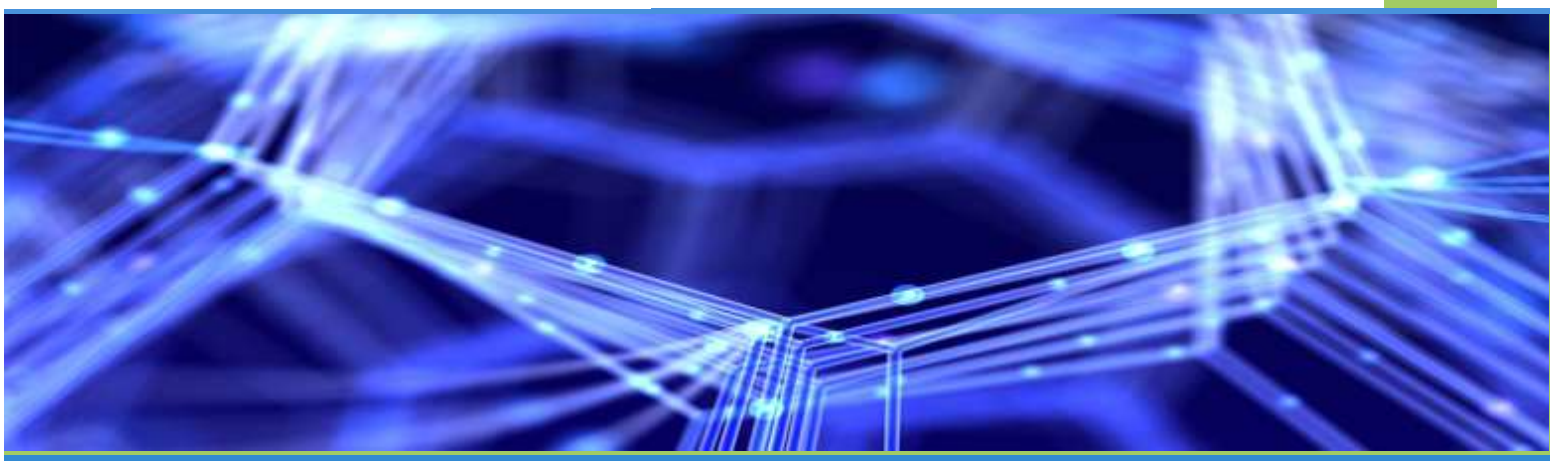
GT GreenbergTraurig | 50 ANNIVERSARY



Intellectual Property & Technology | Advisory

May 2017

The Defend Trade Secrets Act - One Year Later

The Defend Trade Secrets Act (DTSA) celebrates its one-year anniversary on May 11, 2017. The DTSA is the most significant expansion of intellectual property law since the Lanham Act was passed in the 1940s. Approximately 70 cases were filed in California federal courts asserting DTSA claims in the past year; but, after one year of litigation, it is still too early to tell how much impact the DTSA has made on trade secret law in California. Nevertheless, even a one year anniversary is worth marking.

The Differences Between the California Uniform Trade Secret Act and the DTSA

The DTSA automatically bestows federal jurisdiction on trade secret claims, allowing DTSA claims to be brought exclusively in federal court. Although trade secret theft has been a federal crime since 1996, prior to the passage of the DTSA, civil claims for trade secret misappropriation were typically governed by state law. The California Uniform Trade Secret Law (CUTSA) cannot be brought in federal court, absent a showing of diversity or concurrent jurisdiction under another claim arising from the same transaction or occurrence as the CUTSA claim. CUTSA also broadly preempts common law claims based on the same nucleus of facts as the trade secrets claim, however the claim is characterized, such as breach of fiduciary duty, breach of loyalty, conversion, fraud, interference with contract, or unfair competition. In contrast, the DTSA does not preempt any provisions of law, including state trade secret laws, such that a plaintiff filing suit in California can bring both a DTSA and CUTSA claim in federal court. The plaintiff must weigh, in bringing both, whether it wants to allege a CUTSA violation and thereby bar the assertion of related state law tort and restitution claims. Notably, a DTSA claim cannot be brought in state court. Finally, because there are many parallels between the CUTSA and DTSA, federal courts can be expected to consider CUTSA precedent and, longer-term, California courts will likewise consider DTSA decisions.

> **Standing**

Under CUTSA, a plaintiff does not have to be a current owner of a trade secret, whereas DTSA only allows an "owner of a trade secret" to bring a DTSA claim. This may be a distinction without much difference given that the issue of trade secret ownership does not ordinarily arise unless there is a bankruptcy proceeding calling ownership into question, a contractual dispute concerning whether an employee owns (and disclosed) a trade secret prior to employment and appropriately utilized that trade secret at some point after disclosure, or an issue of standing that might arise out of a licensing agreement.

