THOMSON REUTERS
PRACTICAL LAW™

Trade Secrets Litigation

by Peter A. Steinmeyer, Epstein, Becker & Green, P.C., and Zachary C. Jackson, with Practical Law Labor & Employment

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/5-523-8283**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note discussing trade secrets litigation for employers whose employees or former employees have misappropriated trade secrets. This Note describes pre-litigation investigations, sending cease and desist letters, and contacting law enforcement. It also addresses filing a legal action, including forum selection and choice of law issues, deciding whether to include the employee's new employer and third parties, common causes of action (including misappropriation under the Defend Trade Secrets Act (DTSA)), discovery, injunctive relief, damages, and attorneys' fees. It includes best practices for preparing to counter potential defenses and counterclaims and maintaining confidentiality during litigation. This Note applies to private employers and is jurisdiction-neutral. For more information on state-specific laws, see Trade Secret Laws: State Q&A Tool.

Trade secrets are often an employer's most valuable assets. When an employee or former employee misappropriates an employer's trade secrets, the employer frequently initiates litigation with several goals in mind, including:

- Preventing further unauthorized use or disclosure of its trade secrets.
- Recovering the trade secrets.
- Obtaining damages.

This Practice Note discusses trade secrets litigation. In particular, it addresses:

- Preliminary steps to consider, such as sending a cease and desist letter and contacting law enforcement.
- Filing a legal action.
- Common causes of action.
- Discovery, including expedited discovery.
- Injunctive relief, damages, and attorneys' fees.
- Best practices for preparing to counter potential defenses and counterclaims.
- Maintaining confidentiality during trade secrets litigation.

For more information on what constitutes a trade secret and how to protect trade secrets from unauthorized use or disclosure, see Practice Notes, Protection of Employers' Trade Secrets and Confidential Information and Employment Litigation: DTSA Claims: Trade Secrets Defined.

Preliminary Steps

Investigating the Suspected Misappropriation

A prompt and thorough investigation can be critical to successful trade secrets litigation. One of the first steps in an investigation is determining which information of the employer is truly secret and valuable because it is secret. Next, the employer must investigate what, if any, trade secret information the employee actually misappropriated. This investigation often consists of an in-depth forensic analysis of the employee's:

- Email (especially emails sent to a personal email account).
- Desktop and laptop computers (including indicia that USB memory devices have been plugged in).
- Handheld electronic devices.
- Cloud storage accounts.
- Office files.
- Calendar.

- Computer and telephone logs.
- Records of office access.
- Travel and expense records.

The investigation should be performed by an experienced electronic forensic analyst who not only can perform the investigation, but can later act as electronic forensic expert in support of the employer's claims.

An investigation's revelation that the employee misappropriated trade secret information is often sufficient to obtain a court order directing the employee to cease all use and disclosure of that information and return it to the employer. This result rests on the evidence or presumption that:

- As a former employee, the defendant has no authorized or legitimate purpose for using or disclosing the employer's trade secret information.
- The employer will be competitively injured by the employee's or the new employer's use or disclosure of this information.

An employer's investigation into suspected trade secrets misappropriation also typically includes gathering information about the employee's new employer and business. For more on gathering this information, see Practice Note, Preparing for Non-Compete Litigation: Best Practices for Gathering Evidence.

Sending a Cease And Desist Letter

Depending on the circumstances, a cease and desist letter can be a valuable preliminary step to litigation or a less expensive alternative. Cease and desist letters typically:

- Remind former employees of their contractual and other obligations to the employer.
- Advise them to cease and desist from conduct that violates their obligations.
- Where appropriate, demand the return of:
  - information;
  - documents; or
  - data.

Depending on the facts of a particular situation, an employer may decide to send a copy of the cease and desist letter or a similar letter to the employee's new employer. For sample letters, see Standard Documents, Restrictive Covenant Cease and Desist Letter to Former Employee and Restrictive Covenant Cease and Desist Letter to New Employer.

The employer should investigate and be able to substantiate its allegations of trade secret misappropriation before sending any cease and desist letter, as its failure to do so can expose the employer to a tortious interference claim by the employee or the employee's new employer (see Preparing for Potential Counterclaims).

Contacting Law Enforcement

When an employer suspects criminal conduct, it may decide to contact law enforcement to investigate and prosecute trade secret theft, in addition to or instead of sending one or more cease and desist letters. Misappropriating trade secrets is a crime under various federal laws. For example, it is illegal to:

- Misappropriate trade secrets or knowingly receive misappropriated trade secrets with the intent to benefit a foreign government or a foreign agent (18 U.S.C. § 1831).
- Misappropriate trade secrets related to a product or service used or intended for use in interstate or foreign commerce (18 U.S.C. § 1832).
- Transport in interstate or foreign commerce stolen property worth $5,000 or more (18 U.S.C. § 2314).
- Use the mail or a wire transmission to misappropriate trade secrets as part of a scheme to defraud (18 U.S.C. §§ 1341, 1343, and 1346).

