling short of trade secret. The Court, however, was not swayed by this argument, noting that where a split

in authority exists at the time of adoption, it cannot be presumed that the legislature intended to incorporate one position over another in adopting similar language. If the legislature had in fact intended to preempt certain causes of action, they would have explicitly done so in the language of the statute.

Ultimately, the Court held "Given that the MUTSA is silent about uniformity with respect to confidential information that may not constitute a trade secret, the text of Section 42F which limits preemption to civil remedies for the misappropriation of trade secrets, the split in authority on the scope of preemption of similar UTSA provisions and the lack of authority in Massachusetts, the Court does not conclude that MUTSA preemption applies to the state law claims that Defendants now challenge where these claims rely upon the alleged the theft of alleged confidential and information." The Court did grant Defendants' motion to dismiss the unjust enrichment claim on the grounds that Neural Magic had an adequate remedy at law.

- e. **Takeaway:** The decision preserves for the time being additional avenues in Massachusetts for the protection of confidential and proprietary information. Perhaps most critically, claims for unfair competition under Massachusetts Chapter 93A may be pursued when appropriate, opening the door for treble damages and attorneys' fees.
- 2. United States v. Haoyang Yu, No. CR 19-10195-WGY, 2020 WL 5995212 (D. Mass. Oct. 9, 2020)
  - a. **Issue:** Whether defendant facing criminal trade secret theft charges may suppress evidence collected by a former employer on the grounds that its collection represented an unreasonable, warrantless search.
  - b. **Holding:** Defendant had no reasonable expectation of privacy in information recovered by former employer, and, therefore, the motion to suppress is denied.
  - c. Procedural Posture: Motion to suppress.
  - d. **Factual Background:** Defendants Haoyang Yu faces 24 criminal charges stemming from an alleged scheme whereby he downloaded and stole proprietary information from his thenemployer, Analog Devices, Inc., for the purposes of setting up a rival company in China.

Yu moved to suppress information recovered by Analog on behalf of the Government. The information was recovered by analyzing Analog's own internal records of Yu's computer usage.

The Court found that Yu had no right to privacy in the information reviewed by Analog because it consisted only of names and access times of various files, and because the information belonged to Analog, not to Yu. The information related to Analog-owned devices and documents, and did not encompass Yu's personal information.

Moreover, Analog had a "Technology Resource Policy" in place that warned employees that they had no expectation of privacy on Analog devices and that Analog could search and inspect the devices at any time.

- e. **Takeaway:** Employees do not have a constitutional right to privacy for activity on employer-owned devices, especially when applicable policies alert them to this fact. As such, information recovered by employers may be used to support criminal trade secret charges where appropriate.
- 3. FabriClear, LLC v. Harvest Direct, LLC, No. CV 20-10580-TSH, 2020 WL 4938340 (D. Mass. Aug. 24, 2020)
  - a. **Issue:** Whether the formula of a product qualifies as a trade secret, where the ingredients are included in the trademark application.
  - b. **Holding:** Where a product's trademark application discloses the ingredients but not the composition of those ingredients, the product formula is not public knowledge and the application does not destroy trade secret status.
  - c. Procedural Posture: Motion to dismiss (denied).
  - d. Relevant Background: FabriClear produces and sells a spray to treat bedbug infestations. In 2013, FabriClear and Harvest Direct, an "As Seen on TV" marketing and sales company, entered into a Confidentiality Agreement pursuant to which, among other things, Harvest Direct agreed that the FabriClear product formula was a trade secret and that Harvest Direct could not reproduce, use, alter or modify it without FabriClear's written permission. The parties then exchanged information about the product, and entered into separate License Agreement, pursuant to which Harvest Direct was granted an exclusive license to market and sell the product and to use FabriClear's trade secrets and other confidential information in exchange for the payment of royalties to FabriClear.

Sales were robust, but suddenly declined in 2018. FabriClear soon learned that Harvest Direct had begun marketing and selling its own competing product in order to avoid making royalty payments to FabriClear. The products are essentially indistinguishable, and evidence demonstrates that Harvest Direct actually repackaged existing bottles of FabriClear product under their own label.

FabriClear filed suit raising claims for breach of the License Agreement, breach of the Confidentiality Agreement, misappropriation of trade secrets, unjust enrichment, breach of the implied covenant of good faith and fair dealing, Lanham Act violations, and state unfair competition claims. Harvest Direct moved to dismiss.

As to the trade secret claim, Harvest Direct argued that the misappropriation claim fails as a matter of law because FabriClear had not demonstrated that the disclosed information qualifies as a trade secret. In particular, Harvest Direct argued that the formula for the product cannot qualify as a trade secret because it is a matter of public knowledge due to the disclosure of its ingredients in its trademark application. However, the Court noted that while FabriClear published the ingredients for the formula in its trademark application, it did not disclose the composition of those ingredients. As a result, the court denied Harvest Direct's motion to dismiss the misappropriation of trade secrets claim.

e. **Takeaway:** Careful protection of trade secret information, both in the trademark application process and in the context of a licensing relationship in which the information will necessarily be exchanged, is critical to ensure continued protection.

