PROGRAM MATERIALS
Program #31108
May 18, 2021

DTSA: An Overview and Update of Recent Cases

- John Adams, Esq. – Lynn Pinker Hurst & Schwegmann
- Sara Chelette, Esq. – Lynn Pinker Hurst & Schwegmann

Celesq® AttorneysEd Center
www.celesq.com
5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

The Defend Trade Secrets Act: An overview and case update

By: Sara Hollan Chelette and John S. Adams

LYNN PINKER HURST & SCHWEGMANN

Purpose

The [DTSA] offers a needed update to Federal law to provide a Federal civil remedy for trade secret misappropriation. Carefully ***balanced to ensure an effective and efficient remedy*** for trade secret owners whose intellectual property has been stolen, the legislation is designed to avoid disruption of legitimate businesses, ***without preempting State law.***

This narrowly drawn legislation ***will provide a single, national standard*** for trade secret misappropriation with clear rules and predictability for everyone involved. Victims will be able to move quickly to Federal court, ***with certainty of the rules, standards, and practices*** to stop trade secrets from winding up being disseminated and losing their value. As trade secret owners increasingly face threats from both at home and abroad, the bill equips them with the tools they need to effectively protect their intellectual property and ensures continued growth and innovation in the American economy.

H.R. Rep. No. 114-529, at 6 (2016).

Notable verdicts

- **$855 million** verdict for various claims, including under the DTSA.

  (*Syntel Sterling Best Shores Mauritius Ltd. et al. v. The Trizetto Group Inc. et al.*, No. 1:15-cv-00211 (S.D.N.Y. October 27, 2020))

- **$764 million** verdict in favor of Motorola, including for claims under the DTSA

  (*Motorola Solutions, Inc. v. Hytera Communications Corp. Ltd.*, No. 1:17-cv-01973, ECF No. 947 at 1 (N.D. Ill. Mar. 5, 2020)).

- **$91.3 million** verdict against L'Oreal, including for claims under the DTSA.

  (*Liqwd, Inc. v. L'Oréal USA, Inc.*, CIVIL ACTION NO. 17-14-JFB-SRF, (D. Del. Dec. 16, 2019))

Pleading Elements

(1) the existence of a trade secret that relates to a product or service used in, or intended for use in, interstate or foreign commerce;

(2) the acquisition of the trade secret, or the use or disclosure of the trade secret without consent; and

(3) the person acquiring, using, or disclosing the trade secret knew or had reason to know that the trade secret was acquired by improper means.

Zvelo, Inc. v. Akamai Techs., Inc., 19-CV-00097-PAB-SKC, 2019 WL 4751809, at *2 (D. Colo. Sept. 30, 2019); *see also Alta Devices, Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868, 880–81 (N.D. Cal. 2018) ; *Parker v. Petrovics*, 2:19-CV-00699-RDP, 2020 WL 3972761, at *4 (N.D. Ala. July 14, 2020); *Ruby Slipper Cafe, LLC v. Belou*, CV 18-1548, 2019 WL 1254897, at *5 (E.D. La. Mar. 19, 2019).

Failure to Adequately Plead

Figure 20: Ownership Findings for Cases Terminated from 2010 to 2019

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Judgment as a Matter of Law	Trial	Any Judgment Event
Ownership / Validity	0	4	6	20	53	0	83
Failure to Identify Trade Secret	3	0	41	101	11	1	156
Failure to Maintain Secrecy	0	0	23	74	18	3	116
Generally Known / Readily Ascertainable	0	0	4	54	13	1	72
No Ownership / Validity: Wrong Entity	0	0	7	10	2	0	19

(Lex Machina Trade Secret Litigation Report 2020 at 18).

“Trade Secret”

The term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;

18 U.S.C. § 1839 (3).

“Misappropriation”

The term “misappropriation” means—

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who--

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was--

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that--

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake;

18 U.S.C. § 1839 (5).

Acquisition, Disclosure, or Use

Under the statute, proving misappropriation "requires a showing of one of two categories:

- (1) wrongful acquisition, or

- (2) disclosure or use of the trade secret without consent."

Lamont v. Conner, No. 5:18-CV-04327-EJD, 2019 WL 1369928, at *8 (N.D. Cal. Mar. 26, 2019*); Accresa Health LLC v. Hint Health Inc.*, No. 4:18-CV-00536, 2020 WL 3637801, at *12 (E.D. Tex. July 6, 2020).

“Improper Means”

The term “improper means”—

(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and

(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition.

18 U.S.C. § 1839 (6).

Identification

- Due to the nature of the secrecy requirement inherent in the nature of a trade secret, "a plaintiff need not spell out the details of the trade secret" in a pleading.

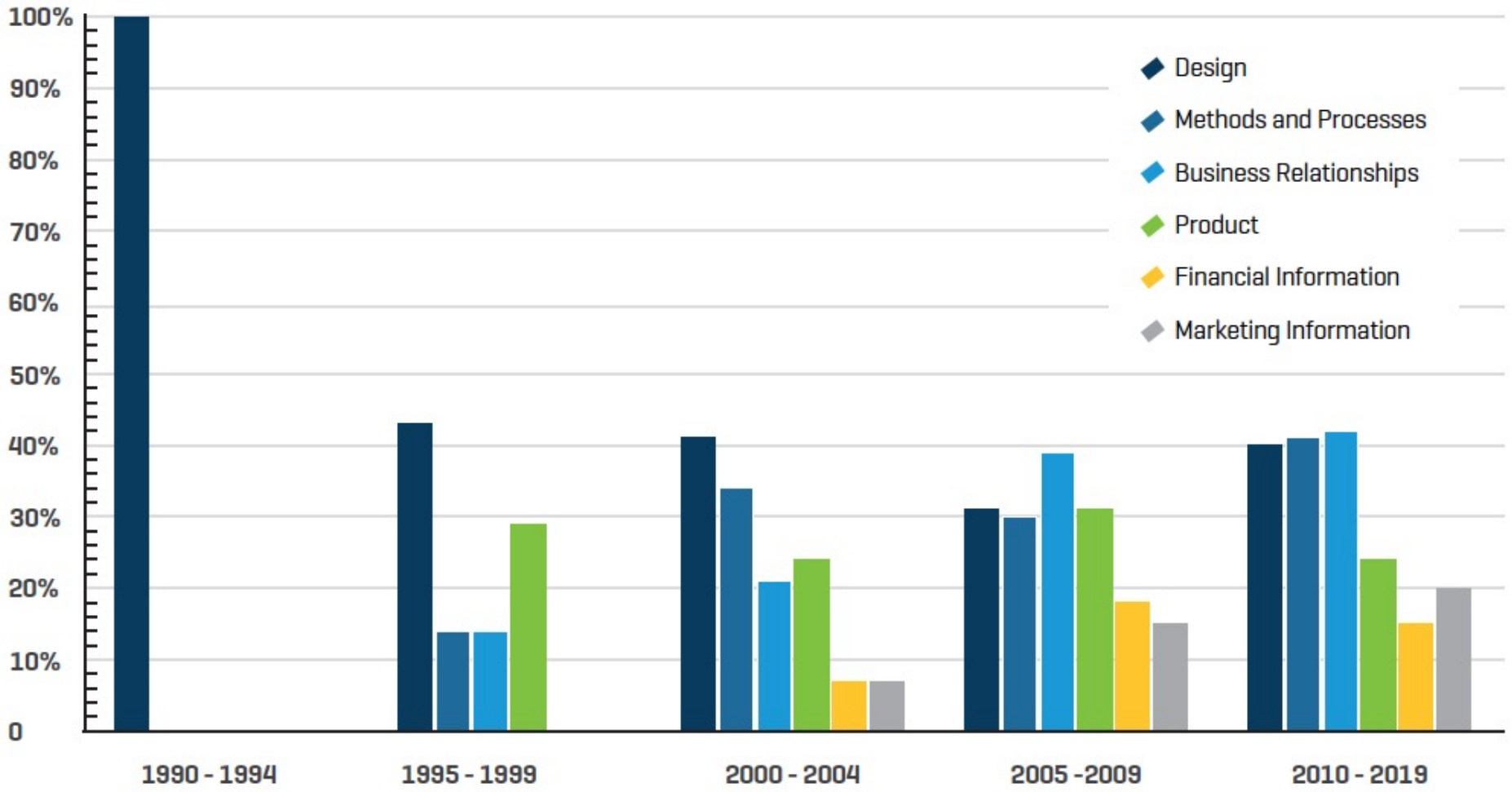
- The plaintiff must "describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies."

Alta Devices, Inc., 343 F. Supp. 3d at 881 (citing *Autodesk, Inc. v. ZWCAD Software Co.*, No. 5:14-cv-01409-EJD, 2015 WL 2265479, at *5 (N.D. Cal. May 13, 2015)) (citing *Vendavo, Inc. v. Prixe f(x) AG*, No. 17-cv-06930-RS, 2018 WL 1456697, at *4 (N.D. Cal. Mar. 23, 2018)).

Common Trade Secrets

FIGURE 2:

Portion of Cases by Type of Trade Secrets Over 29-Year Period



(Stout Trends in Trade Secret Litigation Report, Figure 2 at 27).

Reasonable Measures

Figure 20: Ownership Findings for Cases Terminated from 2010 to 2019

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Trial	Judgment as a Matter of Law	Any Judgment Event
Ownership / Validity	0	4	6	20	53	0	83
Failure to Identify Trade Secret	3	0	41	101	11	1	156
Failure to Maintain Secrecy	0	0	23	74	18	3	116
Generally Known / Readily Ascertainable	0	0	4	54	13	1	72
No Ownership / Validity: Wrong Entity	0	0	7	10	2	0	19

(Lex Machina Trade Secret Litigation Report 2020 at 18).

Internal Security

Table 2. Identity of Alleged Misappropriator

	1950–2007	2008
Employee or former employee	52% (142)	59% (71)
Business partner	40% (109)	31% (37)
Unrelated third party	3% (8)	9% (10)
Other or unknown	7% (19)	5% (6)

(Statistical Analysis of Trade Secret Litigation, 45 Gonzaga L. Rev. 291, 302).

General Measures

- Pleadings that identify internal control measures like employee handbooks and password protected databases may be sufficient to survive a motion to dismiss.

- Other cases have found reasonable measures existed when the information was not only protected by a confidentiality agreement, but the plaintiff also demanded return or destruction of its information following the terms of the agreement

ATS Grp., LLC v. Legacy Tank & Indus. Servs. LLC, 407 F. Supp. 3d 1186, 1199–200 (W.D. Okla. 2019); *see also Par Pharm., Inc. v. QuVa Pharma, Inc.*, 764 F. App'x 273, 278 (3d Cir. 2019); *RKI, Inc.*, 177 F. Supp. 2d at 866; *Zoppas Indus. de Mexico, S.A. de C.V. v. Backer EHP Inc.*, CV 18-1693-CFC, 2019 WL 6615421, at *3 (D. Del. Dec. 5, 2019), report and recommendation adopted, CV 18-1693-CFC, 2020 WL 205485 (D. Del. Jan. 14, 2020).

Electronic Information

For electronically stored information, reasonable measures include "[using an] access-limited, password-protected server and that there was a limited group of employees with that access to the server[.]" Employers can protect trade secrets also by using tailored "access profiles," limiting its computer users to only access appropriate company information, and prohibiting employees from saving confidential information on public portions of the company's computer network. And employers can prohibit "employees from forwarding confidential information to a personal email account or by email generally without proper labeling and authorization."

S. Field Maint. & Fabrication LLC v. Killough, 2:18-CV-581-GMB, 2019 WL 360515, at *4 (M.D. Ala. Jan. 29, 2019); *Magnesita Refractories Co. v. Tianjin New Century Refractories Co.*, No. 1:17-CV-1587, 2019 WL 1003623, at *10 (M.D. Pa. Feb. 28, 2019); *see also Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1135–38 (N.D. Ill. 2019); *SKF USA Inc. v. Bjerkness*, 2010 WL 3155981, at *6 (N.D. Ill. Aug. 9, 2010).

Interstate Commerce

"Plaintiff must demonstrate that the trade secret implicates interstate or foreign commerce. Defendant does not dispute this element and the Court finds the pleading sufficient. Here, the purported information relates to services used and intended for use in interstate and foreign commerce because it contains business plans, procurement strategies and subcontractor and vendor relationships."

Space Sys./Loral, LLC v. Orbital ATK, Inc., 306 F. Supp. 3d 845, 854–55 (E.D. Va. 2018); *see also Hawkins*, 301 F. Supp.3d at 658–59, 2017 WL 4613664, at *6.

Extraterritoriality

Courts have extraterritorial jurisdiction when:

(1) the offender is a …citizen …of the United States …; or

(2) an act in furtherance of the offense was committed in the United States.

18 U.S.C. § 1837(2).

DTSA Immunity

(1) Immunity.--An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that--

(A) is made--

(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and

(ii) solely for the purpose of reporting or investigating a suspected violation of law; or

(B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

(2) Use of trade secret information in anti-retaliation lawsuit.--An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual--

(A) files any document containing the trade secret under seal; and

(B) does not disclose the trade secret, except pursuant to court order.

18 U.S.C. § 1833.

Employee Whistleblower Notice

It is important for employers to provide notice of the whistleblower immunity to preserve their ability to recover exemplary damages and attorneys' fees against an employee under the DTSA. An employer forfeits these valuable remedies under the DTSA in litigation against an employee who was not afforded notice of the immunity.

18 U.S.C. § 1833(b)(3).

Employee Immunity

Most courts confronted with an employee's claim of immunity consider immunity to be an affirmative defense that cannot be addressed through a motion to dismiss pursuant to Rule 12(b)(6). Those courts note the reluctance "to dismiss complaints based on affirmative defenses at the pleading stage before any discovery has been conducted." Dismissal at the 12(b)(6) stage is possible under the right circumstances—if "the plaintiff's own allegations show that a defense exists that legally defeats the claim for relief."

See, e.g., FirstEnergy Corp. v. Pircio, Case No. 1:20-cv-1966, 2021 WL 857107 at * 7 (N.D. Ohio Mar. 8, 2021) ("Without question, immunity constitutes an affirmative defense."); *see also Christian v. Lannet Co.*, No. 16-CV-963, 2018 WL 1532849 (E.D. Pa. March 29, 2018); *Unum Group v. Loftus*, 220 F. Supp. 3d 143, 147 (D. Mass. 2016); *Garcia v. Vertical Screen Inc.,* Civil Action No. 19-3184, 2020 WL 2615624, at *5 (E.D. Penn. May 22, 2020).

No Preemption

FIGURE 3:

Frequency of Other Claims Accompanying Trade Secret Misappropriation
(Out of 257 cases researched)

ACCOMPANYING CAUSE OF ACTION	NO. OF CASES	PERCENTAGE OF TOTAL
Contract Claims	179	69.6%
Tortious Interference	117	45.5%
Unfair/Deceptive Practices	110	42.8%
Fraud Claims	78	30.4%
Breach of Responsibility / Fiduciary Duty	78	30.4%
Conversion	73	28.4%
Infringement	60	23.3%
Unjust Enrichment	49	19.1%
Conspiracy	40	15.6%
Defamation/Disparagement	11	4.3%
Trespass	5	1.9%
Emotional/Mental Distress	1	0.4%
Other	100	38.9%

(Stout Trends in Trade Secret Litigation Report, Figure 3at 29).