Contacting law enforcement regarding suspected trade secrets misappropriation has three main advantages:

- The mere threat of criminal prosecution and penalties may encourage employees to explain what happened.
- Prosecutions are public, and publicity may deter other employees who are contemplating similar acts.
- If an employee has misappropriated trade secrets and left the country, law enforcement can obtain evidence abroad and possibly hold foreign conspirators accountable for their involvement.

The main drawback of contacting law enforcement is the potential for disclosure of the employer's trade secrets in connection with the prosecutorial proceedings. Law enforcement officials and judges typically try to avoid disclosing sensitive, confidential, or trade secret information unnecessarily. However, the risk exists that the employer's trade secrets may be disclosed, purposefully or inadvertently, if it helps in the prosecution of the case.

Filing a Legal Action

Forum Selection and Choice of Law

Unless the employee and employer have signed an agreement with an enforceable and exclusive forum selection provision, the employer decides where to initiate litigation. Depending on the particular facts, an employer may have the option of filing a complaint in federal or state court. If an employer has evidence that an employee misappropriated or used its trade secrets, it may opt to bring a claim under the Defend Trade Secrets Act (DTSA) in federal court and join state law claims in the federal action under the court's supplemental jurisdiction. Typically, the circumstances of the case help an employer determine the most advantageous option (see, for example, Practice Note, Employment Litigation: DTSA Claims: Choosing the Litigation Forum).

Note that employers with businesses or employees in California are limited in their ability to impose forum selection clauses that require the parties to litigate outside of California or apply a law other than the law of that state. For all contracts entered into, modified, or extended on or after January 1, 2017, involving any person who primarily resides or works in California, choice of law and choice of venue contract provisions are prohibited if they apply another state's law or require adjudication in another state as a condition of employment, unless the employee was represented by counsel during the contract negotiations (Cal. Lab. Code § 925). For more information, see Legal Update, California to Prohibit Choice of Law and Venue Provisions in Employment Contracts.

Other states similarly limit the ability of employers to impose choice or law or forum selection clauses on employees. For example, the Massachusetts Noncompetition Agreement Act (MNAA) also limits an employer's ability to impose the law of a jurisdiction other than Massachusetts against individuals who live or work in the state (M.G.L. ch. 149, § 24K(e)). Similarly, in Washington state, provisions in non-competition covenants that would require a Washington-based employee or independent contractor to litigate a noncompetition covenant outside of Washington state or that apply another state's law are not enforceable (RCW 49.62.050).

In the absence of a choice of law provision, the court decides which state's trade secrets law should be applied if the employer and employee are located in different states. Depending on the states and the case law involved, an employer may argue that the employee violated the trade secrets law of the state or states where:

- The employer electronically stored its trade secrets.
- The employee accessed the employer's trade secrets to misappropriate them.
- The employee used the employer's trade secrets to harm the employer.

For more information on determining where to file, see Practice Notes, Preparing for Non-Compete Litigation: Where to File the Lawsuit and Choice of Law and Choice of Forum: Key Issues.

Deciding Whether to Include the Employee's New Employer in the Action

Before initiating litigation, employers must decide which parties to name in the complaint. In certain instances, an employer may be inclined to include the employee's new employer. For example, employers should consider naming the new employer if there is evidence that:

- The former employee was acting under the new employer's direction when the employee misappropriated the former employer's trade secret information.
- The new employer has agreed to indemnify the former employee for any liability arising out of the employee's move to the new employer or breach of contract with the former employer.
- The new employer gained a competitive benefit by the former employee's trade secret misappropriation.

For more information, see Practice Note, Preparing for Non-Compete Litigation: Deciding Whether to Include the Employee's New Employer in the Action.

Deciding Whether to Include Third Parties in the Action

In addition to naming former employees and their new employers, employers should consider naming any third parties who:

- Procured or assisted in the misappropriation of the trade secrets.
- Received those trade secrets.

Naming third-party defendants in the lawsuit can help ensure the return of all copies or derivatives of the trade secrets. Employers may also be able to obtain discovery

more easily than using the third-party subpoena discovery process. For more about the subpoena process generally, see Document Requests and Subpoenas in Federal Court Toolkit.