#### b. State Court

- I. Automile Holdings, LLC v. McGovern, 483 Mass. 797, 136 N.E.3d 1207 (2020)
  - a. **Issue:** Whether the duration of an anti-raiding provision should be extended, where monetary damages are available.
  - b. **Holding:** Although anti-raiding provision was enforceable, trial court abused its discretion by extending the restriction for an additional year where the plaintiff had not yet attempted to calculate monetary damages.
  - c. **Procedural Posture:** Appeal of motion for preliminary injunction.
  - d. **Relevant Background:** McGovern was the Chief Financial Officer and Vice President of Operations with a minority share ownership of a closely held corporation, Prime Motor Group. In 2016, his employment was terminated as a result of disagreements with the majority shareholders with respect to the potential sale of the company. In late 2016, as the result of significant financial pressure placed on McGovern, he sold his interest in the company. In connection with the sale, McGovern entered into an 18-month restrictive covenant, pursuant to which he agreed not to solicit Prime's employees or consultants.

Meanwhile, McGovern started his own competing automotive group, McGovern Motors. Despite the restrictive covenant, he hired at least fifteen former Prime employees to work at McGovern Motors. In February 2017, the parties entered into a new agreement "in order to avoid the cost of litigation relating to this dispute." As part of the 2017 agreement, McGovern agreed to enter into a more robust restrictive covenant that would end in August 2018. Unlike the 2016 agreement, the 2017 agreement did not include an exception for the general solicitation of employees. Nevertheless, McGovern went on to solicit and hire still more Prime employees.

In August 2017, Prime brought suit against McGovern and sought a preliminary injunction to enjoin him from continuing to employee one of Prime's former employees. The court did not grant the injunction, noting that there could be no legitimate business interest in prohibiting the solicitation of an employee that Prime had chosen to fire. Despite the court's warning that the same could not be said for current Prime employee, McGovern hired three other then-current Prime employees. Prime once again sought a preliminary injunction which would enjoin McGovern from continuing to employee Prime employees and would extend the restrictive covenant for an additional 18 months.

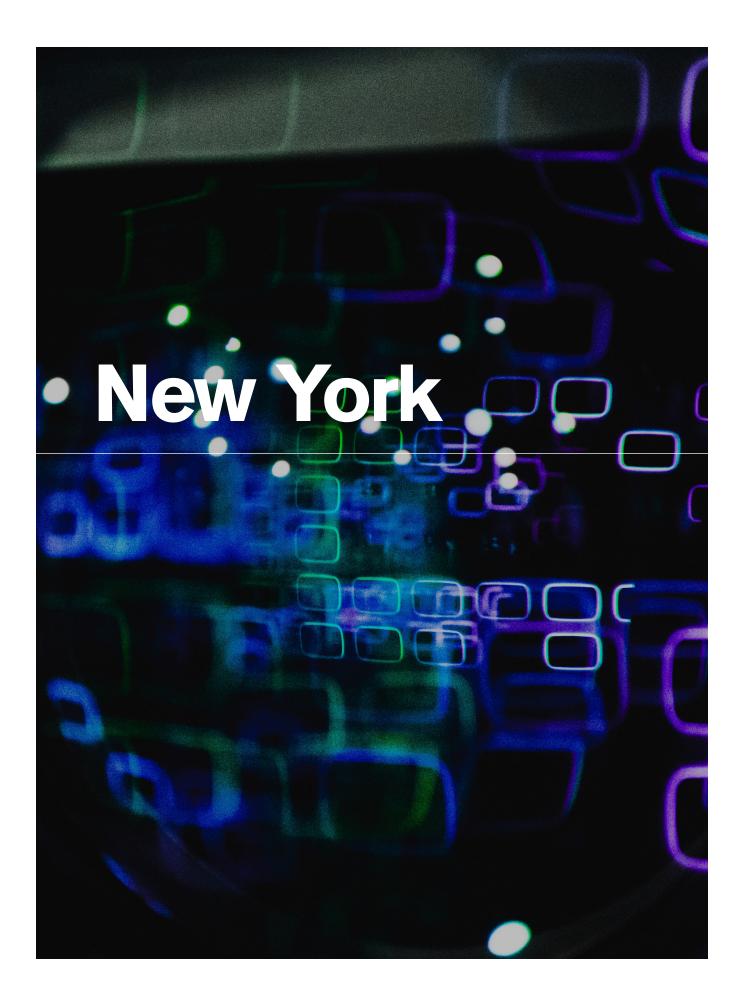
The lower court granted the preliminary injunction in part, enjoining McGovern from soliciting or hiring former Prime employees until further order of the court. The judge also scheduled a jury-waived trial for two months before the restrictive covenant was set to expire. At that time, the judge found that McGovern had breached the agreement by soliciting the three employees, but did not enjoin their employment. Rather, he extended the length of the restrictive covenant by one year beyond its expiration under the agreement. Because the trial was limited to the equitable claims, the judge did not make any findings as to damages.

McGovern appealed the decision to the First Circuit Court of Appeals, arguing that the restrictive covenant contained in the 2017 agreement did not serve a legitimate business interest, and that either the judge lacked the authority to extend the duration of the restrictive covenant or the extension was improper without a showing regarding the inadequacy of damages.