Civil Seizure

The court may not grant a civil seizure application unless the court finds "it clearly appears from specific facts" that:

1. an injunction or other form of equitable relief would be inadequate because the party to which the order would be issues would evade, avoid, or otherwise not comply with the order;
2. an immediate and irreparable injury will occur if such seizure is not ordered;
3. the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;
4. the applicant is likely to succeed in showing that
5. the information is a trade secret; and
6. the person against whom seizure would be ordered
   a. misappropriated the trade secret of the applicant by improper means; or
   b. conspired to use improper means to misappropriate the trade secret of the applicant;
7. the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;
8. the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; ***and***
9. the applicant has not publicized the requested seizure.

18 U.S.C. § 1836(b)(2)(A).

Civil Seizure Order

1. The order must:
2. set forth findings of fact and conclusions of law;
3. provide for the narrowest seizure of property necessary to achieve the purpose and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;
4. be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access is consistent with the requirements of materials in the court's custody set forth in Paragraph D of the statute (addressing storage medium, confidentiality protections, and appointment of a special master);
5. provide guidance to law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including:
    a. the hours during which the seizure may be executed; and
    b. whether force may be used to access locked areas;
6. set a date for hearing at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; ***and***
7. require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or attempted seizure.

18 U.S.C. § 1836(b)(2)(B).

Cases Denying Seizure

- *000 Brunswick Rail Mgt. v. Sultanov*, Case No. 5:17-cv-00017-EJD, 2017 WL 67119 at 1 (N.D. Cal. Jan. 6, 2017).

- *Hayes Healthcare Servs., LLC v. Meacham*, Case No. 19-60113, 2019 WL 2637053, at *6 (S.D. Fla. Feb. 1, 2019).

Cases Granting Seizure

- *Mission Capital Advisors LLC v. Romaka*, 16-CV-5878 (RA), 2016 WL 11517040, at *1 (S.D.N.Y. July 22, 2016).

- *Axis Steel Detailing, Inc. v. Prilex Detailing LLC,* No. 2:17-CV-00428-JNP, 2017 WL 8947964, at *1 (D. Utah June 29, 2017).

- *AVX Corp. v. Kim,* Civil Action No. 6:17-00624-MGL, 2017 WL 11316598 at *1-2 (D.S.C. Mar. 13, 2017).

Damages

The DTSA provides that a court may award:

- "damages for actual loss caused by the misappropriation of a trade secret"; and

- damages for "unjust enrichment… not addressed in computing damages for actual loss."

18 U.S.C. § 1836(b)(3)(B).

Irreparable harm may be presumed

In *Faiveley Transp. Malmo AB v. Wabtec,* which predated the DTSA, the Second Circuit explained that a rebuttable presumption of irreparable harm "might be warranted in cases where there is a danger that, unless enjoined," a defendant will continue to disseminate already misappropriated trade secrets, "or otherwise irreparably impair the value of those secrets."

Faively Transp. Malmo AB v. Wabtec Corp., 559 F.3d 110, 118 (2d Cir. 2009); *Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1143-44 (N.D. Ill. 2019) (applying a rebuttable presumption in an action brought under the DTSA and the Illinois Trade Secrets Act); *Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc.,* No. 4:06CF114, 2010 WL 3370286, at *2 (N.D. Ohio Aug. 26, 2010) ("Courts in the 6th Circuit have stated only that harm caused by the misappropriation of trade secrets is generally irreparable and may be presumed in some cases." (citations omitted)).

Irreparable harm may not be presumed

In *First Western Capital Mgmt. v. Malamed,* the Tenth Circuit reversed the grant of an injunction in favor of a former employer under the DTSA, without the movant demonstrating irreparable harm. The district court determined that a showing of irreparable harm was excused "when the evidence shows that a defendant is or will soon be engaged in acts or practices prohibited by statute, and that statute provides for injunctive relief to prevent such violations." The DTSA authorizes, but does not require, injunctive relief. Therefore, according to the Tenth Circuit, plaintiffs seeking preliminary injunctive relief under DTSA must demonstrate irreparable harm.

First Western Capital Mgmt. v. Malamed, 874 F.3d 1136, 1138 (10th Cir. 2017).

The Defend Trade Secrets Act:

An overview and case update

By: Sara Hollan Chelette and John S. Adams[1]

[1] With special thanks to Brittany Rummel, Ph.D., Baylor Law School JD Candidate Class of 2022 for her valuable assistance with research and editing.

DTSA's Enactment and Purpose *1*

The DTSA's Significance *3*

Filing Trends **3**

Notable cases and awards **4**

Pleading a DTSA claim *4*

Definitions **6**

"Trade Secret" 6

"Misappropriation" 6

"Improper Means" 7

The plaintiff must disclose its trade secrets. **8**

Trade secrets examples **13**

Reasonable measures to protect trade secrets **15**

Examples of adequate measures: 17

Examples of inadequate measures 19

Marking materials as "confidential" 22

Interstate commerce **23**

Direct and indirect misappropriation **25**

Extraterritoriality **25**

Other issues *26*

Employment agreements and whistleblower immunity **26**

Interaction with other laws *31*

No preemption **31**

No aiding and abetting or conspiracy **32**

Contracts & Economic Loss Rule **32**

Remedies *33*

DTSA's Civil Seizure Remedy **33**

Cases Denying Seizure 37

Cases Granting Seizure 38

Injunctions and Irreparable Harm **39**

Damages theories **41**

Statute of Limitations *45*

DTSA's Enactment and Purpose

The Defend Trade Secrets Act of 2016 ("DTSA") arose out of the recognition that trade secrets are of growing importance and their theft results in an economically devastating crime for American innovators.[2] In its report on the DTSA, the Senate Judiciary Committee noted that "the Commission on the Theft of American Intellectual Property estimated that annual losses to the American economy caused by trade secret theft are over $300 billion, comparable to the current annual level of U.S. exports to Asia."[3] That same report concluded that trade secret theft led to 2.1 million American jobs being lost each year.[4] A separate study conducted by PricewaterhouseCoopers LLP and the Center for Responsible Enterprise and Trade found that the annual cost of trade secret theft may be as high as $480 billion.[5]

Before the DTSA, while other types of intellectual property were protected primarily by Federal law—like patents, trademarks, and copyrights—trade secret protection was largely a matter of State law.[6] The Senate Committee recognized that although the Uniform Trade Secrets Act ("UTSA") had been adopted in 47 states and the District of Columbia as of 2015, differences between State laws and the UTSA that appeared minor could actually prove to be case dispositive: "they may affect which party has the burden of establishing that a trade secret is not readily ascertainable, whether the owner has any rights against a party that innocently acquires a trade secret, and what measures are necessary to satisfy the requirement that the owner employ 'reasonable measures' to maintain secrecy of the information."[7] The differences in the state laws required national companies to tailor costly compliance plans to meet each state's law.[8] And trade secret theft rarely is confined to a single state.[9] The movement of trade secrets

---

[2] S. Rep. No. 114-220, at 1-2 (2016).

[3] *Id.* (citing The IP Commission, The Report of the Commission on the Theft of American Intellectual Property (May 2013), available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf).

[4] *Id.*

[5] *Id.* (citing Richard A. Hertling & Aaron Cooper, Trade Secret Theft: The Need for a Federal Civil Remedy, The National Law Review (June 25, 2014), available at http://www.natlawreview.com/article/trade-secret-theft-need-federal-civil-remedy).

[6] *Id.*

[7] *Id.* at 2-3.

[8] H.R. Rep. No. 113-657, at 7 (2014); H.R. Rep. No.114-529, at 4 (2016).

[9] *Id*.

across state lines make it hard for state courts to control discovery and serve defendants.[10] Additionally, trade secret theft often requires swift action across state lines to preserve evidence and keep a thief from taking the trade secret beyond the United States and the reach of its courts.[11]

The trade secret protection that existed at the Federal level before the DTSA was fairly limited. The Economic Espionage Act of 1996 ("EEA") made it a Federal crime to misappropriate a trade secret that had an interstate or foreign nexus, but it did not create a private right of action.[12] Because Federal criminal enforcement resources are far from unlimited, the EEA was not a complete solution to prevent misappropriation of trade secrets.[13] And, as a criminal statute, the EEA was not suited for making victims of misappropriation whole.[14]

The DTSA's purpose is to "provide a Federal cause of action that will allow trade secrets owners to protect their innovations by seeking redress in Federal court, bringing their rights into alignment with those long enjoyed by owners of other forms of intellectual property, including copyrights, patents, and trademarks."[15] As the House of Representatives Committee on the Judiciary wrote in its report to the House:

> The [DTSA] offers a needed update to Federal law to provide a Federal civil remedy for trade secret misappropriation. Carefully balanced to ensure an effective and efficient remedy for trade secret owners whose intellectual property has been stolen, the legislation is designed to avoid disruption of legitimate businesses, without preempting State law. This narrowly drawn legislation will provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved. Victims will be able to move quickly to Federal court, with certainty of the rules, standards, and practices to stop trade secrets from winding up being disseminated and losing their value. As trade secret

[10] *Id*.

[11] *Id*.

[12] S. Rep. No. 114-220, at 1-2 (2016).

[13] *Id.*

[14] H.R. Rep. No. 113-657, at 7 (2014); at 7; H.R. Rep. No.114-529, at 4 (2016).

[15] S. Rep. No. 114-220, at 1-2 (2016).

> owners increasingly face threats from both at home and abroad, the bill equips them with the tools they need to effectively protect their intellectual property and ensures continued growth and innovation in the American economy.[16]

S. 1890, the DTSA, was introduced in the Senate on June 29, 2015.[17] It passed in the Senate by a vote of 87-0 and in the House by a vote of 410-2.[18] It was signed into law by President Obama on May 11, 2016.[19]

The DTSA's Significance

Filing Trends

Since the DTSA was enacted, trade secret litigation has increased approximately 24%, although other intellectual property litigation has remained steady or even declined.[20] Industry analysts project even further increased trade secret litigation because:

1. the DTSA provides additional remedies, additional forums (federal courts), and more uniform procedures (federal rules);
2. recent patent decisions[21] limit the patentability of certain new inventions, requiring businesses to protect IP through trade secret laws; and

---

[16] H.R. Rep. No. 114-529, at 6 (2016).

[17] Defend Trade Secrets Act of 2016, Pub. Law No. 114-153, 130 Stat. 376 (congress.gov/bill/114th-congress/senate-bill/1890/actions)

[18] *Id.*

[19] *Id.*

[20] Schwartz et al., *INSIGHT: Trade Secrets 2019 Litigation Roundup and 2020 Trends*, BLOOMBERG LAW (January 28, 2020), https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-trade-secrets-2019-litigation-roundup-and-2020-trends.

[21] *See, e.g., Alice Corp. Pty. Ltd. v. CLS Bank International*, 573 U.S. (2014); *see also* Ognjen Zivojnovic, *Patentable Subject Matter After Alice-Distinguishing Narrow Software Patents from Overly Broad Business Method Patents*, 30 Berkeley Tech. L.J. 807, 807 (2015) ("In its most recent decision addressing the patent eligibility of software, *Alice Corp. Pty. Ltd. v. CLS Bank International,* the Supreme Court held that adding the words "apply it with a computer" to a patent-ineligible abstract idea is not "enough" to confer patent eligibility. This holding can be interpreted narrowly, affecting only business method patents-- i.e., software patents that amount to little more than a fundamental economic practice (i.e., a "business method") applied "with a computer." However, *Alice* also endorsed a theory that the exceptions to patent eligibility (including the abstract idea exception) are substantive limitations meant to protect against overly board patents. In

3. increased workforce mobility is likely to lead to more employment related trade secret theft.[22]

Notable cases and awards

Trade secret litigation, particularly under the DTSA, has garnered significant attention due to high-profile parties involved and large damages awards. For example:

- $855 million verdict for various claims, including under the DTSA.[23]
- $764 million verdict in favor of Motorola, including for claims under the DTSA.[24]
- $91.3 million verdict against L'Oreal, including for claims under the DTSA.[25]

Pleading a DTSA claim

Although phrased in a variety of ways, the elements of a DTSA claim essentially mirror the elements of common law claims and claims under UTSA:

> (1) the existence of a trade secret that relates to a product or service used in, or intended for use in, interstate or foreign commerce;
>
> (2) the acquisition of the trade secret, or the use or disclosure of the trade secret without consent; and
>
> (3) the person acquiring, using, or disclosing the trade secret knew or had reason to know that the trade secret was acquired by improper means.[26]

---

the lower court *en banc* decision, four Federal Circuit judges argued that adopting this substantive limitation theory would be the death knell for all software patents. While the Supreme Court left ample room for interpretation between these two extremes, whether due to *Alice* or other factors, ***lower courts have invalidated the majority of software patents challenged under § 101 since the Alice decision***.").

[22] Jeffrey Mordaunt et al., *Trends in Trade Secret Litigation Report 2020* (Stout 2020).

[23] *Syntel Sterling Best Shores Mauritius Ltd. et al. v. The Trizetto Group Inc. et al.*, No. 1:15-cv-00211, ECT No. 931 (S.D.N.Y. October 27, 2020).

[24] *Motorola Solutions, Inc. v. Hytera Communications Corp. Ltd*., No. 1:17-cv-01973, ECF No. 947 at 1 (N.D. Ill. Mar. 5, 2020).

[25] *Liqwd, Inc. v. L'Oréal USA, Inc.*, No. 1:17-cv-00014, ECF No. 1060, (D. Del. Dec. 16, 2019).

[26] *Zvelo, Inc. v. Akamai Techs., Inc*., 19-CV-00097-PAB-SKC, 2019 WL 4751809, at *2 (D. Colo. Sept. 30, 2019); *see also Alta Devices, Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868, 880–81 (N.D. Cal. 2018) ("To reiterate, under

It is important to know and plead the elements of a trade secret claim because judgments on the pleadings are not uncommon, particularly for failing to adequately plead the existence of a trade secret—i.e. sufficiently identifying it and pleading measures to protect its secrecy:

Figure 8: Trade Secret Ownership Findings for Cases Terminated from 2009 to 2018 Q2

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Trial	Judgment as a Matter of Law	Any Judgment Event
Ownership / Validity	0	4	4	21	49	0	78
Failure to Identify Trade Secret	3	0	20	77	8	1	109
Failure to Maintain Secrecy	0	0	12	65	11	2	88
Generally Known / Readily Ascertainable	0	0	1	49	8	1	59
No Ownership / Validity: Wrong Entity	1	0	0	7	0	0	8

(Rachel Bailey, *Lex Machina Trade Secret Litigation Report 2018* at 7).