Common Causes of Action

Misappropriation of Trade Secrets

The most common claim against former employees who use or disclose an employers' confidential, proprietary information is a claim of trade secret misappropriation. Until the DTSA was enacted in May 2016, trade secrets had been protected primarily by state law (see Defend Trade Secrets Act). As of October 1, 2018, all states (except New York) and the District of Columbia have enacted a version of the model Uniform Trade Secrets Act (UTSA), and the requirements for stating a claim of misappropriation under the laws of those states are often similar. Typically, to state a claim under state law, employers must allege that:

- The information at issue is the employer's trade secret.
- The employee misappropriated the trade secret.
- The employee used or intended to use the trade secret in the employee's or the new employer's business.
- The employer suffered or will suffer damages.

For more information on demonstrating trade secrets misappropriation under state law, see Trade Secret Laws: State Q&A Tool: Question 9.

Defend Trade Secrets Act

Private Cause of Action

The DTSA creates a private cause of action for civil trade secret misappropriation under federal law (18 U.S.C. § 1836(b)). The law supplements but does not preempt or eliminate state law remedies for trade secret misappropriation (see Article, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers: How Does the DTSA Affect Existing State Non-Compete Laws?). The DTSA applies to misappropriation on or after the law's May 11, 2016 effective date.

The DTSA uses the definition of trade secret already contained in the Economic Espionage Act (18 U.S.C. § 1836(e)). Under that definition, a trade secret is business or scientific information that:

- Derives independent economic value from not being generally known to or readily accessible by the public through proper means.
- The owner has taken reasonable measures to keep secret.

(18 U.S.C. § 1839(3).)

Under the DTSA, misappropriation occurs when a person:

- Acquires a trade secret that the person knows or has reason to know was acquired through improper means.
- Discloses or uses a trade secret of another without express or implied consent and:
  - used improper means to acquire knowledge of the trade secret; or
  - knew or had reason to know that knowledge of the trade secret was derived through improper means or under circumstances giving rise to a duty to maintain its secrecy.
- Before a material change in position of the person:
  - knows or has reason to know that the information was a trade secret; and
  - acquires knowledge of the trade secret by accident or mistake.

(18 U.S.C. § 1839(b)(5).)

Improper means includes:

- Theft.
- Bribery.
- Misrepresentation.
- Breach or inducement of a breach of duty to maintain secrecy.
- Espionage through electronic or other means.

The DTSA expressly states that improper means do not include:

- Reverse engineering.
- Independent derivation.
- Any other lawful means of acquisition.

(18 U.S.C. § 1839(b)(6).)

An owner of a trade secret that is misappropriated may bring a civil action under the DTSA if the trade secret is related to a product that is used in or intended for use in interstate or foreign commerce (18 U.S.C. § 1836(b)(1)). The DTSA claim can be combined with any applicable state law claims under statutes or common law (including for misappropriation of trade secrets, breach of a confidentiality or non-competition agreement, or unfair competition). A civil action under the DTSA may be

brought in US district court (18 U.S.C. § 1836(c)). A DTSA action must be brought no later than three years after the date the misappropriation either:

- Was discovered.
- Should have been discovered with reasonable diligence.

(18 U.S.C. § 1836(d).)

The remedies under the DTSA are similar to those under the UTSA (see Remedies Under the DTSA).

The DTSA has no impact on existing state law inevitable disclosure theories, except to the extent that the standard for obtaining injunctive relief may be different in federal than in state court.

For more on the DTSA, see:

- Practice Note, Employment Litigation: DTSA Claims.
- Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist.
- Article, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers.
- Article, Expert Q&A on DTSA Seizure Orders.

Whistleblower Protections

The DTSA includes protections for whistleblowers who disclose trade secrets under certain circumstances by providing criminal and civil immunity under any federal or state trade secret law for the disclosure of a trade secret that either is made:

- In confidence solely for the purpose of reporting or investigating a suspected violation of law to:
  - a federal, state, or local government official; or
  - an attorney.
- In a complaint or other document filed under seal in a lawsuit or other proceeding (see Practice Note, Filing Documents Under Seal in Federal Court).

(18 U.S.C. § 1833(b).)

Employers must give employees, contractors, and consultants notice of this potential immunity in any contract or agreement entered into or amended after the effective date of the DTSA that governs the use of a trade secret or other confidential information. An employer may comply with this requirement by cross-referencing a policy document containing the employer's reporting policy for a suspected violation of law. (18 U.S.C. § 1833(b)(3)(A) and (B).)

For a sample notice provision, see Standard Clause, Notice of Immunity Under the Defend Trade Secrets Act (DTSA) Provision.