The Court of Appeals determined that the restrictive covenant should be analyzed as arising out of the sale of business context given that it was an integral part of the sale of McGovern's minority interest, the parties did not have the unequal bargaining position typical of the employer-employee relationship, and were both represented by counsel. In the sale of business context, restrictive covenants are not rendered unenforceable merely because they protect an interest not recognized in the employment setting – here, an interest in anti-raiding. In light of McGovern's prior position within Prime, his current role as a competitor to Prime, and the additional consideration he received in exchange for the covenant, the Court found the anti-raiding provision to be based in a legitimate business interest and as such enforceable.

Turning next to the decision by the lower court to extend the term of the restriction, the Court of Appeals determined that, on the record of the case before it, the extension was not warranted. In the sale of business context, an extension of the restrictive covenant may be proper, but only if the party seeking the extension has demonstrated that monetary damages would prove inadequate. On the record before the Court of Appeals, there was no evidence that monetary damages would be either impossible to calculate or inadequate. As a result, the Court reversed the lower court's extension of the restrictive covenant.

e. **Takeaway:** Anti-raiding provisions will be more liberally enforced in the sale of business context; however, to secure an extension of any restriction, the party seeking extension must be prepared to demonstrate the insufficiency of monetary damages.



#### VIII. New York

#### a. Federal

- i. Second Circuit
  - I. Broker Genius Inc. v. Gainor, 810 F. App'x 27 (2d Cir. 2020) (unpublished summary order)
    - a. **Issue:** Whether information learned while a customer of a company pursuant to a Terms of Use agreement can form the basis for a misappropriation claim.
    - b. **Holding:** Jury verdict and damages in favor of plaintiff Broker Genius on breach of contract and misappropriation claims in the amount of \$4.5 million, as well as permanent injunction against competitor, were upheld. NY law of unfair competition includes misappropriation for the commercial advantage of one person a benefit or property right belonging to another.
    - c. **Procedural Posture:** Appeal from trial verdict and permanent injunction.
    - d. **Relevant Background:** Broker Genius, a technology company serving ticket brokers on the secondary market, brought claims against Drew Gainor and Seat Scouts LLC, a competing website and its founder, for breach of contract and misappropriation of proprietary information. Broker Genius alleged that Gainor used knowledge obtained while he was a customer of Broker Genius to develop a competing product, in violation of the Broker Genius Terms of Use.

Broker Genius originally sought and obtained a preliminary injunction, enjoining Defendant from using or making available the competing product. However, the same day the injunction went into effect, Defendants debuted a new product with substantially the same functionality as the enjoined product. The district court held Defendants in contempt, finding that the products were essentially one and the same and that Defendant sought to circumvent the injunction. A jury trial resulted in a verdict in favor of Broker Genius and a permanent injunction against Defendants, who promptly appealed.

Defendants argued that the lower court erred in interpreting the use of "derivative works" in the Terms of Use as falling outside the framework of copyright law. However, the Second Circuit Court of Appeals found that the additional provision prohibiting defendants from "attempting to derive any source code or underlying ideas or algorithms of any part of the Site or Apps" expanded the scope such that the Copyright Act did not serve as a limitation to the claim. Rather, the claims should be analyzed under normal contract principles without reference to the Copyright Act.

Defendants also argued that the misappropriation claim was preempted by the Copyright Act; however, because defendants did not raise the defense until a month before trial and over a year after the commencement of the action –the argument was waived.

Finally, defendants argued that the lower court erred in finding them in contempt of the preliminary injunction. However, the Court found that the injunction was clear and unambiguous, that evidence of the Defendants' non-compliance was clear and convincing, since they released an identical product in an attempt to circumvent the injunction, and that their requests for clarification were disingenuous. The contempt ruling was therefore upheld.

Finally, Defendants argued that the district court erred in issuing a permanent injunction because the jury's damages award incorporated future damages. The Court noted that Broker Genius had suffered a loss of goodwill and damage to its reputation that could not be compensated through monetary damages alone, and that Defendants had demonstrated through their past conduct that they would continue to offer derivative products in the absence of an injunction. The permanent injunction was therefore upheld.

e. **Takeaway:** The use of language from the Copyright Act in a website's Terms of Use does not limit construction to copyright principles. Moreover, attempts to circumvent a preliminary injunction through a technicality may result in findings of contempt, damages, and the imposition of a permanent injunction.

#### ii. District Court

I. *Trahan v. Lazar*, 457 F.Supp.3d 323 (S.D.N.Y. 2020)

- a. **Issue:** Whether IP developed at a business belongs to the entity and whether the IP owner can seek misappropriation of trade secrets for failure to turn over previously developed IP.
- b. **Holding:** Plaintiff adequately alleged misappropriation for the trade secrets developed prior to his affiliation with the Defendants because their continued use of the trade secrets was without consent; Plaintiff did not adequately allege misappropriation for the trade secrets developed during his affiliation with Defendants because Defendants' owned the IP at issue.
- c. Procedural Posture: Motion to Dismiss
- d. Relevant Factual Background: Francois Trahan, Plaintiff is a successful portfolio strategist. In 2016, he joined with three partners—Nancy Lazar, Andrew Laperriere and Robert Perli to create a new firm, Cornerstone Macro. The Partnership was organized into three distinct divisions which were run separately by at least one of the Partners. Trahan ran the Market Strategies Advisory Business, Lazar ran the Economic Advisory Business, while Perli and Laperriere jointly ran the Policy Advisory Business. In drafting the Limited Partnership Agreement, the Partners sought to ensure that any Partner could take his or her business with them should they leave the Partnership. Thus, the Agreement provided that "the Leaving Partner was entitled to have assigned him or her upon his or her departure any intellectual property belonging to the Partnership and used solely by his or her division."