> **Ex Parte Seizure**

A potent remedy potentially available under the DTSA that is not permitted under CUTSA or other state Uniform Trade Secrets Acts is the ability to seek an *ex parte* order to seize stolen trade secrets in the defendants' possession "necessary to prevent the propagation or dissemination of the trade secret." 18 U.S.C. § 1836(b)(2)(A)(i). But, there are a number of hoops to jump through to satisfy the prerequisite findings a court must make before ordering the requested *ex parte* seizure—namely, the court must find that: (i) another form of equitable relief would be inadequate because the party to be enjoined would evade, avoid, or otherwise not comply; (ii) immediate and irreparable injury will occur if the requested seizure is not ordered; (iii) the harm to the applicant outweighs the interests of the party to be enjoined and substantially outweighs potential harm to third parties; (iv) the applicant is likely to succeed on the merits; (v) the party to be enjoined has actual possession of the trade secret; (vi) the *ex parte* request specifically describes the items to be seized with reasonable particularity; (vii) the party to be enjoined would destroy, move, hide, or otherwise make the requested items inaccessible to the court; and (viii) the applicant has not publicized the requested seizure. Plaintiff must set forth all the facts necessary to satisfy these findings through a sworn affidavit or pursuant to a verified complaint.

Out of the eight specific findings that must be established before obtaining *ex parte* seizure relief, the first required showing—that a party would evade or otherwise fail to comply with another form of equitable relief—may well be the most significant hurdle for a plaintiff to clear. In California, only one court to date has addressed an *ex parte* request for seizure and declined to order the seizure, despite finding that there was a risk that the former employees might delete or otherwise destroy emails containing the trade secrets or other materials relevant to the DTSA claim, or that the entities hosting those relevant emails might delete the materials as part of an automated response. *See OOO Brunswick Rail Mgmt. v. Sultanov*, 2017 U.S. Dist. LEXIS 2343, *5 (N.D. Cal. Jan. 6, 2017).

In *Sultanov*, the court found seizure under the DTSA unnecessary because it ordered defendant to deliver to the court all the devices plaintiff identified as containing trade secret materials and ordered the devices not to be accessed or modified prior to delivery to the court. It is not clear what evidence would have been necessary to convince the court that defendant would fail to comply with the court's order. As the first test case for *ex parte* seizures pursuant to the DTSA in California federal court, *Sultanov* highlights the substantial difficulty in preparing an *ex parte* application sufficient to obtain the requested seizure relief. In light of the DTSA statute and the *Sultanov* opinion, plaintiffs seeking *ex parte* seizure relief may want to consider making a written demand on the defendant requesting forensic analysis of all devices reasonably believed to contain trade secret information. Because attorneys' fees can be awarded in connection with a seizure order, a plaintiff needs to proceed cautiously.

> **Other Remedies, Statute of Limitations, and the DTSA Effective Date**

With the exception of the *ex parte* seizure remedy, the DTSA provides the same remedies as the CUTSA and shares the same three-year statute of limitations. Under the DTSA, a continuing misappropriation constitutes a single claim of misappropriation, such that each new act of misappropriation does not restart the statute of limitations. Interestingly, the California federal courts have so far held that trade secrets that were allegedly misappropriated before DTSA's May 11, 2016, effective date can form the basis of a DTSA claim, so long as the plaintiff alleges that the trade secrets misappropriated were used after May 11, 2016. *AllCells, LLC v. Jack Zhai*, Case No. 16-cv-07323-EMC (N.D. Cal. Mar. 27, 2017). In reaching this conclusion in *AllCells*, Judge Chen in the Northern District of California held that because the DTSA defines misappropriation of a trade secret to include the acquisition, use, OR disclosure of a trade secret, use of a trade secret after the effective is still actionable, even if the trade secret was unquestionably

acquired before the DTSA was in existence. Notably, both CUTSA and the DTSA contain similar definitions of what constitutes a "trade secret" and at least one California court has relied on California law to determine whether the allegedly misappropriated information at issue qualified as a trade secret based on the congruency between the DTSA and CUTSA definitions of a trade secret. *See Henry Schein v. Cook*, No. 16-cv-03166-JST (N.D. Cal. June 22, 2016). Because the definitions of key terms in the DTSA and CUTSA are nearly identical and the elements of the claim for misappropriation are so similar, it can be expected that California courts will continue to look to CUTSA cases and rely on California authority when ruling on DTSA claims.