Figure 20: Ownership Findings for Cases Terminated from 2010 to 2019

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Trial	Judgment as a Matter of Law	Any Judgment Event
Ownership / Validity	0	4	6	20	53	0	83
Failure to Identify Trade Secret	3	0	41	101	11	1	156
Failure to Maintain Secrecy	0	0	23	74	18	3	116
Generally Known / Readily Ascertainable	0	0	4	54	13	1	72
No Ownership / Validity: Wrong Entity	0	0	7	10	2	0	19

the DTSA and the CUTSA, a plaintiff must allege (1) that it is the owner of a trade secret; (2) that the defendant misappropriated the trade secret; and (3) that it was damaged by the defendant's actions. Courts have held that the DTSA and the CUTSA share the same pleading requirements for the identification of trade secrets."); *Parker v. Petrovics*, 2:19-CV-00699-RDP, 2020 WL 3972761, at *4 (N.D. Ala. July 14, 2020) ("To plead a violation of the DTSA, a plaintiff must allege that he "'(i) possessed information of independent economic value' that (a) 'was lawfully owned by' the plaintiff, (b) for which the plaintiff 'took reasonable measures to keep secret,' and (ii) the defendant 'used and/or disclosed that information' despite (iii) 'a duty to maintain its secrecy.'"); *Ruby Slipper Cafe, LLC v. Belou*, CV 18-1548, 2019 WL 1254897, at *5 (E.D. La. Mar. 19, 2019) ("To prevail on a DTSA claim, a plaintiff must prove: (1) the existence of a trade secret; (2) the misappropriation of the trade secret by another; and (3) the trade secret's relation to a good or service used or intended for use in interstate or foreign commerce.").

(Rachel Bailey, *Lex Machina Trade Secret Litigation Report 2020* at 18).

Definitions

"Trade Secret"

The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

> **(A)** the owner thereof has taken reasonable measures to keep such information secret; and
>
> **(B)** the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;[27]

"Misappropriation"

The term "misappropriation" means—

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who–

> **(i)** used improper means to acquire knowledge of the trade secret;
>
> **(ii)** at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was–
>
> > **(I)** derived from or through a person who had used improper means to acquire the trade secret;
> >
> > **(II)** acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

[27] 18 U.S.C. § 1839 (3).

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that--

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake;[28]

Under the statute, proving misappropriation "requires a showing of one of two categories: (1) wrongful acquisition, or (2) disclosure or use of the trade secret without consent."[29]

Even so, at least one court has quoted pre-DTSA trade secret case law from the Fifth Circuit for the proposition that, "[f]or a plaintiff to recover damages on a trade-secret misappropriation claim, '[t]he defendant must have actually put the trade secret to some commercial use [because] [t]he law governing protection of trade secrets essentially is designed to regulate unfair business competition, and is not a substitute for criminal laws against theft or other civil remedies for conversion.'"[30]

"Improper Means"

The term "improper means" —

(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and

(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition.[31]

---

[28] 18 U.S.C. § 1839 (5).

[29] *Lamont v. Conner*, No. 5:18-CV-04327-EJD, 2019 WL 1369928, at *8 (N.D. Cal. Mar. 26, 2019*); Accresa Health LLC v. Hint Health Inc.*, No. 4:18-CV-00536, 2020 WL 3637801, at *12 (E.D. Tex. July 6, 2020) ("The Court recognizes trade secret misappropriation may be based on either a 'use' theory or an 'acquisition by improper means' theory, and alternative theories may be submitted to the jury if supported by the pleadings and evidence.").

[30] *Source Prod. & Equip. Co., Inc. v. Schehr*, No. CV 16-17528, 2019 WL 4752058, at *11 (E.D. La. Sept. 30, 2019) (quoting *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 539 (5th Cir. 1974)).

[31] 18 U.S.C. § 1839 (6).

The plaintiff must disclose its trade secrets.

Pleading Standard

When pleading a DTSA claim, a plaintiff must, of course, satisfy the *Twombly–Iqbal* standard to survive a motion to dismiss. Federal courts have held that the DTSA and a state's Uniform Trade Secret Act "share the same pleading requirements for the identification of trade secrets."[32] To survive a Rule 12(b)(6) motion to dismiss for failure to state a claim, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'"[33] While the plaintiff must disclose the trade secret that he is alleging has been misappropriated under the DTSA, "courts have found allegations to be adequate in instances where the information and the efforts to maintain its confidentiality are described in general terms."[34] Requiring trade secrets to be disclosed in detail in complaints alleging misappropriation would result in the public disclosure of such trade secrets.[35] Courts have found trade secret allegations to be "adequate in instances where the information and the efforts to maintain its confidentiality are described in general terms."[36] Due to the nature of the secrecy requirement inherent in the nature of a trade secret, "a plaintiff need not spell out the details of the trade secret" in a pleading.[37] 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."[38]

The DTSA plaintiff must allege facts sufficient to provide notice to the defendant that the relevant information constitutes a trade secret.[39] "At the pleading stage, alleging categories of trade secrets are sufficiently specific to support a claim under DTSA and

---

[32] *Alta Devices, Inc. v. LG Electronics, Inc.*, 343 F. Supp. 3d 868, 881 (N.D. Cal. 2018).

[33] *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

[34] *Packaging Corp. of Am., Inc. v. Croner*, 419 F. Supp. 3d 1059, 1066 (N.D. Ill. 2020).

[35] *Mission Measurement Corp. v. Blackbaud, Inc.*, 216 F. Supp. 3d 915, 921 (N.D. Ill. 2016).

[36] *Id*. at 920 (citing *Covenant Aviation Sec., LLC v. Berry*, 15 F. Supp. 3d 813, 818 (N.D. Ill. 2014)).

[37] *Alta Devices, Inc.*, 343 F. Supp. 3d at 881 (citing *Autodesk, Inc. v. ZWCAD Software Co.*, No. 5:14-cv-01409-EJD, 2015 WL 2265479, at *5 (N.D. Cal. May 13, 2015)).

[38] *Id*. (citing *Vendavo, Inc. v. Prixe f(x) AG*, No. 17-cv-06930-RS, 2018 WL 1456697, at *4 (N.D. Cal. Mar. 23, 2018)).

[39] 18 U.S.C. § 1836(b)(1).

provide sufficient notice to the defendant."[40] In *Kraus USA, Inc. v. Magarik*, the plaintiff allegedly misappropriated several specific categories of information, "including technical product specifications, information on upcoming designs, sales data, e-commerce data, and other commercially sensitive information including customer lists, vendor relationships, the identity of contractual counterparties, internal cost structure and operating expenses, and e-commerce knowledge."[41] These categories alleged in the complaint were sufficiently specific to survive a motion to dismiss and to provide the defendant with notice of the claims against him.[42]

Kraus relied upon another Southern District of New York case, *Medidata Solutions, Inc. v. Veeva Systems Inc.*, that also held the plaintiff had sufficiently pled its trade secret claim with enough specificity by identifying specific categories of information pertaining to software, marketing, and business plans, such that the defendant was adequately informed of the alleged misappropriation claims brought against him.[43]

Similarly, the District Court of Colorado recently denied a motion to dismiss when the complaint noted various product designs allegedly misappropriated by the defendant, as well as detailed explanations of how the plaintiff had previously modified the designs.[44] In *Luckyshot LLC v. Runnit CNC Shop, Inc.*, the plaintiff alleged that he provided product specifications and drawings to defendant in order for defendant to manufacture the product.[45] The Court denied the defendant's motion to dismiss on grounds that the plaintiff's pleading of specific aspects of the product's design sufficiently identified the trade secret at issue.[46]

In addition to specific categories of trade secrets alleged in a pleading, a plaintiff's allegation that the trade secrets at issue include customer or client information may be sufficient to survive a motion to dismiss in early stages of the litigation.[47] In *Packaging*

---

[40] *Kraus USA, Inc. v. Magarik*, No. 17-CV-6541 (ER), 2020 WL 2415670, at *5 (S.D.N.Y. May 12, 2020) (citing *Medidata Solutions, Inc. v. Veeva Sys. Inc.*, 17 Civ. 589 (LGS), 2018 WL 6173349, at *3 (S.D.N.Y. Nov. 26, 2018)).

[41] *Id*.

[42] *Id*.

[43] *Medidata Solutions*, 2018 WL 6173349, at *3.

[44] *Luckyshot LLC v. Runnit CNC Shop, Inc.*, No. 19-cv-03034-RBJ, 2020 WL 5702281, at *6 (D. Colo. Sep. 24, 2020).

[45] *Id*.

[46] *Id*.

[47] *Packaging Corp. of Am., Inc. v. Croner*, 419 F. Supp. 3d 1059, 1066 (N.D. Ill. 2020).

Corp. of Am., Inc. v. Croner, the plaintiff's complaint alleged trade secret misappropriation of customer purchase histories, customer preferences, and internal pricing processes.[48] The Court found these allegations sufficed to provide the defendant with adequate notice as to the basis of the trade secret claims.[49] The Court dismissed plaintiff's claim on other grounds.[50]

In another case, *ExpertConnect, LLC v. Fowler*, the plaintiff alleged various specific categories of information pertaining to plaintiff's services, including "client lists and client preferences, contract details, expert lists and performance criteria," in addition to the plaintiff pointing to specific documents it alleges to be trade secrets.[51] The Court determined that plaintiff's allegations sufficed to give the defendant adequate notice of the misappropriation claims.[52]

The sufficiency of a disclosure relates to the stage of the litigation.

Generally, the trend is that cases are not dismissed for a lack of specificity in disclosing trade secrets until later stages in the litigation, well past the motion to dismiss phase.[53] The detail required for trade secret actions in early-stage pleadings was also considered in *Parker v. Petrovics*.[54] The *Parker* court provides, "in a trade secret action, the plaintiff bears the burden of demonstrating both that the specific information it seeks to protect is secret and that it has taken reasonable steps to protect this secrecy."[55] Further, the court emphasized that at early stages in litigation, "for a complaint to survive a

---

[48] *Id*. at 1065.

[49] *Id*. at 1066.

[50] *Id*. (plaintiff failed to sufficiently allege that defendant misappropriated).

[51] *ExpertConnect, LLC v. Fowler*, 18 Civ. 4828 (LGS), 2019 WL 3004161, at *4 (S.D.N.Y. July 10, 2019).

[52] *Id*.

[53] *See Luckyshot LLC*, 2020 WL 5702281, at *6 ("[C]ases rejecting trade secret claims for lack of specificity are predominantly at later stages in the litigation process than at a motion to dismiss.") (citing *SBM Site Servs., LLC v. Garrett*, No. 10-CV-00385-WJM-BNB, 2012 WL 628619, at *10 (D. Colo. Feb. 27, 2012)); *Heska Corp. v. Qorvo US, Inc.*, No. 1:19cv1108, 2020 WL 5821078, at *17 (M.D.N.C. Sep. 30, 2020) ("[A] plaintiff can survive a motion to dismiss at the early stages in litigation even if it does not yet know precisely what was taken.") (the court denied defendant's motion to dismiss because the plaintiff's pleadings were sufficient to put defendant on notice of the basis for plaintiff's misappropriation claim, even if plaintiff's pleadings only identified specific prototype versions of a product and did not precisely identify the trade secret).

[54] *Parker v. Petrovics*, 2020 WL 3972761 (N.D. Ala. 2020).

[55] *Id*. at *5 (citing *Am. Red Cross v. Palm Beach Blood Bank, Inc.*, 143 F.3d 1407, 1410 (11th Cir. 1998).

motion to dismiss, it need not contain detailed factual allegations."[56] Rather, the court stated, "it must contain only enough facts to state a claim to relief that is plausible on its face. The factual allegations must be enough to raise a right to relief above the speculative level."[57]

Several cases have addressed the plaintiff's requirement to establish the existence of the allegedly infringed trade secret and to adequately disclose such trade secret prior to the start of discovery.[58] The Ninth Circuit recently reversed the Central District of California for abuse of discretion in denying the plaintiff discovery because genuine disputes of material fact remained as to whether the plaintiff demonstrated that it had protectable trade secrets.[59] Pursuant to Rule 56(d), the plaintiff "had submitted declarations showing that it would receive information necessary to refine its [trade secret] identifications through discovery."[60] "The issue of whether all of the plaintiffs' alleged trade secrets have been publicly disclosed is a factual issue which is the proper subject of discovery."[61]

The Ninth Circuit held that "there is a genuine issue of material fact as to whether [the plaintiff] identified its trade secrets with sufficiently particularity."[62] The court went on to further state that, "at this stage, particularly where no discovery whatsoever had occurred, it is not fatal to [the plaintiff's] claim that its hedging language left open the possibility of expanding its identifications later."[63]

---

[56] *Id*.

[57] *Id*. (citing *Martin v. Auburn Univ. Montgomery*, No. 2:11-cv-715-WHA, 2012 WL 787047, at *1 (M.D. Ala. Mar. 12, 2012)).

[58] *See generally, Inteliclear, LLC v. ETC Global Holdings, Inc.*, 978 F.3d 653 (9th Cir. 2020); *Freeman Inv. Mgmt. Co., LLC v. Frank Russell Co.*, No. 13-CV-2856 JLS (RBB), 2016 WL 5719819 (S.D. Cal. Sep. 30, 2016) (plaintiff failed to plead its misappropriation claims with sufficient specificity following discovery and at the summary judgment phase of litigation) (granting defendant's motion for summary judgment).

[59] *Inteliclear*, 978 F.3d at 664.

[60] *Id*. at 662.

[61] *Id*. (quoting *E. & J. Gallo Winery v. Instituut Voor Landbouw-En Visserijonderzoek*, No. 17-cv-00808-DAD-EPG, 2018 WL 2463869, at *6 (E.D. Cal. June 1, 2018).

[62] *Id*. at 659.

[63] *Id*.

Conclusory assertions of trade secret claims are insufficient.

While alleging specific categories of trade secrets in the pleadings is sufficient to survive a motion to dismiss and provide notice to the defendant, conclusory assertions will not suffice in the pleadings.[64] "Although the complaint need not spell out the details of the trade secret, the complaint must describe the subject matter of the trade secret with sufficient particularity to separate the trade secret from matters of general knowledge in the trade."[65] Other cases emphasize the rule that failing to identify trade secrets in the pleadings with sufficient particularity will result in dismissal of the misappropriation claim under the DTSA.[66] In *Lithero, LLC v. Astrazeneca Pharmaceuticals LP*, the court dismissed plaintiff's misappropriation claim because it only "points to large, general areas of information that plaintiff alleges to have shared with defendant but does not identify what the trade secrets are within those general areas."[67] The court explained, "without knowing, for example, what about [defendant's] training process is a trade secret, defendant is not put on sufficient notice of what it is accused of misappropriating."[68] Similarly, in *Vendavo, Inc. v. Price f(x) AG*, the plaintiff merely alleged its "purported trade secrets in broad, categorical terms, more descriptive of the types of information that generally *may* qualify as protectable trade secrets than as any kind of listing of particular trade secrets [plaintiff] has a basis to believe actually were misappropriated here."[69] Thus, the court granted the motion to dismiss plaintiff's misappropriation claims on the grounds that the complaint's "conclusory and generalized allegations" were insufficient.[70]

---

[64] *See Prov. Int'l, Inc. v. Rubens Dalle Lucca*, No. 8:19-cv-978-T-23AAS, 2019 WL 5578880, at *3 (M.D. Fla. Oct. 29, 2019) (granting motion to dismiss plaintiff's misappropriation claim on grounds that conclusory assertions of the defendant's alleged misappropriation of "proprietary practices" and "operating procedures" was insufficient to provide notice to the defendant of the trade secrets that were allegedly violated).