On August 3, 2018, Trahan was informed he was being removed from the partnership. Upon notice, Trahan demanded that Cornerstone Macro return his intellectual property. refused.

Defendants allegedly maintained copies of Trahan's intellectual property on Cornerstone Macro servers, on local drives of certain Cornerstone Macro employees, on Cornerstone Macro's data provider, and on Defendant's "own personal servers in their private residences." Defendants allegedly "copied and pasted" information from electronic pages of Trahan intellectual property, and printed out or took photographs of the code to aid them in re-creating the intellectual property without leaving a digital footprint.

The Court held that Trahan had adequately pled a DTSA claim with respect to the intellectual property he brought with him to Cornerstone Macro. In so holding, the Court recognized that a DTSA misappropriation claim can exist where – as here – the trade secrets were not obtained by improper means, but rather were in use without consent under circumstances that may give rise to a duty to limit use. The Court held that Trahan had not, however, stated a claim with respect to the IP developed while he was at Cornerstone. Toward that end, Trahan conceded that the IP developed while at Cornerstone was owned by the Cornerstone Partnership. Because the Partnership was still the legal owner of the Cornerstone IP, it could not have misappropriated the Cornerstone IP because misappropriation requires the trade secret at issue to be the "trade secret of another." 18 U.S.C. § 1839(5).

- e. **Takeaway:** Exercise care in addressing IP rights, including ownership and continued use, when drafting executive and partnership agreements paying particular attention to contingencies for termination or the relationship or partnership.
- 2. *Zirvi v. Flatley*, 433 F.Supp.3d 448 (S.D.N.Y. 2020)
  - a. **Issue:** Whether equitable tolling be applied to the DTSA statute of limitations for the claims at issue; and does DTSA apply to acts that occurred before its enactment?
  - b. **Holding:** Equitable tolling does not apply because the date on which the alleged misappropriation should have been discovered "by the exercise of reasonable diligence" had long past given Defendants' USPTO applications, and the Plaintiffs' allegations of fraudulent concealment fail because the facts alleged confirm notice. Moreover, Plaintiffs' DTSA claim fails because they did not allege because post-enactment activity, and the DTSA does not have retroactive application.
  - c. **Procedural Posture:** Motion to Dismiss for Lack of Subject Matter Jurisdiction; Motion to Dismiss for Failure to State a Claim.
  - d. **Relevant Factual Background:** The plaintiffs' claims, arise out of two alleged instances of misappropriation of trade secrets, one occurring in 1994 when certain trade secrets were allegedly stolen from a confidential grant proposal, and one occurring in 1999 when alleged trade secrets

were allegedly misappropriated during confidential communications. The plaintiffs allege that these two acts of misappropriation resulted in the theft of both positive and negative trade secrets.

The first alleged instance of misappropriation occurred on or around June 1, 1994 when Stephen Fodor, the Chief Technology Officer of the biotechnology company Affymetrix, in his capacity as a peer reviewer for the National Institute of Health ("NIH"), reviewed the Barany proposal. According to the plaintiffs, upon reviewing the grant proposal, Fodor "immediately resolved to steal those ideas" contained in the grant proposal in violation of confidentiality agreements that he was bound to obey in his capacity as an NIH reviewer.

The second alleged instance of misappropriation occurred in 1999 after Zirvi, then a medical student at Cornell working with Barany, developed 187 files of Microsoft Excel and Word documents containing, among other things, the design of 4,633 zip codes including an alleged proprietary set of 465 zip codes.

The plaintiffs allege that the misappropriation included both negative and positive trade secrets, defining negative trade secrets as negative experimental results that are crucial to the ultimate invention and success of the trade secret.

To overcome statute of limitations issues, plaintiffs alleged they only discovered the conspiracy in 2015, and as such the action filed on August 3, 2018 is timely because the statutes of limitations should be equitably tolled until the discovery of the alleged conspiracy. The court stated that the timeline of events undermined any argument that the plaintiffs acted with reasonable due diligence in investigating, as a matter of law, and pointed specifically to information in Defendant's USPO applications. The court dismissed the claims with prejudice, as no amended complaint could cure these deficiencies.

In addition, the court stated that the DTSA claims failed because plaintiffs did not allege post-enactment conduct and affirmatively held that the DTSA does not have retroactive application. Moreover, the court stated that the plaintiffs failed to allege that the 187 files containing the 465-zip code set are a trade secret. Although the plaintiffs described these alleged trade secrets with sufficient particularity, the plaintiffs have failed to allege how this zip code set derives independent economic value from not being publicly known given the quantity of similar zip code sets publicly available.

e. Takeaway: Developers of intellectual property must exercise reasonable investigative diligence in protecting against theft, including investigation of submissions to the USPO. While courts will entertain tolling arguments, and fraudulent concealment arguments, as to the statute of limitations, those arguments may not succeed where the party knew or should have known through diligent investigation that misappropriation occurred.