An employer that does not provide the required notice is precluded from recovering exemplary damages or attorneys' fees under the DTSA in an action against an employee to whom notice was not provided (18 U.S.C. § 1833(b)(3)(C)) (see Remedies Under the DTSA).

Inevitable Disclosure of Trade Secrets

An employer that fails to discover evidence of an employee's actual or intended misappropriation, use, or disclosure of trade secret information should consider an inevitable disclosure claim. This claim may apply where it is impossible for the former employee to perform the new job without relying on the employee's knowledge of the former employer's trade secrets, disclosing them to the employee's new employer, or both. Employers alleging this type of claim argue that it is inevitable that the former employee will:

- Use or disclose those trade secrets in the employee's new position.
- Cause injury to the former employer as a result.

Not every state recognizes claims for inevitable disclosure of trade secrets. In the jurisdictions that recognize this cause of action, employers should emphasize in their pleadings that:

- The companies are engaged in fierce competition in a niche market.
- The former employee was a high level executive privy to strategic plans or information.
- It would be impossible for the former employee to perform the new job without using or disclosing the plans or information.
- Circumstances support or highlight the employer's concern, such as the employee being dishonest or misleading about his departure from the former employer.

In *PepsiCo, Inc. v. Redmond*, the seminal case on inevitable disclosure, Pepsi introduced evidence that:

- Quaker was one of its principal competitors.
- They were engaged in fierce competition in the new age drink niche market.
- One of Pepsi's high-level executives had been privy to its strategic plans for the next steps in its efforts to gain market share.

- A high-level executive had resigned to work for Quaker in that same niche market.
- It would have been impossible for the former employee to perform his job at Quaker in that same niche market without bearing Pepsi's strategic plans in mind.
- Its concern was well-founded because the former executive had been dishonest about the scope of his new position at Quaker when he left Pepsi.

(54 F.3d 1262 (7th Cir. 1995).)

As a practical matter, however, courts are relatively reluctant to recognize inevitable disclosure claims because:

- The claims may effectively prevent an employee from accepting a new job even where the employee is not violating any contractual or other obligation.
- There is no evidence that the employee misappropriated anything or did anything wrong.

To convince a court to apply the inevitable disclosure doctrine, the former employer should be able to demonstrate, as in *PepsiCo*, that it is in a position where its star player has left to join the rival team right before the big game with the former employer's playbook in hand.

Some practitioners originally argued that the DTSA does not allow for inevitable disclosure claims. However, the language of the DTSA clear states that it:

- Allows for claims based on threatened misappropriation (18 U.S.C. § 1836(b)(3)).
- Does not preempt state law, and therefore has no impact on the ability to bring inevitable disclosure claims under state law (18 U.S.C. § 1838).

Courts in jurisdictions that otherwise recognize the inevitable disclosure doctrine have specifically allowed inevitable disclosure claims under the DTSA as well (see, for example, *Gen. Elec. Co., v. Uptake Techs. Inc.*, 394 F. Supp. 3d 815, 834 (N.D. Ill. 2019) (DTSA claim based on inevitable disclosure may survive a motion to dismiss); *Pkg. Corp. of Am., Inc. v. Croner*, 419 F. Supp. 3d 1059, 1069-70 (N.D. Ill. 2020) (recognizing availability of inevitable disclosure theory under the DTSA but holding that plaintiff did not allege sufficient facts to prevail under that theory)).

For more on inevitable disclosure, see Trade Secret Laws: State Q&A Tool: Question 17 and Practice Note, Non-Compete Agreements with Employees: Protection in the Absence of Non-Competes: Inevitable Disclosure.

For more on litigating DTSA claims, see Practice Note, Employment Litigation: DTSA Claims.

Additional Claims

Employers investigating suspected trade secret misappropriation or the potential inevitable disclosure of trade secrets should consider whether alternative causes of action also apply. The employer may be able to obtain compensation for damages it has suffered by using alternative legal claims such as:

- Breach of contract.
- Common law torts.
- Violation of the Computer Fraud and Abuse Act (CFAA).

Because the burden of proof and available relief are not the same under each claim, employers should consider each claim to maximize their chances of recovery. Although beyond the scope of this Note, additional claims may be available if an employer involves law enforcement to pursue claims of, for example:

- Conspiracy.
- Criminal trade secret theft under the Economic Espionage Act of 1996.
- Mail or wire fraud.

(See Contacting Law Enforcement.)

Breach of Contract

Breach of contract claims can be based on:

- A non-compete agreement if the former employee is working for a competitor in violation of the agreement (see Standard Document, Employee Non-Compete Agreement).
- A non-solicitation agreement if the former employee is soliciting customers or employees in violation of the agreement (see Standard Clause, Non-Solicitation Clause).
- A nondisclosure or confidentiality agreement if the former employee disclosed confidential or trade secret information to the employee's new employer or another party (see Standard Document, Employee Confidentiality and Proprietary Rights Agreement).