[65] *Id*.

[66] *See Lithero, LLC v. Astrazeneca Pharms. LP*, No. 19-2320-RGA, 2020 WL 4699041, at *2 (D. Del. Aug. 13, 2020); *see also Vendavo, Inc. v. Price f(x) AG*, No. 17-cv-06930-RS, 2018 WL 1456697, at *4 (N.D. Cal. Mar. 23, 2018).

[67] *Lithero*, 2020 WL 4699041, at *2.

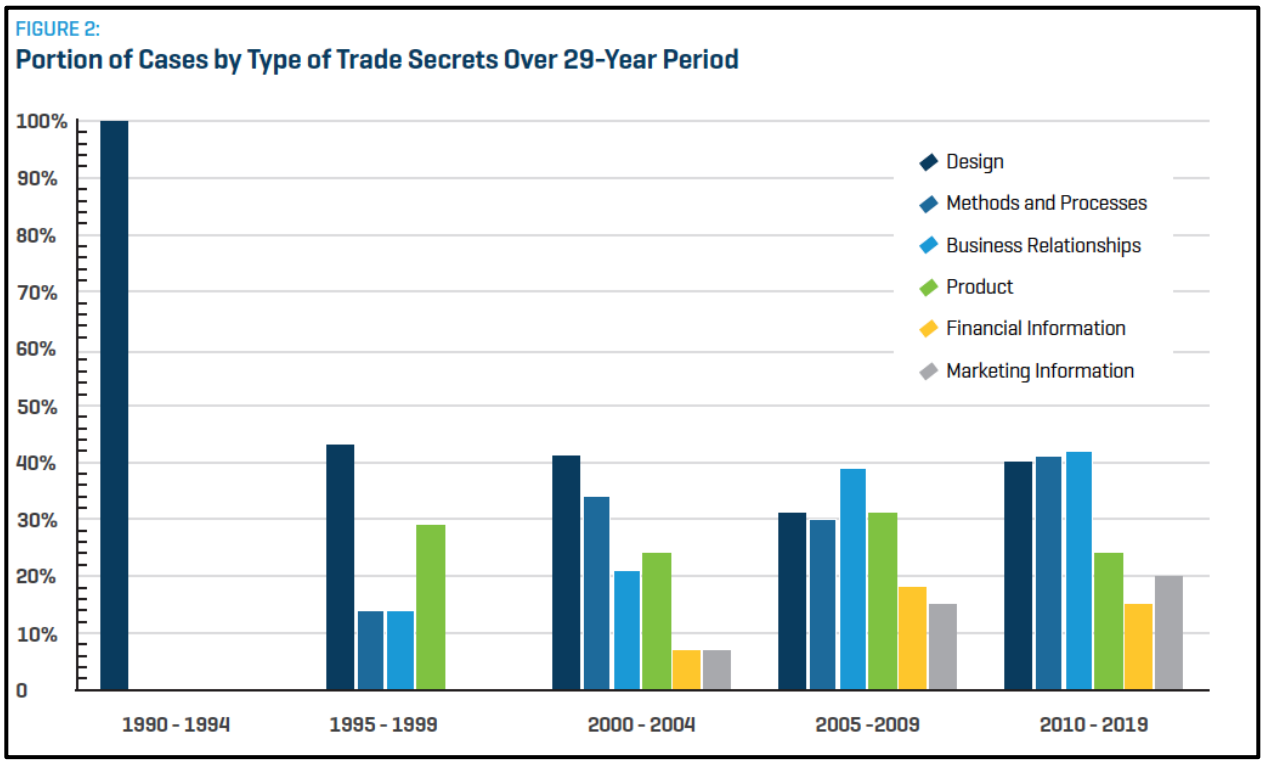
[68] *Id*.

[69] *Vendavo*, 2018 WL 1456697, at *4 (italics in original).

[70] *Id*.

Trade secrets examples

Trade secrets take many forms. In the first year of the DTSA's enactment, most (approximately 58%) trade secret cases involved customer lists and business information.[71] Fewer cases (approximately 40%) involved technical information, and even fewer (approximately 8%) involved a secret formula.[72] This is part of a larger trend in trade secret litigation toward more employment-related disputes focused on customer information and business relationships:



(Jeffrey Mordaunt et al., *Trends in Trade Secret Litigation Report 2020,* Figure 2 at 27 (Stout 2020).

[71] David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 Wake Forest L. Rev. 105, 145–46 (2018).

[72] *Id*.

Table 3. Type of the Alleged Trade Secrets

	1950–2007	2008
Formulas	4% (12)	9% (11)
Technical information and know-how	46% (126)	35% (42)
Software or computer programs	11% (29)	10% (12)
Customer Lists	32% (86)	31% (38)
Internal business information	31% (84)	35% (42)
External business information	2% (5)	1% (1)
"Combination" trade secrets	2% (5)	1% (1)
"Negative" trade secrets	1% (2)	0
Other or unknown	5% (14)	9% (11)

(David S. Almeling et al, *Statistical Analysis of Trade Secret Litigation*, 45 Gonzaga L. Rev. 291, 304).

Specific examples of information that courts have found constitute trade secrets under the DTSA include:

- source code;[73]
- manufacturing procedures;[74]
- customer lists;[75]

[73] *WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834, 847 (N.D. Cal. 2019), modified in part, 5:18-CV-07233-EJD, 2019 WL 5722620 (N.D. Cal. Nov. 5, 2019) ("Courts have found that source code can receive trade secret protection. WeRide represents that many engineers developed the source code over 18 months with investments of over $45 million. The investment and development make the source code confidential and proprietary to WeRide, giving it an advantage over competitors. The source code has value. Huang asserts during WeRide's 'earlier startup days,' it derived much of its source code from open source code, but this does not mean that the source code allegedly misappropriated a year later was not confidential.") (citing *Integral Dev. Corp. v. Tolat*, 675 Fed. App'x 700, 703 (9th Cir. 2017); *Altavion, Inc. v. Konica Minolta Sys. Lab., Inc.*, 226 Cal. App. 4th 26, 60 (Cal. Ct. App. 2014)).

[74] *Par Pharm., Inc. v. QuVa Pharma, Inc.*, 764 F. App'x 273, 278 (3d Cir. 2019) ("1Par demonstrated a reasonable likelihood that the APS Plan was a trade secret. The Plan discloses aspects of Par's economically valuable FDA-mandated sterile manufacturing procedures. . . . 'while some individual elements of the APS Plan may be known in the industry, Par's combination of the elements' in its own process likely constitutes a trade secret itself."); *see also Navigation Holdings, LLC v. Molavi*, 445 F. Supp. 3d 69, 77 (N.D. Cal. 2020) (anodizing process).

[75] *Albert's Organics, Inc. v. Holzman*, 445 F. Supp. 3d 463, 472–73 (N.D. Cal. 2020) ("Courts have frequently held that customer-related information qualifies as a trade secret, especially if a plaintiff has spent 'considerable time, effort, and resources,' in developing some of that information.") (citing *MAI Sys. Corp. v. Peak Comput., Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) (holding that, under CUTSA, soliciting of customers

- data compilation;[76]
- customer strategies and pricing;[77]

Reasonable measures to protect trade secrets

The second most common basis for a court to grant summary judgment in a trade secret case is for the plaintiff's failure to take adequate measures to protect its trade secret:

Figure 20: Ownership Findings for Cases Terminated from 2010 to 2019

Findings	Default Judgment	Consent Judgment	Judgment on the Pleadings	Summary Judgment	Judgment as a Matter of Law	Trial	Any Judgment Event
Ownership / Validity	0	4	6	20	53	0	83
Failure to Identify Trade Secret	0	0	11	101	11	1	156
Failure to Maintain Secrecy	0	0	23	74	18	3	116
Generally Known / Readily Ascertainable	0	0	4	34	13	1	72
No Ownership / Validity: Wrong Entity	0	0	7	10	2	0	19

(Rachel Bailey, *Lex Machina Trade Secret Litigation Report 2020* at 18).

Many cases focus their analysis on internal security measures, protecting information among employees, in part, because most trade secret cases involve an employee or business partner:

---

of former firm constituted trade secret misappropriation); *see also H.Q. Milton, Inc. v. Webster*, No. 17-CV-06598-PJH, 2017 WL 5625929, at *3 (N.D. Cal. Nov. 22, 2017) (finding "customer list and contact information, sales leads, customer interests, and [plaintiff's] proprietary pricing" constituted trade secrets); *Henry Schein, Inc. v. Cook*, No. 16-03166C, 2016 WL 3418537, at *4 (N.D. Cal. June 22, 2016) (holding customer information, margins, and profit percentages used to gain an advantage over competitors were protectable as trade secrets); *Brocade Commc'n Sys. Inc. v. A10 Networks, Inc.*, 873 F. Supp. 2d 1192, 1214 (N.D. Cal. 2012) ("[C]ustomer-related information including ... pricing guidelines ... and customers' business needs/preferences ... is routinely given trade secret protection.")).

[76] *Compulife Software Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020) (data compilation of life insurance quotes, although each quote was publicly available, compilation was largen enough to qualify for protection)

[77] *API Americas Inc. v. Miller*, 380 F. Supp. 3d 1141 (D. Kan. 2019).

Table 2. Identity of Alleged Misappropriator

	1950–2007	2008
Employee or former employee	52% (142)	59% (71)
Business partner	40% (109)	31% (37)
Unrelated third party	3% (8)	9% (10)
Other or unknown	7% (19)	5% (6)

(David S. Almeling et. al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291, 292 (2009)).

Although it is generally a fact question for the jury whether the plaintiff proved it took sufficient measures to protect its trade secrets,[78] key issues in motions to dismiss and for summary judgment include:

- Physical and electronic security systems;
- Non-disclosure agreements; and
- Limiting the number of people who know the information.

"Reasonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required."[79] In some instances, pleadings that reference confidentiality agreements and internal control measures have been sufficient.[80]

One key issue that arises frequently is whether information disclosed to a third party must be marked as "confidential" to retain its trade secret status: "[A]n employer's failure to mark documents as confidential or trade secret 'precludes in many cases trade secret protection for those materials,'"[81] but "[if] the employee knows or has reason to

[78] *See, e.g., Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 724 (7th Cir. 2003) (whether measures taken to protect trade secrets were reasonable is generally a question of fact for the jury, and only in extreme cases can be decided as a matter of law).

[79] *AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 974 (8th Cir. 2011).

[80] *Deluxe Fin. Servs., LLC v. Shaw*, No. 16-3065 (JRT/HB), 2017 WL 3327570 at *3 (D. Minn. Aug. 3, 2017); *Signal Fin. Holdings LLC v. Looking Glass Fin. LLC*, 17 C 8816, 2018 WL 636769, at *4 (N.D. Ill. Jan. 31, 2018) (marking documents confidential and requiring third parties to sign an NDA sufficient to warrant trade secret protection); *Huawei Techs. Co. v. Motorola, Inc.*, No. 11-cv-497, 2011 WL 612722, at *9 (N.D. Ill. Feb. 22, 2011) (same).

[81] *Mattel, Inc. v. MGA Ent., Inc.*, 782 F. Supp. 2d 911, 959 (C.D. Cal. 2011).

know that the owner intends or expects the information to be secret, confidentiality measures are sufficient."[82]

Examples of adequate measures:

Perhaps the quintessential example of a trade secret is the formula for Coca Cola. Coca Cola Bottling Co. has described the following measures it takes to protect its trade secrets:

> (1) storing the sole written versions of the formulas in a vault in Atlanta;
> (2) establishing a policy that only two employees may know the formulas at any given time;
> (3) maintaining confidentiality regarding the identities of the two employees who know the formulas;
> (4) allowing only the two employees who know the formulas to oversee production of Coca-Cola's secret ingredients; and
> (5) barring the two employees from flying on the same plane at the same time.[83]

In more routine cases, pleadings that identify internal control measures like employee handbooks and password protected databases may be sufficient to survive a motion to dismiss.[84] Other cases have found reasonable measures existed when the information was not only protected by a confidentiality agreement, but the plaintiff also demanded return or destruction of its information following the terms of the agreement.[85]

---

[82] *Lasermaster Corp. v. Sentinel Imaging*, 931 F. Supp. 628, 635 (D. Minn. 1996).

[83] *Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co.*, 107 F.R.D. 288, 294 (D. Del. 1985).

[84] *ATS Grp., LLC v. Legacy Tank & Indus. Servs. LLC*, 407 F. Supp. 3d 1186, 1199–200 (W.D. Okla. 2019) (employee handbook required confidentiality of business information and prohibited disclosure of trade secrets; corporate information on computers was password protected); *see also Par Pharm., Inc. v. QuVa Pharma, Inc.*, 764 F. App'x 273, 278 (3d Cir. 2019) ("Par took reasonable steps to protect the secrecy of its plan through the use of non-disclosure agreements and appropriate facility security measures."); *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 866 (N.D. Ill. 2001) (granting preliminary injunction where plaintiff only provided information to employees on a need-to-know basis, maintained the security of the information through "such means as limited access and password-protected computer databases," and required employees to sign employment agreements or acknowledge the receipt of employee handbooks that contained non-disclosure clauses).

[85] *Zoppas Indus. de Mexico, S.A. de C.V. v. Backer EHP Inc.*, CV 18-1693-CFC, 2019 WL 6615421, at *3 (D. Del. Dec. 5, 2019), report and recommendation adopted, CV 18-1693-CFC, 2020 WL 205485 (D. Del. Jan. 14, 2020).

For electronically stored information, reasonable measures include "[using an] access-limited, password-protected server and that there was a limited group of employees with that access to the server[.]"[86] Employers also can protect trade secrets by using tailored "access profiles," limiting its computer users to only access appropriate company information, and prohibiting employees from saving confidential information on public portions of the company's computer network.[87] And employers can prohibit "employees from forwarding confidential information to a personal email account or by email generally without proper labeling and authorization."[88]

More sophisticated measures to protect electronic information include restricting access to employees who are physically located at the office or are logged into a proprietary network through a password protected VPN.[89] Additionally, electronic information can be encrypted, requiring an additional layer of password protection to access.[90]

---

[86] *S. Field Maint. & Fabrication LLC v. Killough*, 2:18-CV-581-GMB, 2019 WL 360515, at *4 (M.D. Ala. Jan. 29, 2019) (also noting the defendant "was informed of the need to maintain the confidentiality of the information contained within the specific documents at issue.").