#### b. State Court

- i. Appellate Court
  - I. Hyperlync Technologies, Inc. v. Verizon Sourcing LLC, 2020 WL 2951291 (N.Y.A.D. 1 Dept., June 04, 2020)
    - a. **Issue:** Whether speed and functionality ideas for an app merit protection; and whether the plaintiff can establish the ideas as confidential if shared publicly and with requests for confidential treatment, but without agreement for confidential treatment?
    - b. **Holding:** The ideas underlying plaintiffs' phone application were not confidential or sufficiently novel to merit protection.
    - c. Procedural Posture: Appeal; MSJ
    - d. **Relevant Factual Background:** Plaintiffs allege that, in breach of a nondisclosure agreement, defendant Verizon Sourcing, LLC disclosed confidential information about a peer-to-peer phone provisioning application to plaintiff's competitor, which then released its own phone provisioning app allegedly based on the misappropriated information.

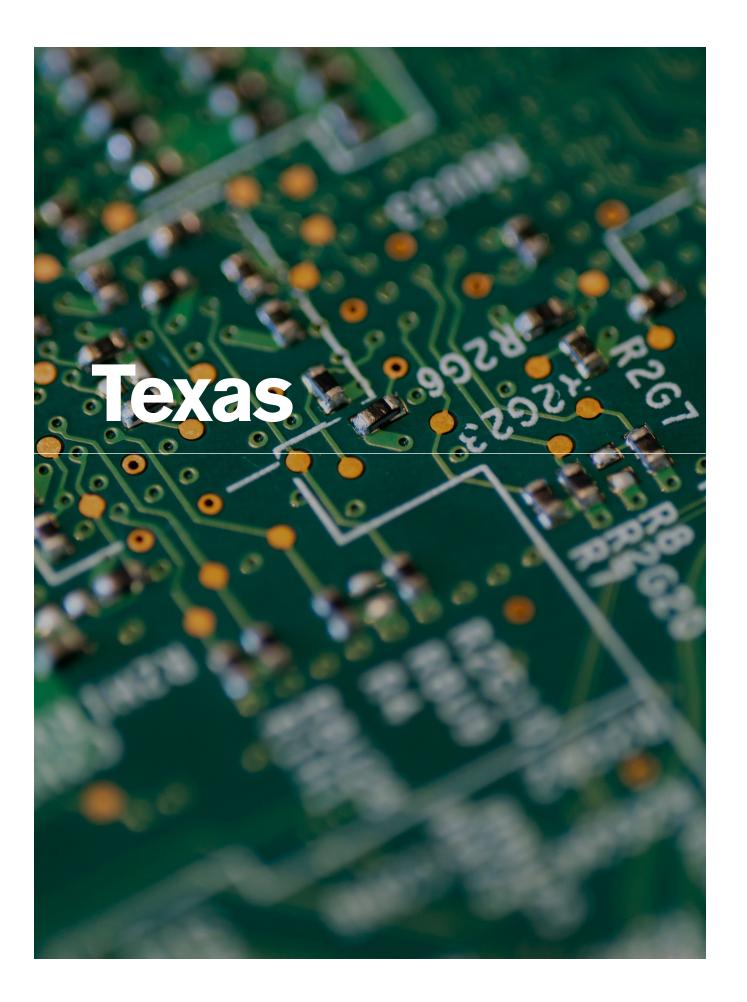
Plaintiffs argued that their app was an improvement in speed and functionality over the apps that existed in 2013. The court held, however, that a smart adaptation of existing knowledge is not novel enough to merit protection. The concepts behind plaintiffs' app were not new, were readily

available in the public domain, and were used by a number of other apps on the market at the time.

The court further held that the ideas were not confidential. Beginning in May 2013, before the alleged misappropriation, plaintiffs posted the app's demo videos on YouTube and shared those videos with companies with which it did not have nondisclosure agreements. Plaintiffs' argument that the materials were promotional and did not contain confidential information, the court stated, is belied by their own emails in which they requested assurances of confidentiality. The court stated that Plaintiffs' subjective understanding that there was an assurance of confidentiality does not create third-party obligations of confidentiality.

Plaintiffs also failed to establish that Verizon actually conveyed its ideas to Synchronoss. Plaintiffs did not share the app's source code, and they encrypted its builds, making the source code inaccessible to Verizon.

- e. **Takeaway:** Parties should exercise caution in securing the confidential treatment of proprietary information.
- 2. *Photonics Indus. Int'l, Inc. v. Xiaojie Zhao*, 185 A.D.3d 1064, 127 N.Y.S.3d 568 (2020)
  - a. **Issue:** Whether customer lists and other proprietary information qualified for trade secret protection.
  - b. **Holding:** Plaintiff sufficiently articulated certain trade secret information that had been misappropriated, but did not meet its burden with respect to other information.
  - c. **Procedural Posture:** Appeal of order compelling additional discovery and granting motions for summary judgment.
  - d. Relevant Background: The plaintiff Photonics Industries International, Inc. ("Photonics"), a laser manufacturing and development company, entered into an employment agreement with the defendant, Xiaojie Zhao. When Zhao's employment with Photonics ended, he began working at Yuco Optics, a newly formed laser manufacturing company. Photonics initiated suit against Zhao and others, alleging misappropriation of trade secrets, breach of non-compete, and common-law unfair competition.
    - The misappropriation claim related to both the manufacture of lasers and to customer identification and lists. The Supreme Court upheld the dismissal of the claim to the extent it related to customer lists, noting that the list was not proprietary information since it could be obtained with little effort from non-confidential sources. However, to the extent the claim related to the manufacture of lasers, the claim should survive since plaintiff raised triable issues of fact as to whether Zhao used its trade secrets in the manufacture of particular lasers. Indeed, Photonics submitted an expert affidavit opining that Zhao could not have developed the particular lasers within three months without use of the Photonic's confidential information.
  - e. **Takeaway:** A claim for trade secret misappropriation may fail if information, such as a customer list, is readily available in the public domain. However, the failure to plead one type of trade secret does not doom the claim as a whole if some other, separate trade secret can be articulated.