(See Practice Notes, Protection of Employers' Trade Secrets and Confidential Information: Breach of Contract and Preparing for Non-Compete Litigation).

For more on breach of contract claims generally, see Practice Note, Asserting Breach of Contract Claims.

Tortious Interference with Contract

An employer should consider a tortious interference with contract claim against an employee's new employer. This claim may apply if the new employer was aware that the former employee was a party to a non-compete, non-solicitation, or nondisclosure agreement, and the new employer hired the employee in a capacity where the employee would violate the agreement with the old employer. (See Practice Note, Protection of Employers' Trade Secrets and Confidential Information: Tortious Interference with Contract.)

Often an employer sends a cease and desist letter to the new employer before initiating legal action against it. For a sample letter, and drafting notes about the factors employers should weigh before sending a cease and desist letter, see Standard Document, Restrictive Covenant Cease and Desist Letter to New Employer.

For more about tortious interference claims generally, see Practice Note, Tortious Interference: Asserting a Claim.

Breach of Duty of Loyalty or Fiduciary Duty

Under the laws of most states, employees owe a duty of loyalty to their employers. Employers that discover a former employee acted contrary to their interests while still employed may also have a claim for breach of that duty. (See Practice Note, Protection of Employers' Trade Secrets and Confidential Information: Breach of Duty of Loyalty or Fiduciary Duty.)

For information on state common law duties prohibiting employees from disclosing employer information, see Trade Secret Laws: State Q&A Tool: Question 16.

For more about fiduciary duty claims generally, see Practice Note, Breach of Fiduciary Duty: Asserting a Claim.

Defamation

Employers may consider a defamation claim if a former employee or the new employer made defamatory statements to:

- The former employer's customers in an effort to encourage them to transfer their business to the new employer.
- Former coworkers in an attempt to recruit them.

For more about defamation claims generally, see Practice Note, Defamation Claims in Employment and Defamation in Employment References State Laws Chart: Overview.

Unfair Competition or Tortious Interference with Business

Employers may have a claim for tortious interference if a former employee or the new employer, or both, took an unprivileged action in an effort to interfere with the former employer's business relationships. This claim is also known as tortious interference with:

- Business relations.
- Prospective economic advantage.
- Expectancy.

For more about tortious interference with business relationship claims, see Practice Note, Tortious Interference: Asserting a Claim: Elements of Tortious Interference with Business Relationship.

Violation of the CFAA

The CFAA provides a civil cause of action against employees who access a protected computer without authorization or exceed their authorized access (18 U.S.C. § 1030). For many years, there had been a circuit split about the breadth of the CFAA and the meaning of these terms (see *Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 668-71 (E.D. Pa. 2018) (summarizing circuit split)). Some jurisdictions took a broad approach, holding that the CFAA covered claims against a former employee who accessed the employer's computer system and obtained the employer's information for an illegitimate purpose, even if the individual was still an employee and otherwise was authorized to access the computer system (see, for example, *Int'l Airport Ctrs, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2005)). In other jurisdictions, courts interpreted the CFAA more narrowly, holding that an employee's access was not without authorization and did not exceed the employee's authorized access under similar circumstances (see, for example, *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 205 (4th Cir. 2012)).

On June 3, 2021, the US Supreme Court resolved this circuit split, adopting the more narrow reading of the statute (*Van Buren v. U.S.*, 141 S. Ct. 1648, 1652-62 (2021) (reversing police officer's criminal conviction under the CFAA because he was authorized to access the information)). The Court held that individuals who access information in violation of policy or with improper motives are not covered by the CFAA if the information is otherwise available to them. The *Van Buren* decision will make it more difficult to assert CFAA claims against current or former employees who were authorized to

access an employer's confidential information but merely used it for improper purposes, such as unfairly competing with the employer or misappropriating trade secrets.

The CFAA also may not provide an appropriate remedy for misappropriation in the employment context, as plaintiffs must plead "damage or loss" (18 U.S.C. § 1030(e), (g)). Many courts have found that damages typically associated with misappropriation claims, such as lost profits and goodwill, are not a loss covered by the CFAA because they are not caused by an "interruption of service" as required by the statute (*Millenium Home Mtg. LLC v. Thierry*, 2019 WL 4015626, at *3-4 (E.D. Pa. Aug. 26, 2019) (citing cases where courts have rejected lost profits and related damages under the CFAA); see also *BCRS1, LLC v. Unger*, 2021 WL 3667094, at * (E.D.N.Y. Aug. 18, 2021) ("loss" in the CFAA context "does not include damage to . . . lost revenue due to unfair competition"); *Pipeline Production Inc. v. S&A Pizza, Inc.*, 2021 WL 4811206, at *6 (W.D. Mo. Oct. 14, 2021) (damage or loss generally requires "an actual computer impairment") (internal citations omitted); *Teva Pharm.*, 291 F. Supp. 3d at 674).