[87] *Magnesita Refractories Co. v. Tianjin New Century Refractories Co.*, No. 1:17-CV-1587, 2019 WL 1003623, at *10 (M.D. Pa. Feb. 28, 2019) (also noting "Employees needing access to Magnesita's confidential information must execute nondisclosure agreements or secrecy agreements."); *see also Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1135–38 (N.D. Ill. 2019) ("Likewise, it limited access to the Salesforce database—where Plaintiff kept all the documents containing the information examined above with the exception of financial data—to only those employees whose jobs required them to access it."); *SKF USA Inc. v. Bjerkness*, 2010 WL 3155981, at *6 (N.D. Ill. Aug. 9, 2010) (finding plaintiff took reasonable efforts to maintain the secrecy of its information where it (1) required employees to sign secrecy agreements, (2) implemented password protection for important files and granted access to different sets of documents based on employees' duties, (3) instructed employees not to share its databases with customers, (4) and only shared information with customers after having the customer sign a nondisclosure agreement).

[88] *Magnesita Refractories Co.*, 2019 WL 1003623, at *10.

[89] *WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834, 847 (N.D. Cal. 2019), modified in part, 5:18-CV-07233-EJD, 2019 WL 5722620 (N.D. Cal. Nov. 5, 2019) (also noting that "WeRide requires all of its employees to sign the PIIA, which includes provisions protecting WeRide's confidential information.").

[90] *See id.*; *see also Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1135–38 (N.D. Ill. 2019) ("requiring laptops, servers, *etc.* to be encrypted using complex passwords as well as multi-factor authentication to access its network remotely.").

Examples of inadequate measures

Although there are myriad factors courts have considered to determine whether trade secrets were adequately protected, likely the most important factor is the existence of confidentiality agreements.[91]

The Second Circuit detailed examples of inadequate measures to protect trade secrets in *Mason v. Amtrust Fin. Servs., Inc.*, when reviewing the district court's decision to deny a preliminary injunction.[92] The first issue the court addressed was that even to the extent an alleged confidentiality agreement had, in fact, existed, "it was unreasonable for [the plaintiff] not to have this agreement described with particularity in his Employment Agreement or a standalone licensing agreement."[93] Additionally, the court described it as "careless" and not an adequate measure for the plaintiff to send purported trade secrets from a personal email account without labelling the material as "confidential".[94] The Second Circuit upheld the district court's ruling finding the plaintiff failed to use adequate measures even though the plaintiff:

- referred to trade secret "as his personal and proprietary property";
- insisted that the trade secret "be kept off of [the defendant's] central operating system and servers"; and
- monitored who used the trade secret.[95]

Ultimately, the court of appeals characterized the record in *Mason* by stating the plaintiff "had little control over who used" the trade secret at issue.[96]

In *Dichard v. Morgan*, the District Court for New Hampshire dismissed a claim where the claimant "failed to adequately plead that it took reasonable measures to preserve the secrecy of the information" and provided significant insight into why the pleading failed to reach that threshold.[97] For example, the court noted the claimant failed to allege:

---

[91] *See, e.g.*, *Farmers Edge Inc. v. Farmobile, LLC*, 970 F.3d 1027, 1033 (8th Cir. 2020).

[92] *Mason v. Amtrust Fin. Servs., Inc.*, No. 20-1256, 2021 WL 772298, at *2–3 (2d Cir. Mar. 1, 2021).

[93] *Id*.

[94] *Id*.

[95] *Id*.

[96] *Id*.

[97] No. 17-CV-00338-AJ, 2017 WL 5634110, at *2–4 (D.N.H. Nov. 22, 2017).

- that its "computer system or the documents in question had any particular security, such a restricted server, password protection, or encryption."[98]
- "that its employees were trained regarding the sensitive nature of this information or that it otherwise made those who used the information subject to confidentiality provisions and limitations, such as nondisclosure agreements."[99]
- "that it implemented any policies or procedures regarding the preservation of the information at issue."[100]

Although the court was unpersuaded by the particular measures alleged, it did acknowledge "the possibility that a company's size and sophistication might have some bearing on whether the measures a company took were reasonable under the circumstances." [101]

In another case where the plaintiff failed to take adequate measures to safeguard information, the Northern District of Illinois stated "the company's failure to require those with access to its supposed trade secrets to enter into non-disclosure and confidentiality agreements has to be counted among the most fundamental omissions by the company."[102] A "vague, generalized admonition" to not discuss business outside of

---

[98] *Id*. (citing *Grow Fin. Fed. Credit Union v. GTE Fed. Credit Union*, No. 8:17-cv-1239-T-30JSS, 2017 WL 3492707, at *3 (M.D. Fla. Aug. 15, 2017); *Heralds of Gospel Found., Inc. v. Varela*, No. 17-22281-CIV, 2017 WL 3868421, at *5 (S.D. Fla. June 23, 2017); *Sleekez, LLC v. Horton*, No. CV 16-09-BLG-SPW-TJC, 2017 WL 1906957, at *4 (D. Mont. Apr. 21, 2017), *report and recommendation adopted*, No. CV 16-09-BLG-SPW, 2017 WL 1929473 (D. Mont. May 9, 2017); *Prot. Techs., Inc. v. Ribler*, No. 3:17-cv-144-LRH-WGC, 2017 WL 923912, at *2 (D. Nev. Mar. 8, 2017)).

[99] *Id*. (citing *Grow Fin. Fed. Credit Union*, 2017 WL 3492707, at *3; *Syntel Sterling Best Shores Mauritius Ltd.*, 2016 WL 5338550, at *6; *Heralds of Gospel Found., Inc.*, 2017 WL 3868421, at *5).

[100] *Id*. (citing *Deluxe Fin. Servs., LLC*, 2017 WL 3327570, at *3).

[101] *Id*.

[102] *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 898–903 (N.D. Ill. 2019) ("Failure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims.") (citing *Arjo, Inc. v. Handicare USA, Inc.*, No. 18 C 2554, 2018 WL 5298527, at *4 (N.D. Ill. Oct. 25, 2018) ("Pricing information shared freely with customers without confidentiality requirements is insufficiently secret to garner protection."); *Dryco, LLC v. ABM Industries, Inc.*, No. 07 CV 0069, 2009 WL 3401168, at *6 (N.D. Ill. Oct. 16, 2009) (concluding that plaintiff failed to protect alleged trade secrets because plaintiff did not require confidentiality agreements or label information confidential); *Conxall Corp. v. Iconn Sys., LLC*, 406 Ill. Dec. 813, 61 N.E.3d 1081, 1093 (Ill. App. Ct. 2016) (holding that where plaintiff could not prove it had a confidentiality agreement, "its trade secret claim...suffered a total failure of proof as to a critical element, namely that the designs were a trade secret"); *Liebert Corp. v. Mazur*, 827 N.E.2d 909, 923–24 (2005)

work failed to "define, delineate, or specify which information was considered confidential."[103] The court also emphasized the plaintiff " did nothing to train or instruct employees as to their obligation to keep certain categories of information confidential."[104] And the court faulted the plaintiff's "benign neglect benign neglect when employees left the company":

> Although employees were instructed to return CGW property when they separated from CGW, they were not asked whether they possessed any of the information at issue or instructed to return or delete such information. Requiring that departing employees or contractors return company property when their relationship with the company ends is a routine, normal business practice, but precautions must go "beyond normal business practices" for the information to qualify for trade secret protection.[105]

Additionally, when dealing with electronic information, the plaintiff "assigned the same password to many [of its] employees to facilitate their access to the shared drive, files were not encrypted, and there were no restrictions on employees' ability to access, save, copy, print, or email the information at issue."[106] Finally, the court concluded that

---

(affirming finding of no trade secrets where plaintiff did not, among other things, require employees to sign confidentiality agreements)).

[103] *Abrasic 90 Inc.*, 364 F. Supp. 3d at 898–903 (citing *Gillis Associated Indus., Inc. v. Cari-All, Inc.*, 564 N.E.2d 881, 885–86 (1990) (noting that plaintiff's failure to specify which information it deemed confidential was inadequate to protect subset of information)).

[104] *Id*. (citing *Jackson v. Hammer*, 274 Ill. App. 3d 59, 69, 653 N.E.2d 809, 817 (1995) (denying trade secret status where "record contain[ed] no evidence that plaintiff took steps to explain the secrecy or confidentiality of the lists to his employees"); *Gillis*, 564 N.E.2d at 886 (concluding that information did not qualify as trade secret based, in part, on plaintiff's failure to conduct "entrance and exit interviews imparting the importance of confidentiality")).

[105] *Id*. (citing *Weather Shield Mfg., Inc. v. Drost*, 2018 WL 3824150, at *3 (W.D. Wis. Aug. 10, 2018) (internal quotation marks and citation omitted)); see also *See CMBB LLC v. Lockwood Mfg., Inc.*, 628 F. Supp. 2d 881, 885 (N.D. Ill. 2009) (The company's "failure to *ensure* that [defendant]'s laptop was stripped of [allegedly protected Information] when she left the company goes to show that it did not treat such Information as confidential or a trade secret.").

[106] *Id*. (citing *Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005) (denying trade secret protection and distinguishing from another case where adequate protections were used such as "limiting computer access through the use of passwords, allowing only managers the ability to print [allegedly protected] files, limiting internet and e-mail availability of the information, and keeping physical copies of the information in a file cabinet in an office in which permission was necessary to access the cabinet"); *Fleetwood Packaging v. Hein*, 2014 WL 7146439, at *4 (N.D. Ill. Dec. 15, 2014) ("Customer lists can constitute

what may have been "the most telling evidence" was that the plaintiff "took no measures to protect that information that were in any way different (much less more exacting) than the steps that it took to protect information that was indisputably not a trade secret."[107]

Regardless of the general measures taken to protect information, if that information is ever disclosed without following protocols to protect its confidentiality, then the court may find the information is not adequately protected. [108] Similarly, even if information is generally well protected, failing to protect it in some instances, like by allowing employees without express confidentiality agreements to retain the information on their personal electronic devices may preclude its designation as a trade secret.[109]

Marking materials as "confidential"

A reoccurring issue is whether confidential information must be labelled "confidential" to maintain its trade secret status. Some courts treat this as a bright-line rule, while others provide a more flexible approach. For example, in *Field Maint. &*

---

trade secrets only where reasonable steps to preserve secrecy have been taken, such as encrypting the lists or requiring review in only restricted-access rooms."); *Starsurgical, Inc. v. Aperta, LLC*, 40 F. Supp. 3d 1069, 1082 (E.D. Wis. 2014) (noting that "normal business practices like restricting access and requiring passwords" were not even enough for trade secret protection) (internal quotation marks and citation omitted); *Arko Plumbing Corp. v. Rudd*, 230 So. 3d 520, 529–30 (Fla. Dist. Ct. App. 2017) (finding that maintaining customer pricing information in a password-protected file and limiting access to two employees were "the sorts of reasonable efforts to maintain secrecy required by the trade secret statute")).

[107] *Id*. (citing *Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC*, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018) (rejecting trade secret claim where plaintiff did "nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information")).

[108] *Temurian v. Piccolo*, 18-CV-62737, 2019 WL 1763022, at *11 (S.D. Fla. Apr. 22, 2019), reconsideration denied, 18-CV-62737, 2019 WL 2491781 (S.D. Fla. June 14, 2019) (despite password protection and restrictions to essential personnel, the plaintiff failed to take adequate measures to protect the secrecy of information because it disclosed the information to third parties without a confidentiality agreement in place) (quoting *M.C. Dean, Inc. v. City of Miami Beach, Fla.*, 199 F. Supp. 3d 1349, 1353 (S.D. Fla. 2016) ("[d]isclosing the information to others who are under no obligation to protect the confidentiality of the information defeats any claim that the information is a trade secret.")).

[109] *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279, 1299–301 (11th Cir. 2018) ("Yellowfin states that the information is held within its computer system which requires a username and password to access, is accessible by fewer than five percent of the company's employees, and is not accessible by or shared with third parties. . . . But Yellowfin compromised the efficacy of these measures by encouraging Barker to keep the Customer Information on his cellphone and personal laptop. . . . Thus, at bottom, Yellowfin's efforts to secure the Customer Information rest upon a purported "implicit understanding" between Yellowfin and Barker that the information was to be kept confidential.").

Fabrication LLC v. Kilough, the Middle District for Alabama held that the plaintiff had taken reasonable measures to protect the stolen trade secrets, even though the plaintiff company had not marked the document at issue as "confidential."[110] But in *Call One, Inc. v. Anzine*, the Northern District of Illinois found the plaintiff failed to take adequate measures because the company-plaintiff had a policy to mark confidential and trade secret documents as such, yet the information purportedly stolen was not marked.[111]

Interstate commerce

Most courts to address the issue hold that the DTSA also requires pleading a jurisdictional element, but "[b]ecause the DTSA was enacted only recently, there is limited case law relating to whether pleading this specific aspect of a DTSA claim is required."[112] It is clear, however, that if the issue is raised, to invoke the DTSA, the trade secret at issue must be "related to a product or service used in, or intended for use in, interstate or foreign commerce."[113] And the "interstate commerce" requirement is jurisdictional.[114] Accordingly, many courts hold that plaintiffs must plead a nexus to interstate commerce:

> Plaintiff must demonstrate that the trade secret implicates interstate or foreign commerce. Defendant does not dispute this element and the Court finds the pleading sufficient. Here, the purported information relates to services used and intended for use in interstate and foreign commerce because it contains business plans, procurement strategies and subcontractor and vendor relationships.[115]

---

[110] No. 2:18-cv-581-GMB (M.D. Ala. Jan. 29, 2019) ("[U]nder all the circumstances, if the employee knows or has reason to know that the owner intends or expects the information to be secret, confidentiality measures are sufficient.").

[111] 2018 WL 2735089 (N.D. Ill. June 7, 2018).

[112] *Wells Lamont Indus. Group LLC v. Richard Mendoza & Radians, Inc.*, 17 C 1136, 2017 WL 3235682, at *3 (N.D. Ill. July 31, 2017).

[113] 18 U.S.C. § 1836(b)(1).

[114] *United States v. Agrawal*, 726 F.3d 235, 244–45 (2d Cir. 2013); *M.C. Dean, Inc. v. City of Miami*, 199 F.Supp.3d 1349, 1353 (S.D. Fla. 2016); *Donatello v. County of Niagara*, 15–CV–39V, 2016 WL 3090552, at *5 (W.D.N.Y. June 2, 2016); *EmployBridge, LLC v. Riven Rock Staffing, LLC*, Civ. No. 16-833, 2016 WL 7438044, at *2 (D.N.M. Aug. 17, 2016).