#### IX. Texas

#### a. Federal

- i. Fifth Circuit
  - I. Six Dimensions, Inc. v. Perficient, Inc., 969 F.3d 219 (5th Cir. 2020)
    - a. **Issue:** Whether an entity has "acquired" a trade secret under the Texas Uniform Trade Secrets Act ("TUTSA") where an employee improperly retained trade secrets of his former employer for the benefit of his new employer, discussed the content of those materials with his new employer, but did not provide the materials to his new employer.
    - b. **Holding:** Where an individual improperly retains his employer's trade secrets with the intent of providing them to his new employer, but does so prior to commencing employment and never provides the trade secret materials to his new employer, the new employer has not improperly "acquired" trade secrets under TUTSA, even where there is some evidence that the employee verbally disclosed at least some of the content to his new employer.
    - c. **Procedural Posture:** Plaintiff appealed the denial of its motion for a new trial after a defense verdict was entered on its misappropriation of trade secrets claim under TUTSA (denied).
    - d. Relevant Background: Plaintiff Six Dimensions, Inc. ("Six Dimensions"), a digital marketing firm that provides consulting services for information technology ("IT"), entered into multiple employment agreements with one of its managers that contained employee non-solicitation provisions prohibiting the manager from soliciting any Six Dimensions employees for two years after her termination of employment. The manager left Six Dimensions to work for Perficient, Inc. ("Perficient"), another IT servicing company, and solicited and ultimately convinced seven Six Dimensions employees to come work for Perficient, in alleged breach of her employment agreements.

One of the employees solicited by the manager obtained a thumb-drive of Six Dimensions' confidential training materials before he left the company and retained the materials because he intended to use them to benefit Perficient. The employee did so despite having signed an employment agreement in which he agreed to return all materials "of a secret or confidential nature" back to Six Dimensions upon termination.

After the employee began working for Perficient, he discussed the training materials with another Perficient employee who told him to remove any references to Six Dimensions from the materials and upload them to a Perficient shared-document system. The employee described the nature of what the training materials were and what they contained to the Perficient employee, but did not provide the Perficient employee with the materials and did not upload them to the shared-document system.

Six Dimensions filed suit against Perficient and the manager who had solicited the seven Six Dimensions employees, which included a claim that Perficient had misappropriated Six Dimensions' trade secrets in violation of TUTSA. TUTSA provides six theories under which a plaintiff can establish misappropriation of a trade secret, one of which is by showing that the defendant "acquired" the trade secrets through improper means. At trial, the jury found that the training materials constituted a trade secret under TUTSA, but rendered a verdict for Perficient on the grounds that it did not misappropriate trade secrets as defined in the statute. Six Dimensions filed a motion for a new trial on its misappropriation claim, which the trial court denied, and Six Dimensions appealed.

The Fifth Circuit affirmed the trial court's denial of a new trial, even though it found that the Six Dimensions employee possessed confidential training materials through improper means after his termination of employment with Six Dimensions. However, because the employee was not a Perficient employee when he retained those materials, the court held that Perficient did not misappropriate the training materials through the employee's actions. Furthermore, the court found that Perficient did not misappropriate the training materials even though the employee continued to possess them while he was employed by Perficient and described their contents to another Perficient employee. The court based its decision on the fact that the Six Dimensions

employee did not provide the materials to anyone at Perficient. Even though he described their contents to another Perficient employee, the training materials were never entered into evidence and the court held that the witnesses' testimony did not provide sufficient detail regarding what the Six Dimensions employee told the Perficient employee about them to determine whether trade secrets had been disclosed.

- e. Takeaway: Even where an employee improperly retains confidential trade secrets belonging to his former employer and describes their contents to his new employer, the new employer has not "acquired" those trade secrets under TUTSA if he does not provide the actual materials to his new employer, and his former employer does not provide detailed evidence regarding what specifically was conveyed verbally about the confidential materials.
- 2. Hoover Panel Systems, Inc. v. HAT Contract, Inc., 819 Fed. App'x 190 (5th Cir. 2020)
  - a. **Issue:** Whether a party to a confidentiality agreement was required to mark confidential information as such for it to be protected under the agreement, where the agreement contained (i) a provision generally requiring the confidentiality of all information disclosed and (ii) a subsequent paragraph describing procedures for identifying and marking information as confidential.
  - b. **Holding:** Courts must interpret written agreements in a way that does not render any provisions meaningless, and where two provisions conflict such that there are multiple possible interpretations summary judgment is inappropriate.
  - c. **Procedural Posture:** Plaintiff appealed the trial court's grant of summary judgment to defendant on its breach of contract, misappropriation of trade secrets, and other related claims.
  - d. **Relevant Background:** HAT Contract, Inc. ("HAT") approached Hoover Panel Systems, Inc. ("Hoover"), a product developer and manufacturer, about manufacturing and developing a power beam for desks in an open-office environment, which HAT would then sell. Hoover was reluctant to design a product with HAT because of HAT'S history of using overseas manufacturers for its products, but entered into an agreement to design the power beam after the parties executed a confidentiality agreement.