For more on CFAA claims generally, see Practice Note, Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation.

Discovery

Interrogatories and written document requests in trade secret misappropriation cases typically seek information about:

- The employee's skill set and duties.
- The employee's access to confidential and trade secret information, including the nature and extent of the employee's access to confidential computer databases and files.
- Any agreements between the employer and employee, including any restrictive covenants.
- The employee's acknowledgment of and agreement to the employer's policies.
- The employee's wrongful acts of appropriation, including the information and materials misappropriated.
- Collaborative or conspiratorial conduct by the employee and other employees or third parties.
- The employee's contacts and communications with the new employer.
- The employee's contacts and communications with any corporate recruiter involved in the employee's hire by the new employer.
- The policies and practices and any relevant acts of the new employer.
- Records of the new employer's knowledge or use of the former employer's trade secrets, including existing and deleted computer files.
- Indemnification by the new employer of the former employee for claims arising from breach of restrictive covenants or trade secret violations.
- Social media posts and other electronic communications, such as:
  - posts and private messages on social media sites such as Facebook, LinkedIn, or Instagram;
  - communications using workplace collaboration tools, such as chats on Microsoft Teams; and
  - communications using ephemeral messaging applications such as Confide, Telegram, or Wickr, if available (see Practice Note, Ephemeral Messaging: Balancing the Benefits and Risks).

Expedited Discovery

Employers requesting injunctive relief (see Injunctive Relief) should consider requesting that the court permit discovery on an expedited schedule in advance of the hearing. Employers should:

- Narrowly tailor discovery requests to the issues that are essential to the hearing on injunctive relief.
- Emphasize the potential harm the employer is attempting to prevent.
- Demonstrate the reasonableness of the requested information by attaching the proposed discovery requests to the employer's motion for injunctive relief.

Obtaining Relief for Trade Secret Misappropriation

Depending on the facts of the case, the jurisdiction, and the claims alleged, an employer should consider drafting its complaint to include a prayer for relief seeking:

- Temporary, preliminary, or permanent injunctive relief.
- A seizure order under the DTSA (see Remedies Under the DTSA).

- Monetary damages, comprised of any combination of:
  - lost profits;
  - the wrongdoer's unjust enrichment caused by the misappropriation;
  - a reasonable royalty, where damages are difficult to calculate; and
  - exemplary damages under the DTSA or applicable state law.
- Costs.
- Attorneys' fees.
- Pre- and post-judgment interest.

Injunctive Relief

Typically the goal in filing a misappropriation of trade secrets lawsuit is not simply to recover damages, but first and foremost to recover the trade secrets and prevent the misappropriation from inflicting any additional (and often difficult to quantify) harm on the employer. This means that in most cases, employers request that a court issue an injunction in addition to damages.

In a trade secrets case, a temporary restraining order (TRO) may:

- Direct the return of purported trade secret information.
- Prohibit the use or disclosure of trade secret information.
- Prohibit a party from violating a restrictive covenant such as a non-compete or non-solicitation agreement.

(See Practice Note, Preparing for Non-Compete Litigation: Requesting Injunctive Relief.)

Federal courts traditionally consider four factors when evaluating a motion for a preliminary injunction or TRO:

- The moving party's likelihood of success on the merits.
- The likelihood that the moving party will suffer irreparable harm absent preliminary injunctive relief.
- The balance of harms between the moving party and the non-moving party.
- The effect of the injunction on the public interest.

The federal circuits vary in how they weigh these factors. Some circuits apply a balancing test, allowing a weaker showing in one factor to be offset by a stronger showing in another. Other circuits apply the traditional factors sequentially, requiring sufficient demonstration of all four before granting preliminary injunctive relief. For more on the standards for relief in federal court, see Standard for Preliminary Injunctive Relief by Circuit Chart.

Monetary Damages

In addition to injunctive relief, several types of damages are typically available for trade secret misappropriation.

Employers typically request compensatory damages that result from the misappropriation of trade secrets. Under Section 3 of the UTSA, damages can include both:

- The actual loss to the employer caused by misappropriation.
- To the extent the former employee or the new employer, or both, used misappropriated trade secrets, the unjust enrichment caused by misappropriation that is not taken into account in computing the employer's actual loss.