[115] *Space Sys./Loral, LLC v. Orbital ATK, Inc.*, 306 F. Supp. 3d 845, 854–55 (E.D. Va. 2018); *see also Hawkins*, 301 F. Supp. 3d at 658–59, 2017 WL 4613664, at *6 (holding that the plaintiff satisfied interstate commerce

The pleading standard for the nexus to interstate commerce is relatively low. For example, the Northern District of Illinois held that the plaintiff established a jurisdictional nexus by alleging the plaintiff had scheduled a meeting to do business across state lines, even though that meeting was subsequently cancelled.[116] Based on this meeting, the court held it was reasonable to infer the plaintiff's goods, and thus trade secrets, were intended for use in interstate commerce.[117]

Similarly, the Eastern District of Louisiana held that the plaintiff established a jurisdictional nexus by alleging "[the plaintiff] is headquartered in Louisiana but operates in other states, and regularly transacts business in states other than Louisiana, including in person and by phone, internet, and mail. [The plaintiff's] trade secrets relate to this business and are used by CLS in interstate commerce."[118] Additionally, in that case the plaintiff "provided the Court with its customer list, which includes several out of state customers. As a result, to the extent Plaintiffs are required to plead a jurisdictional nexus in order to invoke the DTSA's protections, Plaintiffs have adequately done so."[119]

Thus, to the extent the plaintiff must plead a nexus to interstate commerce, the pleading standard is low: as one court explained the court will obtain jurisdiction unless the claimed nexus is "wholly insubstantial or frivolous."[120]

---

element where trade secret contained information related to commerce with other developers, marketing plans, and feedback with potential customers).

[116] *Wells Lamont Industry Group LLC*, 2017 WL 3235682, at *3; *see also Ruby Slipper Cafe, LLC v. Belou*, CV 18-1548, 2019 WL 1254897, at *5 (E.D. La. Mar. 19, 2019) ("To prevail on a DTSA claim, a plaintiff must prove: (1) the existence of a trade secret; (2) the misappropriation of the trade secret by another; and (3) the trade secret's relation to a good or service used or intended for use in interstate or foreign commerce.").

[117] *Wells Lamont Industry Group LLC*, 2017 WL 3235682, at *3.

[118] *Complete Logistical Services, LLC v. Rulh*, 350 F. Supp. 3d 512, 520 (E.D. La. 2018).

[119] *Id*.; *see also Officia Imaging*, 2018 WL 6137183, at *7 (in a case involving a customer database containing information on pricing and sales, the allegation that products were shipped from Nevada to California alone satisfied the interstate commerce requirement).

[120] *Yager v. Vignieri*, 16CV9367(DLC), 2017 WL 4574487, at *2 (S.D.N.Y. Oct. 12, 2017) (citing *Southern New England Telephone Co. v. Global NAPs Inc.*, 624 F.3d 123, 132 (2d Cir. 2010)).

Direct and indirect misappropriation

Plaintiffs can allege direct or indirect misappropriation of trade secrets. Direct misappropriation is when the defendant obtained the trade secret directly from the plaintiff; indirect misappropriation is when the defendant takes the trade secret from someone other than the plaintiff.[121] To state a claim for indirect misappropriation, the plaintiff must show the defendant:

> (a) knew or had reason to know before the use or disclosure that the information was a trade secret and knew or had reason to know that the disclosing party had acquired it through improper means or was breaching a duty of confidentiality by disclosing it; or
>
> (b) knew or had reason to know it was a trade secret and that the disclosure was a mistake."[122]

Extraterritoriality

Generally, the DTSA only applies to misappropriation occurring within the United States.[123] But courts have extraterritorial jurisdiction when:

> (1) the offender is a …citizen …of the United States …; or
>
> (2) an act in furtherance of the offense was committed in the United States.[124]

In *Inventus Power, Inc. v. Shenzhen Ace Battery Co., Ltd.*, the Northern District of Illinois found acts in furtherance of the offense were committed in the United States when:

- "the stolen materials originated in Woodridge, Illinois and were transferred to the employees who now work at [the defendant] at those employees' request, via shared servers or email. "
- "[The Defendant] marketed and sold in the United States the battery products for which the trade secrets were allegedly taken. In particular,

[121] *Navigation Holdings, LLC v. Molavi*, 445 F. Supp. 3d 69, 78–79 (N.D. Cal. 2020).

[122] *Id*.

[123] 18 U.S.C. § 1837(2).

[124] *Id*.

> a few months after the first known incident of mass downloading in early July 2019, [the defendant] attended a battery technology trade show in Salt Lake City to market and sell such battery products."[125]

Although the statute does not define "act in furtherance," the Eastern District of Texas interpreted it to be consistent with the common law definition in the conspiracy context to mean:

> It is not necessary that an overt act be the substantive crime charged in the indictment as the object of the conspiracy. Nor, indeed, need such an act, taken by itself, even be criminal in character. The function of the overt act in a conspiracy prosecution is simply to manifest that the conspiracy is at work, and is neither a project still resting solely in the minds of the conspirators nor a fully completed operation no longer in existence.[126]

Other issues

Employment agreements and whistleblower immunity

The DTSA does not prohibit, or create a private right of action for, certain conduct specifically covered in exceptions listed in 18 U.S.C. § 1833.[127] Exceptions exist for lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State.[128] The statute also provides immunity for liability for a confidential disclosure of a trade secret to the government or included in a court filing.[129] The immunity extends to criminal or civil liability "under any Federal or State trade secret law" for disclosure of a trade secret that (i) is made "in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney" and is "solely for the purpose of reporting or investigating a suspected violation of law"; or (ii) is made in

---

[125] *Inventus Power, Inc. v. Shenzhen Ace Battery Co., Ltd.*, 20-CV-3375, 2020 WL 3960451, at *7 (N.D. Ill. July 13, 2020).

[126] *Luminati Networks Ltd. v. BIScience Inc.*, 2:18-CV-00483-JRG, 2019 WL 2084426, at *9–10 (E.D. Tex. May 13, 2019) (quoting *Yates v. United States*, 354 U.S. 298, 334 (1957)); *see also Motorola Sols., Inc. v. Hytera Communications Corp. Ltd.*, 436 F. Supp. 3d 1150, 1165 (N.D. Ill. 2020).

[127] 18 U.S.C. § 1833.

[128] 18 U.S.C. § 1833(a)(1).

[129] 18 U.S.C. § 1833(b)(1).

a complaint or other document filed in a lawsuit or other proceeding, if the filing is sealed.[130]

An employee's (defined to include contractors or consultants) limited disclosure of a trade secret is also excepted from liability if the employee is filing a retaliation lawsuit against his employer for reporting a suspected violation of law.[131] The exception applies if the employee discloses the trade secret to his attorney and uses the information in the court proceeding, as long as any documents containing the trade secret are filed under seal and the trade secret is otherwise disclosed, unless pursuant to court order.[132]

It is important for employers to provide notice of the whistleblower immunity to preserve their ability to recover exemplary damages and attorneys' fees against an employee under the DTSA.[133] An employer forfeits these valuable remedies under the DTSA in litigation against an employee who was not afforded notice of the immunity.[134] Notice of whistleblower immunity must be provided to employees in any contract or agreement with the employee that governs the use of trade secret or confidential information.[135] Compliance may be achieved if the employer provides a cross-reference to a policy document to the employee that sets out the employer's reporting policy for a suspected violation of law.[136]

Most courts confronted with an employee's claim of immunity consider immunity to be an affirmative defense that cannot be addressed through a motion to dismiss pursuant to Rule 12(b)(6).[137] Those courts note the reluctance "to dismiss complaints based on affirmative defenses at the pleading stage before any discovery has been conducted."[138] Dismissal at the 12(b)(6) stage is possible under the right circumstances—

---

[130] *Id.*

[131] 18 U.S.C. § 1833(b)(2).

[132] *Id.*

[133] 18 U.S.C. § 1833(b)(3).

[134] *Id.*

[135] 18 U.S.C. § 1833(b)(3)(A).

[136] 18 U.S.C. § 1833(b)(3)(B).

[137] *See, e.g., FirstEnergy Corp. v. Pircio*, Case No. 1:20-cv-1966, 2021 WL 857107 at * 7 (N.D. Ohio Mar. 8, 2021) ("Without question, immunity constitutes an affirmative defense.").

[138] *Id.*

if "the plaintiff's own allegations show that a defense exists that legally defeats the claim for relief."[139]

That is precisely what occurred in *First Energy Corp. v. Pircio*, a recent Northern District of Ohio case.[140] There, an employee of a company that had provided audit services to a business implicated in a scandal involving the indictment of the then-Speaker of the Ohio House downloaded certain files about that business and provided them to a lawyer who, in turn, provided them to the SEC.[141] The former employer asserted, among other things, a DTSA claim and State law misappropriation claim against the employee.[142] The employee moved to dismiss the Federal and State trade secret claims on the basis of immunity.[143] Although the court noted that courts generally cannot grant motions to dismiss on the basis of a defense, it acknowledged that dismissal is proper where the plaintiff has anticipated the defense and explicitly addressed it in the pleadings.[144] Dismissal was appropriate under the facts of this case: "This case presents the unusual circumstance where Plaintiffs' own pleadings demonstrate the applicability of the immunity defense asserted under the Defend Trade Secrets Act. Plaintiffs attached to and incorporated into the complaint materials anticipating the defense and establishing its availability as a matter of law . . . Plaintiffs' briefing acknowledges as much . . . Indeed, counsel for [employee] whose letter Plaintiffs incorporated into the pleadings, tracked the language of Section 1833(b)."[145]

The Eastern District of Pennsylvania reached a similar result in *Christian v. Lannet Co.*[146] In that case, a former employee sued her former employer for discrimination.[147] During the course of the lawsuit, she turned over to her attorney certain confidential information of her former employer that she had retained.[148] That information was

---

[139] *Id.*

[140] *FirstEnergy Corp.*, 2021 WL 857107, at * 1.

[141] *Id.* at *1-2.

[142] *Id.* at *2.

[143] *Id.* at *3-8.

[144] *Id.* at *7.

[145] *Id.*

[146] No. 16-CV-963, 2018 WL 1532849 (E.D. Pa. March 29, 2018).

[147] *Id.* at *1-2.

[148] *Id.* at *2.

produced in discovery and the former employer asserted a DTSA claim against her.[149] The former employee moved to dismiss because the only disclosure that took place after the effective date of the DTSA was through a production of documents to her attorneys in confidence, pursuant to Federal discovery requirements.[150] That disclosure fell "within the immunized disclosure parameters defined by the DTSA" because it was "made to Plaintiff's counsel pursuant to a discovery Order of [the] Court, within the context of a lawsuit regarding violations of Title VII, the ADA, and the FMLA."[151]

Other employees have not been able to end litigation against them so quickly. For example, in *Unum Group v. Loftus,* the District Court for Massachusetts denied the employee's motion to dismiss, noting that the record contained no information to support or refute his claimed status as a whistleblower and whether he turned over all or only a portion of the information at issue (boxes of documents including confidential information and personally identifiable information of insurance policyholders and others in addition to trade secrets) to his counsel.[152]

In *1-800 Remodel, Inc. v. Bodor,* the Central District of California refused to dismiss the former employer's trade secret claims against a former employee because the record did not reveal, and the court could not determine at the pleading stage, the nature of the employees' complaints to the state agency or whether she made those complaints in confidence.[153]

And in *Garcia v. Vertical Screen Inc.,* the Eastern District of Pennsylvania declined to dismiss trade secret misappropriation claims based on an immunity affirmative defense, where the defense could not be established from the face of the counterclaims because it was "'not ascertainable from the [counterclaims] whether [Garcia] turned over all of [Vertical Screen]'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.'"[154]

---

[149] *Id.*

[150] *Id.*

[151] *Id.* at *4-5.

[152] *Unum Group v. Loftus*, 220 F. Supp. 3d 143, 147 (D. Mass. 2016).

[153] No. CV 18-472-DMG, 2018 WL 6340759 at *6 (C.D. Cal. Oct. 17, 2018).

[154] *Garcia v. Vertical Screen Inc.,* Civil Action No. 19-3184, 2020 WL 2615624, at *5 (E.D. Penn. May 22, 2020).

Immunity may not be a complete defense to a misappropriation of trade secrets claim based upon the facts of the case. When confronted with a claim of immunity, courts will look at all of the allegations in the complaint. Some allegations may address conduct for which there is immunity, but others may not. That is what the court determined in *Sorensen v. Polukoff.*[155] In that case, one of the defendants was a cardiologist and a potential purchaser of a cardiology practice.[156] Without authorization, he obtained hard drives and remote access to the cardiology practice's electronic records.[157] After he decided not to take over the practice, he initiated a *qui tam* action against the plaintiff and others, and alleged that the plaintiff had performed unnecessary medical procedures and improperly billed the government.[158] That defendant and his attorneys, also defendants, admitted that they accessed and used information obtained from the hard drive in the *qui tam* action and that the hard drive was provided to the Department of Justice.[159] The plaintiff asserted several claims against the defendants, including that they schemed to deprive him of the hard drive and used the information contained on the hard drive in the *qui tam* action and, importantly, to solicit the plaintiff's former patients to participate in medical malpractice lawsuits against the plaintiff.[160] The District Court for Utah, in analyzing whether to grant a motion to dismiss on the basis of immunity, explained that the defendants may have immunity for their disclosure of the hard drive to the DOJ and to counsel for investigation of False Claims Act violations, but "it cannot be seriously argued that all the allegations in the Complaint demonstrate that the disclosure of the alleged trade secrets was 'solely for the purpose of reporting or investigating a suspected violation of law."[161] The court declined to dismiss the DTSA claim.[162]

---

[155] *Sorensen v. Polukoff,* No. 1:18-CV-67 TS-PMW, 2020 WL 1692815, at *6 (D. Utah Apr. 7, 2020).

[156] *Id.* at *1.

[157] *Id.* at *1-2.

[158] *Id.* at *2.

[159] *Id.*

[160] *Id.*

[161] *Id.* at *6.

[162] *Id.*

Interaction with other laws

No preemption

Although the DTSA's purposes include providing an "efficient remedy" and "a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved,"[163] the DTSA "shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret."[164] Thus, the reality is trade secret claims are typically pleaded as an additional cause of action:

FIGURE 3:
Frequency of Other Claims Accompanying Trade Secret Misappropriation
(Out of 257 cases researched)

ACCOMPANYING CAUSE OF ACTION	NO. OF CASES	PERCENTAGE OF TOTAL
Contract Claims	179	69.6%
Tortious Interference	117	45.5%
Unfair/Deceptive Practices	110	42.8%
Fraud Claims	78	30.4%
Breach of Responsibility / Fiduciary Duty	78	30.4%
Conversion	73	28.4%
Infringement	60	23.3%
Unjust Enrichment	49	19.1%
Conspiracy	40	15.6%
Defamation/Disparagement	11	4.3%
Trespass	5	1.9%
Emotional/Mental Distress	1	0.4%
Other	100	38.9%

(Jeffrey Mordaunt et al., *Trends in Trade Secret Litigation Report 2020,* Figure 3 at 29 (Stout 2020)).

[163] H.R. Rep. No. 114-529, at 6 (2016).

[164] 18 U.S.C. § 1838.