The confidentiality agreement contained an introductory paragraph stating that certain categories of proprietary information disclosed by one party "shall be considered confidential and shall be retained in confidence by the other party." The agreement also contained a paragraph stating that both parties agreed to keep in confidence and "not use for its or others' benefit" all information disclosed by the other party, "which the disclosing party indicates is confidential or proprietary or marked with words of similar import." The paragraph stated that it also applied to information disclosed orally that is reduced to writing within five days and is marked as being confidential or proprietary.

After the parties executed the agreement, Hoover developed a prototype of the product. During the development process, Hoover suggested that HAT should use an existing base for the prototype, and HAT suggested that a local metal shop could develop a suitable one. Later in the process, HAT and Hoover provided the prototype to multiple dealers for their feedback, and Hoover also provided third parties with drawings and "showroom samples" of the prototype. Hoover never marked any information as confidential during the development process.

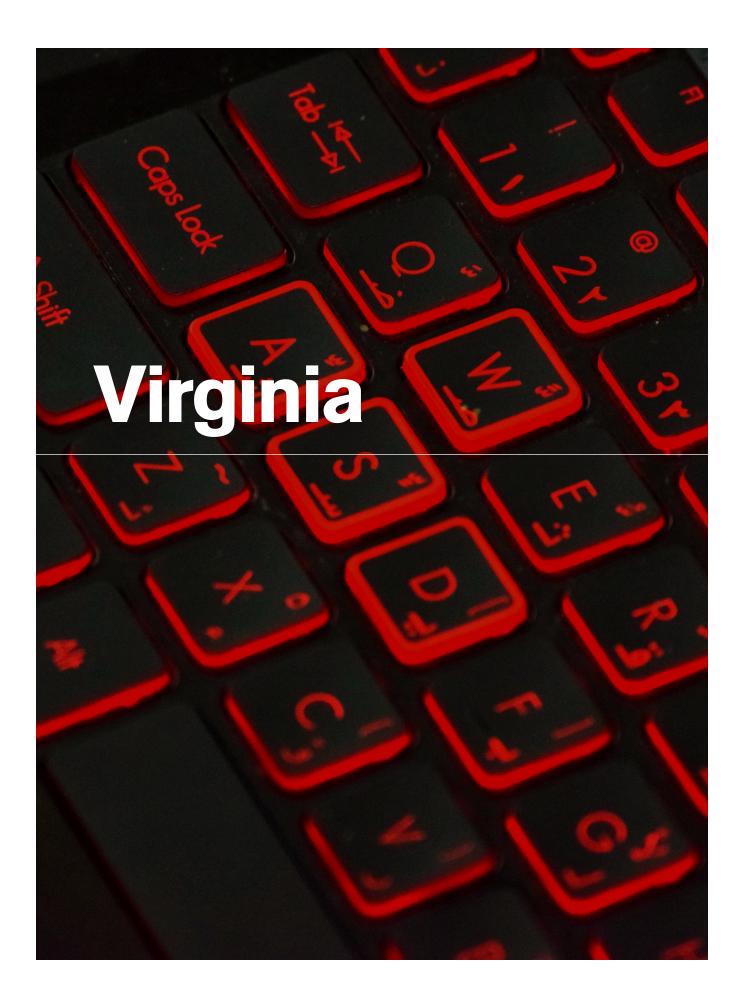
After the prototype was complete, HAT placed several orders with Hoover for the product, but subsequently sent the prototype to an overseas manufacturer and started using it to manufacture similar products to the ones Hoover manufactured. Hoover filed suit against HAT for breach of contract, misappropriation of trade secrets, and several quasi-contractual claims. The trial court granted summary judgment in HAT's favor on each of Hoover's claims, and Hoover appealed.

With respect to Hoover's breach of contract claim, the trial court granted summary judgment in HAT's favor based on its interpretation of the confidentiality agreement as requiring the parties to mark information as confidential in order for it to be protected, and Hoover never marked any information confidential. Hoover argued instead that the introductory paragraph of the agreement required the parties to maintain the confidentiality of Hoover's prototype regardless of whether it was marked.

The Fifth Circuit held that the trial court's grant of summary judgment was improper because it rendered the agreement's introductory paragraph meaningless, and because there were multiple possible interpretations of the agreement that rendered summary judgment inappropriate. For example, Hoover interpreted the introductory paragraph as applying to the prototype and the subsequent paragraph requiring that confidential information be marked as such applied to "other information and communications that were not obviously confidential under the opening paragraph." In contrast, HAT interpreted the introductory paragraph to speak generally about the content of the agreement, and the subsequent paragraph to provide the specific instructions needed to put the confidentiality agreement into effect. Because it was necessary to discern the parties' intent in forming the agreement, which is a matter of fact for a jury, the Fifth Circuit reversed the trial court's grant of summary judgment.