> **California Civil Procedure § 2019.210 and its Potential Interplay with the DTSA**

California Code of Civil Procedure Section 2019.210 requires a trade secret plaintiff to identify the trade secrets it alleges are misappropriated with "reasonable particularity" before discovery can begin on any claim relevant to the allegedly misappropriated trade secret. The Ninth Circuit has not addressed whether Section 2019.210 applies in federal court, and the district courts within the circuit are split. But even some federal courts that do not apply Section 2019.210 nevertheless require, as part of case management responsibilities consistent with the early disclosure requirements of the Federal Rules of Civil Procedure (FRCP), that plaintiff specifically identify its alleged trade secrets in a manner consistent with Section 2019.210 before the commencement of discovery.

The DTSA does not contain the express requirements of Section 2019.210 and it is still too early to tell whether California federal courts will require a plaintiff to comply with Section 2019.210 when bringing a DTSA claim. With one exception, every case out of the approximately 70 filed in California federal court with a DTSA claim or counterclaim also alleged a CUTSA claim, so there is no indication as to whether a DTSA plaintiff will be spared the duty of a Section 2019.210 disclosure. The lone case alleging only a DTSA claim without also asserting a CUTSA claim was voluntarily dismissed before the first case management conference. *See S & P Fin. Advisors v. Kreeyaa, LLC et al.*, Case No. 16-cv-02103-SK (N.D. Cal. 2016). Importantly, complying with the Section 2019.210 requirements in a federal case alleging the DTSA and CUTSA will not cure an ordinary FRCP Rule 8 pleading problem under *Iqbal/Twombly* if the trade secret claimant does not allege particularized facts sufficient to establish the necessary elements of a DTSA claim to survive a motion to dismiss. *See e.g.*, *Space Data Corp. v. X*, No. 16-cv-03260-BLF (N.D. Cal. Feb. 16, 2017). In *Space Data Corp.*, the plaintiff alleged Google's "Project Loon" improperly and unlawfully utilized Space Data's confidential information and trade secrets obtained pursuant to a non-disclosure agreement. The court found that plaintiff failed to 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 (*i.e.*, the definition of a trade secret). In the view of the court, this pleading failure persisted despite plaintiff's compliance with Section 2019.210 because the non-particularized pleadings did not permit defendant Google to ascertain "at least the boundaries within which the secret lies." *Id.* quoting *Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244, 253 (1968).

> **The Inevitable Disclosure Doctrine Is Still Dead in California**

California has long rejected the so-called inevitable disclosure doctrine that allows a plaintiff to allege a claim of trade secret misappropriation by demonstrating that a defendant's new employment will inevitably lead the defendant to rely on the plaintiff's trade secrets. The DTSA is careful not to introduce the inevitable disclosure doctrine into states that have rejected the doctrine, like California. The DTSA expressly forbids an injunction that would limit employing a person based merely on the information the person knows, or that would otherwise conflict with an applicable state law prohibiting restraints on the practice of lawful profession, trade, or business. 18 U.S.C. §§ 1836(b)(3)(A)(i)(I) & (II).

Playing Offense: When Should You Bring a DTSA Claim in California?

If you have a claim for trade secret misappropriation, you want to consider whether you should file a DTSA claim in addition to a CUTSA claim. The DTSA action will put you in federal court and will not preempt other state law claims arising from the same nucleus of facts. Because it remains to be seen whether federal courts in California will require a plaintiff to make a Section 2019.210 disclosure before commencing discovery, although many federal courts already do just that, trade secret plaintiffs should be prepared to describe their allegedly misappropriated trade secrets in detail and revisit the cases where a trade secret has been found to be described with the requisite "reasonable particularity" called for in Section 2019.210.

Playing Defense: Preventative Measures

Putting in place policies, procedures, and practices with respect to your company's intellectual property rights is one of the best ways to protect your company against DTSA claims. Whenever a company hires an employee who worked for a competitor, there is a risk that the new employee's former employer could initiate an action for trade secret misappropriation. Companies can take preventative steps designed to reduce that risk. For example, all new employees can be required to sign a Confidential Information and Inventions Assignment Agreements, or "CIIAA." A general discussion of CIIAAs would take up this entire *GT Advisory*, so instead, we will briefly focus on the portions of a CIIAA that relate to how companies can potentially manage risk of trade secret misappropriation claims.

> **Disclosure of IP rights**

It is important to document any intellectual property rights claims by a new employee. CIIAAs generally contain a "carve-out" provision where the employee lists the inventions that he/she created prior to starting work with your company, any other persons who contributed to the inventions, and relevant dates. Employers should consult with counsel to review this list before the new employee starts his/her employment to determine if any issues need to be explored. California Labor Code 2870 also contains notice requirements as part of any assignment.

> **No Use of Former Employer's Confidential Information**

The risk of a DTSA claim underscores how important it is for every new employee to sign a provision agreeing not to disclose or use any proprietary information, trade secret, or confidential business information of any other person or entity, including any previous employer. It is also important for new employees to represent in writing that they have returned all property, proprietary information, trade secret, and/or confidential business information belonging to any prior employer and to provide copies of any prior non-disclosure agreements (NDAs) they signed.