Fortunately, because the DTSA aligns closely with the UTSA, most courts are able to analyze DTSA claims and State law trade secret claims together.[165]

No aiding and abetting or conspiracy

Although the DTSA itself does not preempt other causes of action, it has been interpreted to exclude related common law causes of action like aiding and abetting and conspiracy.[166] Notably, the statute does include a prohibition against conspiracy to steal trade secrets, but that provision is contained within the criminal portion of the statute and has been held to not create a private cause of action for conspiracy in civil proceedings.[167]

Contracts & Economic Loss Rule

At least one court has considered whether claims under the DTSA are barred by the economic loss rule or "gist of the action" doctrine.[168] In that case, the defendant's employment agreement prohibited disclosure of the trade secrets at issue.[169] And the economic loss rule "operates to 'preclude[ ] plaintiffs from recasting ordinary breach of contract claims into tort claims.'"[170] The Western District of Pennsylvania concluded the economic loss rule did not bar plaintiff's DTSA claims because an independent duty exists:

> The Court has little difficulty concluding that the "gist of the action" doctrine does not operate to bar the trade secrets misappropriation claims here. Mr. Herberger has a duty under the DTSA and PUTSA to refrain from misappropriating the trade secrets of his former employer. Both the DTSA and PUTSA create private rights of actions

---

[165] *See, e.g., MPAY Inc. v. Erie Custom Computer Applications, Inc.*, 970 F.3d 1010, 1017 (8th Cir. 2020) ("[The plaintiff] asserts claims for misappropriation of trade secrets under both the DTSA and the [Minnesota Uniform Trade Secrets Act]. [The plaintiff] does not identify any differences in these statutes or in the construction courts have given them that would be relevant to our analysis, so we analyze [the plaintiff] trade-secrets-misappropriation claims together.").

[166] C-*Ville Fabricating, Inc. v. Tarter*, 2019 WL 1368621 (E.D. Ky. 2019).

[167] *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 271 F. Supp. 3d 835, 842 (E.D. Va. 2017).

[168] *Pittsburgh Logistics Sys., Inc. v. LaserShip, Inc.*, 2:18-CV-1382, 2019 WL 2443035, at *8 (W.D. Pa. June 12, 2019).

[169] *Id*.

[170] *Id*. at *9 (quoting *Jones v. ABN Amro Mortg. Grp., Inc.*, 606 F.3d 119, 123 (3d Cir. 2010)).

> that are enforceable in the absence of a mutual consensus between contracting parties. These claims can be pursued concurrently with a breach of contract claim covering the same information.[171]

Remedies

DTSA's Civil Seizure Remedy

The DTSA's civil seizure provision has been touted as providing trade secret victims with a powerful *ex parte* tool to protect against damage. *Ex parte* seizure orders are not new, as the Lanham Act authorizes *ex parte* seizures of counterfeit goods and the Copyright Act authorizes *ex parte* impoundments of items related to copyright infringement.[172] The DTSA's civil seizure remedy has also proven controversial as commentators question whether it is constitutional, particularly given due process concerns arising out of the broad and vague definition of trade secrets.[173]

In extraordinary circumstances, the DTSA permits courts to issue an order providing for the seizure of property "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[174] The application for civil seizure must be supported by an affidavit or verified complaint.[175]

The court may not grant a civil seizure application unless the court finds "it clearly appears from specific facts" that:

1. an injunction or other form of equitable relief would be inadequate because the party to which the order would be issues would evade, avoid, or otherwise not comply with the order;

2. an immediate and irreparable injury will occur if such seizure is not ordered;

---

[171] *Pittsburgh Logistics Sys., Inc.*, 2019 WL 2443035, at *9.

[172] 15 U.S.C. §116(d); 17 U.S.C. 503(a).

[173] Bandyopadhyay & Weyde, *THE DTSA Civil Seizure Remedy: Constitutional or Not,* 31 No. 12 Intell. Prop. & Tech. L.J. 9 (2019).

[174] 18 U.S.C. § 1836(b)(2)(A).

[175] *Id.*

3. the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;

4. the applicant is likely to succeed in showing that

    a. the information is a trade secret; and
    b. the person against whom seizure would be ordered
        i. misappropriated the trade secret of the applicant by improper means; or
        ii. conspired to use improper means to misappropriate the trade secret of the applicant;

5. the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;

6. the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; ***and***

7. the applicant has not publicized the requested seizure.[176]

Like injunctive relief, the civil seizure remedy has strict requirements applicable to the court's order permitting the seizure. The order must:

1. set forth findings of fact and conclusions of law;

2. provide for the narrowest seizure of property necessary to achieve the purpose and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent

[176] *Id.*

possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;

3. be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access is consistent with the requirements of materials in the court's custody set forth in Paragraph D of the statute (addressing storage medium, confidentiality protections, and appointment of a special master);

4. provide guidance to law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including:

    a. the hours during which the seizure may be executed; and
    b. whether force may be used to access locked areas;

5. set a date for hearing at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; ***and***

6. require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or attempted seizure.[177]

The court must order that the seizure be made by a Federal law enforcement officer who will, upon service, carry out the seizure.[178] State or local law enforcement officials may participate in the seizure, but the applicant and its agents may not be permitted to

[177] 18 U.S.C. § 1836(b)(2)(B).

[178] 18 U.S.C. § 1836(b)(2)(E).

participate.[179] The court may allow a technical expert who is unaffiliated with the applicant and is bound by a court-approved nondisclosure agreement to participate in the seizure if the court finds that the expert will aid in the efficient execution of and minimize the burden of the seizure.[180]

The court must protect the seized material.[181] The seized material must be secured from physical and electronic access during seizure and while in the court's custody.[182] If the seized material includes a storage medium or the seized material is stored on a storage medium, the court must prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the seizure hearing is held.[183] The court also must take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized, unless the person against whom the order is entered consents to disclosure.[184] The court is also permitted to appoint a special master to locate and isolate all misappropriated trade secrets and to facilitate the return of unrelated property and data to the person from whom the property was seized.[185] The special master must agree to be bound by a court approved non-disclosure agreement.[186]

The seizure hearing must be held on the date set forth in the court's seizure order.[187] The party who obtained the *ex parte* order has the burden to "prove the facts supporting the findings of fact and conclusions of law necessary to support the order."[188] If the party fails to satisfy its burden, the seizure order is dissolved, or modified to conform with the applicant's proof.[189]

---

[179] *Id.*

[180] *Id.*

[181] 18 U.S.C. § 1836(b)(2)(D).

[182] 18 U.S.C. § 1836(b)(2)(D)(i).

[183] 18 U.S.C. § 1836(b)(2)(D)(ii).

[184] 18 U.S.C. § 1836(b)(2)(D)(iii).

[185] 18 U.S.C. § 1836(b)(2)(D)(iv).

[186] *Id.*

[187] 18 U.S.C. § 1836(b)(2)(F).

[188] *Id.*

[189] *Id.*

Cases Denying Seizure

Despite being lauded as an important part of the statute, the DTSA's civil seizure remedy has been used in an extremely small fraction of DTSA cases.[190] A significant hurdle for those seeking seizure is establishing that relief under Rule 65 is inadequate.

In *000 Brunswick Rail Mgt. v. Sultanov,* the Northern District of California denied plaintiffs' request for an ex parte seizure.[191] Plaintiffs had alleged that the defendant former employees misappropriated trade secrets.[192] They had allegedly sent several confidential documents to personal email accounts.[193] One of the employees had deleted his sent items and emptied his trash folder.[194] The court entered a preservation order and a temporary restraining order, but declined to seize the company issued laptop and mobile phone in one of the former employee's possession.[195] The court found that seizure was not necessary because the defendant would be ordered to deliver the devices to the court at a show cause hearing on plaintiffs' preliminary injunction request and was prevented, by a temporary restraining order, from accessing or modifying the devices in the meantime.[196]

The plaintiffs' application for seizure was also denied in *Hayes Healthcare Servs., LLC, v. Meacham.*[197] The plaintiffs, healthcare recruiting companies, sued a former employee for misappropriation of trade secrets after they determined that he had created and exported to his personal Google cloud account 1.9 gigabytes of company data and deleted the files he took from the company server.[198] Of the 1,100 files the former employee took, 700 contained confidential information and trade secrets.[199] Plaintiffs sent a demand letter to defendant, and defendant's attorney responded by stating that

---

[190] Duszczyszyn & Roland, *Ex Parte Seizure Under the Defend Trade Secrets Act: Insights on the New Remedy,* 26 No. 26 Westlaw Journal Intellectual Property 02 (April 8, 2020) (noting that since the DTSA's enactment "fewer than 20 ex parte seizures have been requested, with about half being granted").

[191] *000 Brunswick Rail Mgt. v. Sultanov,* Case No. 5:17-cv-00017-EJD, 2017 WL 67119 at 1 (N.D. Cal. Jan. 6, 2017).

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id.* at *2.

[196] *Id.*

[197] *Hayes Healthcare Servs., LLC v. Meacham,* Case No. 19-60113, 2019 WL 2637053, at *6 (S.D. Fla. Feb. 1, 2019).

[198] *Id.* at *2.

[199] *Id.*

defendant was willing to return the confidential information he took and would allow for an inspection of his devices and Google cloud account once a protocol was agreed upon.[200] The Southern District of Florida granted injunctive relief, but declined to order seizure because the defendant had indicated his willingness to turn over his devices and cloud account for inspection. There were no exceptional circumstances warranting seizure.[201]

Cases Granting Seizure

Plaintiffs have been more successful in obtaining seizure relief when the defendants have a history of destroying evidence, evading service, or engaging in other dishonest conduct.

In *Mission Capital Advisors LLC v. Romaka*, a commercial real estate finance company filed suit against a former employee alleging a DTSA claim and seeking a seizure order.[202] The former employee had allegedly downloaded the employer's trade secret contact lists to his personal computer, did so when he was absent from work for several weeks, falsely represented that he had deleted the data, had retained the data and saved it under a different name and in a masked file type, and was receiving several employment offers at the time of this conduct.[203] The Southern District of New York entered a seizure order after notice to the defendant and the defendant's failure to appear at the seizure hearing.[204] The court determined that injunctive relief would not be an adequate remedy because the defendant had been served by mail with, and ignored, a temporary restraining order, evaded personal service, and did not appear at a show cause hearing.[205] The court ordered seizure of the contacts lists from defendant's computer and the deletion of those files.[206]

In *Axis Steel Detailing, Inc. v. Prilex Detailing LLC,* the District Court for Utah entered a seizure order after finding that other equitable and injunctive relief would be inadequate to protect the plaintiff's trade secret digital files because defendants had a

---

[200] *Id.*

[201] *Id.*at *5-6.

[202] *Mission Capital Advisors LLC v. Romaka*, 16-CV-5878 (RA), 2016 WL 11517040, at *1 (S.D.N.Y. July 22, 2016).

[203] *Id.* at *2.

[204] *Id.* at *1.

[205] *Id.*

[206] *Id.* at *2.

high level of computer technical proficiency, had attempted in the past to delete information, and had shown a willingness to provide false and misleading information.[207]

Seizure was also ordered in *AVX Corp. v. Kim.*[208] The plaintiff former employer filed suit against defendant former employee and alleged that the former employee had "surreptitiously" downloaded and copied files without authorization, lied and attempted to conceal the access and downloading of the files, and retained possession of the stolen files after his employment was terminated. The District Court for South Carolina ordered seizure, finding among other things, that relief under Rule 65 would be inadequate because defendant's "likelihood to evade, avoid, or otherwise not comply with such an order is demonstrated by his deceptive actions when he repeatedly lied and attempted to conceal the fact that he surreptitiously accessed and downloaded the Stolen Computer Files."[209]

Injunctions and Irreparable Harm

"A preliminary injunction is an extraordinary remedy never awarded as of right."[210] Under Rule 65, a party seeking a preliminary injunction is required to show "(1) the movant is substantially likely to succeed on the merits; (2) the movant will suffer irreparable injury if the injunction is denied; (3) the movant's threatened injury outweighs the injury the opposing party will suffer under the injunction; and (4) the injunction would not be adverse to the public interest."[211]

Some courts employ a rebuttable presumption of irreparable harm in trade secret misappropriation cases.[212] In *Faiveley Transp. Malmo AB v. Wabtec,* which predated the DTSA, the Second Circuit explained that a rebuttable presumption of irreparable harm "might be warranted in cases where there is a danger that, unless enjoined," a defendant

---

[207] *Axis Steel Detailing, Inc. v. Prilex Detailing LLC,* No. 2:17-CV-00428-JNP, 2017 WL 8947964, at *1 (D. Utah June 29, 2017). The same factual findings regarding the inadequacy of other relief were made in *Solar Connect, LLC v. Endicott*, No. 2:17-CV-1235, 2018 WL 2386066, at *1 (D. Utah Apr. 6, 2018).

[208] *AVX Corp. v. Kim,* Civil Action No. 6:17-00624-MGL, 2017 WL 11316598 at *1-2 (D.S.C. Mar. 13, 2017).

[209] *Id.*

[210] *Winter v. Natural Res. Def. Council,* 555 U.S. 7, 24 (2008).

[211] *Fish v. Kobach,* 840 F.3d 710 (10th Cir. 2016).

[212] *Faively Transp. Malmo AB v. Wabtec Corp.,* 559 F.3d 110, 118 (2d Cir. 2009).

will continue to disseminate already misappropriated trade secrets, "or otherwise irreparably impair the value of those secrets."[213]

Other courts recognize no presumptions and require a showing of irreparable harm. In *First Western Capital Mgmt. v. Malamed,* the Tenth Circuit reversed the grant of an injunction in favor of a former employer under the DTSA, without the movant demonstrating irreparable harm.[214] The district court determined that a showing of irreparable harm was excused "when the evidence shows that a defendant is or will soon be engaged in acts or practices prohibited by statute, and that statute provides for injunctive relief to prevent such violations."[215] The Tenth Circuit clarified the limited circumstances in which a court may presume irreparable harm and grant injunctive relief—when a statute *mandates* injunctive relief as a remedy for a violation.[216] In that situation, the statute has "effectively constrained the courts' traditional discretion to determine whether such relief is warranted."[217] "But when a statute merely authorizes—rather than mandates—injunctive relief, courts must determine that the moving party has established all four elements to grant injunctive relief."[218] The DTSA authorizes, but does not require, injunctive relief. Therefore, according to the Tenth Circuit, plaintiffs seeking preliminary injunctive relief under DTSA must demonstrate irreparable harm.[219]

---

[213] *Id.; see also Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1143-44 (N.D. Ill. 2019) (applying a rebuttable presumption in an action brought under the DTSA and the Illinois Trade Secrets Act); *Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc.,* No. 4:06CF114, 2010 WL 3370286, at *2 (N.D. Ohio Aug. 26, 2010) ("Courts in the 6th Circuit have stated only that harm caused by the misappropriation of trade secrets is generally irreparable and may be presumed in some cases." (citations omitted)).

[214] *First Western Capital Mgmt. v. Malamed,* 874 F.3d 1136, 1138 (10th Cir. 2017).

[215] *Id.* at 1140.