(Unif. Trade Secrets Act § 3.)

At times, damages in trade secret misappropriation cases depend on future events or sales and therefore are difficult to quantify. In those cases, the damages caused by misappropriation may be measured by the imposition of liability for a reasonable royalty for the employee's unauthorized disclosure or use of a trade secret.

If willful and malicious misappropriation exists, the court may award exemplary damages. Nearly all state laws follow the UTSA and permit exemplary damages limited to double the underlying award (see, for example, 765 Ill. Comp. Stat. § 1065/4(b)).

Similar damages are available under the DTSA (see Remedies Under the DTSA).

Courts have several tools at their disposal to ensure that damages are calculated accurately under the circumstances, such as the ability to:

- Appoint a special master.
- Award pre-judgment interest.
- Order an equitable accounting.

Attorneys' Fees

In addition to damages, successful employers can sometimes recover the attorneys' fees they incur in bringing a trade secret misappropriation case if the misappropriation is willful and malicious. Under Section 4

of the UTSA, attorneys' fees can also be awarded to a prevailing party where:

- A claim of misappropriation is made in bad faith.
- A motion to terminate an injunction is made or resisted in bad faith.

(Unif. Trade Secrets Act § 4.)

The DTSA also allows for the recovery of attorneys' fees if the employer complied with the notice of immunity requirement, if applicable (see Remedies Under the DTSA).

Remedies Under the DTSA

The remedies under the DTSA are similar to those under the UTSA. Available remedies include:

- An injunction to preserve evidence and prevent trade secret disclosure, provided that it does not:
  - prevent a person from entering into an employment relationship, and that any conditions placed on the employment relationship are based on evidence of threatened misappropriation and not merely on the information the person knows; or
  - otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business.
- Compensatory damages measured by:
  - actual loss and unjust enrichment, to the extent not accounted for in the actual loss calculation; or
  - a reasonable royalty for the unauthorized disclosure or use of the trade secret.
- Exemplary damages up to two times the amount of the damages for willful and malicious misappropriation.
- Reasonable attorneys' fees for the prevailing party if:
  - a misappropriation claim is made in bad faith;
  - a motion to terminate an injunction is made or opposed in bad faith; or
  - a trade secret was willfully and maliciously misappropriated.

(18 U.S.C. § 1836(b)(3); see also Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist.)

Unlike the UTSA, the DTSA also permits the court to issue an ex parte seizure order (18 U.S.C. § 1836(b)(2)). The DTSA includes protections designed to prevent abuse of this powerful remedy and only allows an ex parte seizure order under extraordinary circumstances. A party seeking an ex parte seizure order must demonstrate as a threshold matter that an order granting injunctive relief under FRCP 65 would be futile (18 U.S.C. § 1836(b)(2)(A)(ii)). The courts have set a high bar for making this showing.

For more information on the civil seizure of property under the DTSA, see Article, Expert Q&A on DTSA Seizure Orders.

Preparing for Potential Defenses and Counterclaims

Although a defendant's defenses may vary by claim and circumstance, employers can make a complaint less susceptible to attack by anticipating several common defenses.

The Information Is Not a Trade Secret

Former employees' and new employers' first line of defense often is claiming that the information at issue is not a trade secret. Employers should take the following steps in anticipation of that argument.

Do Not Overreach on What Is Claimed as a Trade Secret

Typically, defendants scrutinize a complaint for categories of information that are purportedly trade secrets but are actually publicly available. For example, if an employer claims that its pricing (rather than the methodology by which it sets its pricing) is a trade secret, the employee or new employer may argue that pricing is disclosed to third-party customers and potential customers and, as a result, is not secret. Employers should only claim that information is a trade secret if they have evidence to support the claim and if that information is pertinent to the facts of the case.

Consider What Information Is Common Industry Knowledge

Defendants also frequently try to undermine the claim that information is secret by arguing that the information is commonly known in the industry. To fuel that argument, defendants look to their peers at other companies that compete with the employer to obtain testimony that the other companies' employees know this information, as well. For example, if an employer claims that its manufacturing process is a trade secret, the defendant may try to obtain testimony from the employer's competitor demonstrating that it knows the details of the employer's manufacturing process. Employers should consider what information may be known by the

employer's competitors when deciding what information the employer claims is a trade secret.