If the new employee plans to use any device that was used while at his/her prior employer, including laptop, tablet, phone, or other device, the employer should consider having it analyzed prior to the start of employment by a member of its technology team.

If the company discovers that a new employee has disclosed confidential information (CI) belonging to another person or entity, a swift and focused response is key. An immediate investigation regarding the disclosure can be critical. The company should consider reassigning the employee, potential unpaid leave, and possible disciplinary action against the employee including but not limited to termination, if warranted. It is also important to consult with counsel upon discovering there has been a breach, as the company may have an obligation to report the breach to law enforcement. If the disclosure potentially tainted the company's ongoing projects, the company may consider clean room procedures to isolate the tainted intellectual property.

Employees or consultants in sensitive positions may be prohibited from emailing attachments, uploading or downloading data, or using external media on their computers. For certain types of companies that require the highest level of security, all such activity may be monitored and flagged.

Whistleblower Protection

A very new twist that was part of the negotiations leading to the DTSA's passage is a provision that whistleblowers are immune from criminal or civil liability for disclosing a trade secret in confidence to a federal, state, or local government official or attorney, when such disclosure is solely for the purpose of reporting or investigating a suspected violation of law.

The DTSA does not mandate, but encourages employers to disclose the whistleblower immunity by providing a penalty of sorts: an employer cannot recover punitive damages or attorneys' fees in a DTSA action against an employee/consultant unless the employer protected notice of the DTSA whistleblower protections in its employment

contract or agreement with the employee/consultant. There is nothing in the statute that suggests that this same immunity extends to new employers or others who were not in an employment relationship with the employer.

The first reported decision applying the whistleblower immunity provision was issued on Dec. 6, 2016. *Unum Group v. Loftus*, CIVIL ACTION NO. 4:16-CV-40154-TSH (D. Mass. Dec. 6, 2016). In that case, employee Loftus removed several boxes of information and a laptop computer from the Unum offices after usual business hours, ultimately returning the laptop and contending that the information removed related to government inquiries and investigations of misconduct. Unum sued Loftus for federal and state trade secret misappropriation as well as state law conversion. Loftus moved to dismiss the complaint. In refusing to dismiss the action, the court treated the whistleblower provision as an affirmative defense, noting that: the record lacked facts to support or reject his affirmative defense at this stage of litigation; there had been "no discovery to determine the significance of the documents taken or their contents"; Loftus had not filed any potential lawsuit; it was not ascertainable from the complaint whether Loftus turned over all of Unum's documents to his attorney, which documents he took, and what information they contained, or whether he used, is using, or plans to use, those documents for any purpose other than "investigating a potential violation of law."

Courts will continue to address and resolve issues relating to whistleblower immunity. There was no indication Unum had adopted DTSA's immunity language, but the case certainly highlights that employees sometimes actively seek to become whistleblowers. Thus, some companies may conclude that including the DTSA immunity language conceivably encourages misguided "whistleblowing." Companies should assess their own risks and, in conjunction with counsel, make decisions regarding disclosure of the whistleblower protections in the DTSA. For example, a company may determine that the risk of encouraging misguided "whistleblowing" outweighs the risk of losing the ability to recover punitive damages and attorney's fees against an employee who misappropriates trade secrets, particularly when they may be judgment proof in any event.

Some commentators have identified another area of concern relating to the DTSA whistleblower protection provisions. The whistleblower immunity could potentially have the effect of allowing the government greater authority to obtain information regarding companies' IP, even when that particular company has not violated, and is not suspected of violating, any laws. For example, if the government was pursuing a criminal investigation regarding suspected international money-laundering activities and the government needed certain encryption technology to access encrypted data, the government could theoretically contact employees of a technology company and request that they disclose the tech company's encryption technology. If the employee cooperated, such disclosure could arguably fall under the whistleblower immunity. The end result would be that the employee is immune from civil or criminal liability, and the company's trade secrets are now in the hands of the government, with whatever attendant risks that may entail.

This *GT Advisory* was prepared by **Kurt A. Kappes**, **Karen Rosenthal**, and **Sarah E. Barrows**. Questions about this information can be directed to:

- Kurt A. Kappes | +1 916.442.1111 | kappesk@gtlaw.com
- Karen Rosenthal | +1 650.289.7868 | rosenthalk@gtlaw.com
- Sarah E. Barrows | +1 415.655.1251 | barrowss@gtlaw.com
- Or your Greenberg Traurig attorney

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+82 (0) 2.369.1000

Shanghai
+86 (0) 21.6391.6633

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+03.636.6000

Tokyo¤
+81 (0)3 4510 2200

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900