The Fifth Circuit also reversed the trial court's ruling that Hoover waived its right to enforce the agreement and ratified HAT's conduct because Hoover suggested that HAT send the sample to a third party, and was aware that multiple third parties had seen the prototype during the development process. However, because a factual dispute existed over whether Hoover was aware of the full scope of HAT's disclosure of the prototype to overseas manufacturers, the Fifth Circuit found that summary judgment was inappropriate.

- e. **Takeaway:** Courts interpret confidentiality and other agreements by examining the entire writing, and must give effect to all of the provisions so that none are rendered meaningless. As such, when drafting a confidentiality agreement with multiple provisions that address confidentiality of trade secrets, parties should ensure that the provisions do not conflict and can be read together in a way that does not render any part without meaning, or create conflicting or ambiguous interpertations.
- 3. *Richter v. Carnival Corp.*, No. 20-10480, 2020 WL 7054033 (5th Cir. Dec. 1, 2020)
  - a. **Issue:** Whether purported owner's claims for quantum meruit, fraud, and misappropriation against corporation were preempted by the Texas Uniform Trade Secret Act (TUTSA).
  - b. **Holding:** The Court affirmed the lower court's ruling holding that purported owner's claims for quantum meruit, fraud, and misappropriation against the corporation were preempted by the TUTSA.
  - c. **Procedural Posture:** On Appeal—Motion to Dismiss for Failure to State a Claim.
  - d. **Relevant Factual Background:** Sue Richter sued Carnival Corporation alleging that Carnival unlawfully utilized Richter's reality television concept SeaGals to create its own reality television show, Vacation Creation. The district court granted Carnival's Rule 12 (b)(6) motion finding that Richter failed to state a plausible breach of contract claim and that her state law fraud and quantum meruit claims were preempted by TUTSA. On appeal Richter asserted that the district court erred in determining that no implied contract had been formed between Carnival and herself and in finding her state law claims preempted. Richter also claimed that her pleading sought damages not for misappropriation of a trade secret but "for the value of the goods and services she provided to Carnival that were used to create Vacation Creation." Richter fails to identify any goods and services she provided to and were used by Carnival that did not involve the alleged misappropriation of her television show concept. In her complaint, Richer repeatedly referred to the concept for SeaGals as a "trade secret" in alleging that Carnival had misappropriated the concept in its creation of Vacation Creation. However, on appeal, Richter asserted that the SeaGals concept "is likely not a trade secret," and raised the argument at the appellate level for the first time, which the court did not consider since it was not raised in the lower court. Without deciding whether the alleged concept was a trade secret, the court found no error in the district court's determination that the claims are preempted under TUTSA.
  - e. **Takeaway:** All claims under Texas state law for misuse of trade secrets must be brought under the TUTSA.



#### X. Virginia

#### a. State Court

- i. Circuit Court
  - I. *The Metis Group, Inc. v. Allison, et al.*, No. CL 2019-10757, 2020 WL 201152, at \*I (Va. Cir. Ct. Jan. 08, 2020)
    - a. Issue: Whether the restrictive covenants were enforceable as a matter of law
    - b. **Holding:** The Court granted the plea in bar and dismissed all claims, due to its determination that the covenants were unenforceable as a matter of law. The non-compete agreement was unenforceable because it prevented the contractors from pursuing opportunities unrelated to the Metis Group's business model. The Court also found the non-solicitation provision to be overbroad because it also prevented the independent contractors from engaging in opportunities unrelated to Metis' business needs.
    - c. Procedural Posture: Plea in Bar
    - d. Factual Background: The Metis Group (Metis) sued two former independent contractors and the company with whom they were newly affiliated, Preting LLC (Preting). The two former independent contractors were doctors who had provided psychological services for the United States Army on a task order for Metis under a Blanket Purchase Agreement issued by the United States Government. The contractors signed Independent Contractor Agreements with Metis that contained restrictive covenant agreements. The covenants prohibited them from engaging in any professional services with the United States Army anywhere in the world for any purpose, as well as from soliciting Metis employees or contractors. After the conclusion of the Metis task order, the independent contractors provided services to the US Army for Preting. Metis filed suit alleging breach of contract claims against the contractors and tortious interference of contract claims against Preting for interfering with the restrictive covenants. Defendants filed a plea in bar attacking the enforceability of the restrictive covenants. Metis did not seek a TRO or Preliminary lunction.
    - e. **Takeaway:** In Virginia, defendants who seek to invalidate the covenants and dismiss the claims early in the action should do so through plea in bar in order to permit an evidentiary hearing on the scope of the covenants and sufficiency of the legitimate business interests.

#### **About Us**

Founded in 1942, Arent Fox is internationally recognized in core practice areas where business and the law intersect. With more than 430 lawyers and professionals, the firm provides strategic legal counsel and multidisciplinary solutions to a global roster of corporations, governments, and trade associations.

BOSTON LOS ANGELES NEW YORK SAN FRANCISCO WASHINGTON, DC