Explain How the Employer Protects Its Trade Secrets

After attacking the secrecy of the information, defendants often argue that the employer did not take appropriate steps to protect the secrecy (or purported secrecy) of the information. For example, defendants may argue that:

- The employer did not have a policy defining and protecting its confidential information.
- The employer did not require employees to sign nondisclosure or confidentiality agreements.
- The employer did not train its employees on its confidentiality policy or duty to safeguard confidential information.
- The employer did not follow its confidentiality policy.
- The employer permitted employees unfettered access to files, computer systems, and information.
- The employer did not ask departing employees to return confidential information or did not conduct exit interviews.
- Employees shared this information with clients and competitors.

(Compare, for example, *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888 (N.D. Ill. 2019) (denying preliminary injunction because plaintiff did "virtually nothing to protect" its trade secrets) with *Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115 (N.D. Ill. 2019) (granting injunctive relief and noting all the steps the plaintiff took to protect its trade secrets).)

Employers should describe all efforts they take to protect the secrecy of their trade secrets in their complaints. All policies, training, access restrictions, and restrictive covenants that are used to protect that information should be identified. For a sample confidentiality policy, see Standard Document, Confidential Information Policy. For a sample confidentiality agreement, see Standard Document, Employee Confidentiality and Proprietary Rights Agreement.

For information on what efforts to maintain secrecy have been deemed reasonable or sufficient for trade secret protection under state law, see Trade Secret Laws: State Q&A Tool: Question 8.

The Information Was Not Misappropriated

Defendants often argue that they did not misappropriate any information. Without surveillance footage of a former employee leaving the office with files or the hard drive from the copy machine showing mass copying of sensitive files, it can be difficult to establish otherwise. An employer's initial investigation is often the key to demonstrating the information was misappropriated. Employers, therefore, should ensure that their initial investigation includes reviewing any records concerning access to the physical work environment, as well as electronically stored information.

Typically, the best evidence of a former employee's misconduct is contained in the employee's computer and email files. Creating a forensic image of the hard drive from the former employee's work computer and examining that forensic image and emails for any evidence of inappropriate activities can help an employer successfully demonstrate that the employee misappropriated the employer's information.

For more on preserving electronically stored information, see Practice Note, Preparing for Non-Compete Litigation: Preserving Electronic Evidence.

For more on the defenses available under state law, see Trade Secret Laws: State Q&A Tool: Question 11.

Preparing for Potential Counterclaims

When considering initiating litigation, employers should consider the possibility that their former employee and the employee's new employer may file counterclaims. The universe of potential counterclaims is limited only by the imagination of former employees and their new employers. However, counterclaims can often include claims of:

- Unpaid wages or commissions.
- Discrimination.
- Retaliation.
- Damage caused by wrongful seizure under the DTSA (18 U.S.C. § 1836(b)(2)(G)).

Plaintiffs also may assert tortious interference claims arising from cease and desist letters. To minimize the risk of a tortious interference claim, employers should avoid sending a cease and desist letter if the allegations of trade

secret misappropriation may be found to be baseless. (See Standard Document, Restrictive Covenant Cease and Desist Letter to New Employer: Drafting Note: Potential Risks of Sending a Cease and Desist Letter.)

Maintaining Confidentiality During Litigation

Employers that file a lawsuit concerning trade secrets should take appropriate steps to prevent their trade secrets from being publicly exposed. The UTSA and many states' trade secrets laws specifically authorize courts to take appropriate steps to protect alleged trade secrets. This may include:

- Granting a protective order in connection with discovery proceedings.
- Holding in-camera hearings.
- Sealing the records of the action (see Practice Note, Filing Documents in Federal District Court: Filing Documents Under Seal).
- Ordering persons involved in the litigation not to disclose an alleged trade secret without prior court approval.

(Unif. Trade Secrets Act § 5.)

Typically employers protect their trade secrets by requesting that the court enter a protective order (see Practice Note, Protective Orders: Overview (Federal)). In general, courts are familiar with and typically willing to enter protective orders in trade secrets cases. Because they simply provide procedural protections and do not substantively affect the facts in dispute, protective orders are commonly submitted with the agreement of all parties. Many courts, however, have local rules that govern the drafting of protective orders. Therefore, counsel should review the local rules before requesting that the court enter a protective order.

The DTSA codifies the obligation to seal trade secrets in court proceedings, a benefit which may not be as readily available in state court (18 U.S.C. § 1835). Where the court orders the civil seizure of property under the DTSA, the court may take appropriate action to protect the:

- Seized property from disclosure (18 U.S.C. § 1836(b)(2)(B)(iii)).
- Person against whom seizure is ordered from publicity (18 U.S.C. § 1836(b)(2)(C)).
- Confidentiality of seized materials unrelated to the trade secret information that was ordered seized (18 U.S.C. § 1836(b)(2)(D)(iii)).