[216] *Id.* at 1141; *see also Bedrossian v. Nw. Mem'l Hosp.*, 409 F.3d 840, 843 (7th Cir. 2005) ("'unless a statute *clearly mandates* injunctive relief . . . , the courts are to employ traditional equitable considerations (including irreparable harm) in deciding whether to grant such relief'") (emphasis added) (citing *Weinberger v. Romero*-Barcelo, 456 U.S. 305, 313, 317-18 (1982)); *In re Sac & Fox Tribe of the Missippe of the Mississippi on Iowa/Meskwaki Casino Litig.*, 340 F.3d 749, 760-62 (8th Cir. 2003) (requiring all elements to be established in the absence of a statute providing only equitable remedies); *C.B. v. Bd. of School Comm'rs of Mobile, Cty.*, 261 Fed. Appx. 192, 194 (11th Cir. 2008) (refusing to presume irreparable harm where state did not mandate injunctive relief).

[217] *First Western Capital Mgmt.*, 874 F.3d at 1141.

[218] *Id.*

[219] *Id.; see also Cutera, Inc. v. Lutronic Aesthetics, Inc.*, 444 F. Supp. 1198, 1208 (E.D. Cal. 2020) ("While the Ninth Circuit has yet to directly address . . . courts' power to presume irreparable harm in trade secrets cases, in particular, this court joins those districts who have declined to rely on a presumption in determining irreparable harm in the intellectual property context.")

Damages theories

Damage awards in trade secret litigation may include awards for actual damages and unjust enrichment. The DTSA provides that a court may award "damages for actual loss caused by the misappropriation of a trade secret."[220] It also permits recovery of damages for "unjust enrichment . . . not addressed in computing damages for actual loss."[221] The Fourth Circuit has described these two methods for assessing misappropriation damages as either: (1) calculating the damages sustained by the victim, or (2) disgorging the profits earned by the wrongdoer from the misappropriation.[222]

Because of the numerous ways that damages can be calculated in trade secret misappropriation cases, "[c]omputing damages in a trade secrets case is not cut and dry."[223] The value gained by the defendant due to defendant's misappropriation of a trade secret can be measured by the defendant's actual profits due to use of the trade secret, the value that the trade secret would have had to a reasonably prudent investor, or the value of development costs that were not incurred.[224]

In some cases, a court may instead award reasonable royalties, especially where the plaintiff's actual damages are uncertain or where the defendant minimally benefitted from the misappropriated trade secrets. "If neither damages nor unjust enrichment caused by misappropriation are provable…a reasonable royalty is appropriate."[225] "To determine the amount of a reasonable royalty, the court calculates what the parties would have agreed to as a fair licensing price at the time that the misappropriation occurred."[226]

---

[220] 18 U.S.C. § 1836(b)(3)(B).

[221] *Id*.

[222] *Sperry Rand Corp. v. A–T–O, Inc.*, 447 F.2d 1387, 1392 (4th Cir. 1971).

[223] *Am. Sales Corp. v. Adventure Travel, Inc.*, 862 F. Supp. 1476, 1479 (E.D. Va. 1994).

[224] *Southwestern Energy Prod. Co. v. Berry-Helfand*, 491 S.W.3d 699, 711 (Tex. 2016); *see also Syntel Sterling Best Shores Mauritius Limited, v. The Trizetto Group, Inc.*, 15 CIV. 211 (LGS), 2021 WL 1553926, at *6 (S.D.N.Y. Apr. 20, 2021) ("These avoided costs are recoverable as damages for unjust enrichment under the DTSA and its state law counterparts derived from the Uniform Trade Secrets Act ("UTSA")."); *Motorola Sols., Inc. v. Hytera Comm'cns Corp.*, 2020 WL 6554645, at *12-15 (N.D. Ill. Oct. 19, 2020) (ratifying jury's award of defendant's avoided research and development costs as unjust enrichment under the DTSA); *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 2018 WL 2172502, at *6 (E.D. Va. May 10, 2018) (explaining that avoided costs are "appropriately considered" a part of the trade secret plaintiff's "unjust enrichment damages" recoverable under the DTSA).

[225] *DiscoverOrg Data, LLC v. Bitnine Global, Inc.*, No. 19-CV-08098-LHK, 2020 WL 6562333, at *9 (N.D. Cal. Nov. 19, 2020).

[226] *Id*. (citing *Ajaxo Inc. v. E*Trade Financial Corp.*, 187 Cal. App. 4th 1295, 1308 (Cal. Ct. App. 2010)).

Unjust Enrichment

Unjust enrichment damages include "avoided cost" damages under both, the DTSA, as well as the State-law UTSA.[227] Because the DTSA permits actual damages awards and unjust enrichment, both can be recovered, given that there is no double recovery:[228]

> [T]he DTSA expressly permits recovery of the loss to a claimant and/or the unjust enrichment to a wrongdoer, as long as there is no double counting. Damages characterized as the total value of the trade secret belong in the former category—loss to a claimant—and logically could not be awarded if the value in fact is not lost. However, avoided costs damages are in the latter category of unjust enrichment and represent the wrongful gain to the party that misappropriated the trade secret.[229]

In *Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.*, the plaintiff sought the amount that the defendant saved in its development costs by using its own development costs as a proxy way to determine and calculate the avoided costs of the alleged wrongdoer.[230] Other courts have applied the same method in order to calculate the avoided costs that the defendant saved through misappropriation.[231]

Furthermore, the *Syntel* court states, "that [the defendant's] revenue from the misappropriation can be determined also does not preclude avoided costs as a measure of damages."[232] Although both, defendant's profits due to the misappropriation and defendant's avoided losses, are possible forms of unjust enrichment, avoided costs may

---

[227] *Syntel Sterling Best Shores Mauritius Ltd.*, 2021 WL 1553926, at *6; *Steves & Sons, Inc. v. JELD-WEN, Inc.*, No. 3:16-cv-545, 2018 WL 2172502, at *6 (E.D. Va. May 10, 2018) (a trade secret claim under the DTSA appropriately includes avoided costs as a form of unjust enrichment to the defendant); *Motorola Sols., Inc.*, 1:17-cv-1973, 2020 U.S. Dist. LEXIS 210899, at *12–15 (N.D. Ill. Oct. 19, 2020) (granting jury's award of unjust enrichment to the plaintiff for defendant's avoided research and development costs).

[228] *See* 18 U.S.C. § 1836(b)(3)(B); *Syntel*, 2021 WL 1553926, at *7.

[229] *Syntel*, 2021 WL 1553926, at *7.

[230] *Id*.

[231] *See GlobeRanger Corp. v. Software AG United States of Am., Inc.*, 836 F.3d 477, 499 (5th Cir. 2016).

[232] *Syntel*, 2021 WL 1553926, at *7.

be a more appropriate metric of damage calculation when the defendant minimally benefits or does not in fact benefit from its misappropriation of another's trade secrets.[233] From a public policy perspective, the misappropriating party, and "not the aggrieved party," should be required to "bear the business risk that the wrongdoer's use of purloined trade secrets will not be profitable."[234]

Reasonable Royalties

Under the DTSA, where exceptional circumstances exist, a court can order impose reasonable royalties as a form of prospective relief.[235]

Under most states' adopted versions of the UTSA, as well as under the DTSA, the misappropriation of trade secrets is not considered to be an ongoing tort for purposes of accrual.[236] However, ongoing damages can certainly result from a non-continuing tort.[237] While reasonable royalties may be referred to as a type of prospective injunctive relief, royalties can be awarded apart from an award of injunctive relief. In cases where injunctive relief is not appropriate due to an availability of monetary damages (and therefore, there is no irreparable injury), "it would be perverse for the Court to hold that, having denied injunctive relief because of the availability of a monetary award for future injuries, such a monetary award is not available after all."[238] Furthermore, if state law will allow a permanent injunction to issue that would prohibit any action by the plaintiff, "then it is surely permissible for a court to grant equitable relief that is significantly less burdensome, in the form of an ongoing royalty with a cut-off date."[239] In other cases, reasonable royalties have been granted where plaintiffs may have proven their entitlement to injunctive relief, but where the court determined that a traditional prohibitory injunction would have been contrary to the public policy.[240] Often, in cases

---

[233] *Id*.

[234] *Id*.

[235] 18 U.S.C. § 1836 (b)(3)(A)(iii).

[236] *Bianco v. Globus Med., Inc.*, No. 2:12-CV-00147-WCB, 2014 U.S. Dist. LEXIS 151967, at *71 (E.D. Tex. Oct. 27, 2014) (ongoing royalty was the only way to ensure that the plaintiff was fully compensated after the misappropriation).

[237] *Id*.

[238] *Id*. at *73.

[239] *Id*. at *72.

[240] *Skycam, LLC v. Bennett*, 104 U.S.P.Q.2d (BNA) 1463, 1466 (N.D. Okla. 2012).

where the defendant has not been enriched or profited, reasonable royalties are an appropriate measure of damages.[241]

The plaintiff must satisfy the threshold requirement of showing that the defendant "actually put the trade secret to some commercial use" in order to obtain an award for reasonable royalty damages.[242] "Employing the confidential information in manufacturing, production, research or development, marketing goods that embody the trade secret, or soliciting customers through the use of trade secret information, all constitute use."[243]

A reasonable royalty can be ordered to be paid out in different forms.[244] However, "the proper form of the royalty is dependent upon what would have been the most likely agreement during the hypothetical negotiation."[245] In determining the amount of the royalty using this hypothetical negotiation approach, the proper standard for a reasonable royalty "would be a willing buyer–willing seller test," where the primary inquiry is "what the parties would have agreed upon, if both were reasonably trying to reach agreement."[246] Often lump-sum royalty payments are the best option for parties who are hostile or otherwise do not wish to continue ongoing interactions with one another.[247]

When determining the value of the reasonable royalty to be awarded had the parties reached the hypothetical agreement, the trier of fact should consider the following factors: (1) the resulting and foreseeable changes in the parties' ability to compete; (2) the prices of previous sales of products or licenses; (3) the value of the trade secret in the

---

[241] *See Vermont Microsystems, Inc. v. Autodesk, Inc.*, 138 F.3d 449, 450 (2d Cir. 1998) (Proof of the unjust enrichment of the defendant was too speculative, and therefore, reasonable royalties were awarded); *Walker Mfg., Inc. v. Hoffmann, Inc.*, 261 F. Supp. 2d 1054, 1083–88 (N.D. Iowa 2003) (Court awarded reasonable royalties because the plaintiff did not enjoy any profits, nor did the defendant profit from the misappropriation).

[242] *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 539 (5th Cir. 1974).

[243] *O2 Micro Int'l Ltd. v. Monolithic Power Sys., Inc.*, 399 F. Supp. 2d 1064, 1072 (N.D. Cal. 2005) (citing *PMC, Inc. v. Kadisha*, 78 Cal. App. 4th 1368, 1383 (Cal. Ct. App. 2000)).

[244] *LinkCo, Inc. v. Fujitsu Ltd.*, 232 F. Supp. 2d 182, 188 (S.D.N.Y. 2002).

[245] *Id.*

[246] *Univ. Computing Co.*, 504 F.2d at 537 (citing *Egry Register Co. v. Standard Register Co.*, 23 F.2d 438, 443 (6th Cir. 1928).

[247] *See InfoSpan, Inc. v. Emirates NBD Bank PJSC*, No. SACV 11-1062 JVS (ANx), 2016 WL 8849699, at *13 (C.D. Cal. June 8, 2016) ("[A] one-time arrangement would avoid the necessity of monitoring an ongoing relationship given the evident distrust which had grown up.").

plaintiff's hands, including development costs; (4) the nature and extent of defendant's misappropriation, and; (5) other unique factors that may have affected the parties' agreement.[248]

Statute of Limitations

Inquiry Notice

Like the UTSA, the limitations period under the DTSA begins to run three years from the date the trade secret misappropriation was actually discovered or should have been discovered through a reasonable exercise of due diligence.[249] A continuing period of misappropriation constitutes a single claim under the DTSA.[250] Therefore, the statute of limitations for the continuing misappropriation claim would begin to run when the misappropriation actually was or should have been discovered and would not start anew upon each instance of disclosure.[251]

When a party to a suit "should have been aware of the existence of their cause of action, they are said to be on inquiry notice of the same."[252] "A party is placed on inquiry notice when it gains sufficient knowledge of facts that would put that person on notice of the existence of a problem or potential problem."[253] Since the passage of the DTSA, the Second, Eighth, and Tenth Circuits have all affirmed judgments that a party to the suit

[248] *University Computing*, 504 F.2d at 539.

[249] 18 U.S.C. § 1836(d).

[250] *Id*.

[251] *CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 16-CV-33-LRR, 2017 WL 6210920, at *8 (N.D. Iowa Dec. 8, 2017), aff'd, 920 F.3d 560 (8th Cir. 2019) ("Both statutes treat a continuing violation as a single claim for the purposes of determining when an action becomes time barred.").

[252] *CMI Roadbuilding*, 2017 WL 6210920, at *8.

[253] *Id*. (citing *Buechel v. Five Star Quality Care, Inc.*, 745 N.W.2d 732, 736 (Iowa 2008).

was put on inquiry notice of the party's claim under the DTSA.[254] And various district courts have addressed the issue of inquiry notice under the DTSA since its inception.[255]

Because what constitutes inquiry notice for statute of limitations purposes seems to be identical under the UTSA and the DTSA, several cases alleging violations under the DTSA rely on case precedent decided prior to the DTSA's inception in 2016. *Alta Devices, Inc. v. LG Electronics, Inc.*, relied on *Wang v. Palo Alto Networks, Inc.*, a case decided in 2014, prior to the passage of the DTSA.[256] *Ptp Oneclick v. Avalara, Inc.*, subsequently relied on *Alta Devices* and *Wang*, in its determination that the plaintiff had been put on inquiry notice, barring plaintiff's DTSA claim under the three-year limitations period.[257]

[254] *See CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 920 F.3d 560, 565–66 (8th Cir. 2019) (The Court affirmed that plaintiff was put on inquiry notice at the time plaintiff sent letters to the defendant, a former employee, demonstrating plaintiff's awareness of the potential for defendant to abscond with trade secret documentation and customer lists); *Zirvi v. Flatley*, 838 Fed. App'x 582, 586 (2nd Cir. 2020) (Prior litigation involving substantially the same claims and many of the same parties put "a person of ordinary intelligence" at least on inquiry notice); *Camick v. Holladay*, 758 Fed. App'x 640, 643 (10th Cir. 2018) (The Court affirmed that the plaintiff was put on inquiry notice when defendant refused to return alleged trade secret items).

[255] *See Alta Devices, Inc. v. LG Elecs., Inc.*, No. 18-CV-00404-LHK, 2019 WL 1924992, at *12 (N.D. Cal. Apr. 30, 2019) (Plaintiff was put on inquiry notice by the defendant's failure to return documents containing the alleged trade secrets in violation of a mutual non-disclosure agreement); *Ptp Oneclick v. Avalara, Inc.*, Case No. C19-0640JLR, 2020 WL 4729174, at *5–6 (W.D. Wash. May 27, 2020) (Plaintiff was put on inquiry notice by defendant's failure to return plaintiff's confidential information at the end of the disclosure period in breach of a confidentiality agreement).

[256] *See Wang v. Palo Alto Networks, Inc.*, No. C 121-05579 WHA, 2014 WL 1410346 (N.D. Cal. Apr. 11, 2014).

[257] *Ptp Oneclick*, 2020 WL 4729174, at *5–6.