PRACTICAL LAW
THE JOURNAL

Trade Secret Claims in Employment Litigation

Guidance for employers and their counsel on navigating litigation involving trade secret misappropriation, including pre-litigation steps, cease and desist letters, forum selection, choice of law, claims, defenses, discovery, remedies, and confidentiality issues.

PETER A. STEINMEYER
MEMBER
EPSTEIN BECKER & GREEN, P.C.

Pete is managing shareholder of the firm's Chicago office. He counsels employers on a wide variety of workplace challenges, including protecting trade secrets and other valuable information and employee discipline and discharge. Pete also leads investigations of alleged workplace misconduct, such as harassment and retaliation.

Reprinted from Practical Law The Journal with permission of Thomson Reuters

Trade secrets are often an employer's most valuable assets. When a current 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 the trade secrets.
- Recovering the trade secrets.
- Obtaining relief.

This article discusses key issues related to trade secret litigation, including:

- Preliminary steps before commencing an action, such as sending a cease and desist letter and contacting law enforcement.
- Considerations when filing a legal action.
- Common causes of action.
- Discovery, including expedited discovery.
- Injunctive relief, damages, and attorneys' fees.
- Best practices for preparing to rebut potential defenses and counterclaims.
- Maintaining confidentiality during trade secret litigation.

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

PRELIMINARY STEPS

The employer and its counsel should consider several preliminary steps when they suspect or learn of trade secret misappropriation.

INVESTIGATING THE SUSPECTED MISAPPROPRIATION

A prompt and thorough investigation can be critical to successful trade secret litigation. One of the first steps in an investigation is identifying the employer's information that is truly confidential and valuable because it remains confidential. 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:

- Emails (especially emails sent to an employee's personal email account).
- Desktop and laptop computers (including indicia that USB memory devices have been plugged in to transfer information).
- 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 can not only conduct the investigation but also preserve the information and later act as an 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:

- The employee 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 new employer's use or disclosure of the employer's trade secret information.

An employer's investigation into suspected trade secret misappropriation also typically includes gathering information about the employee's new employer and business (for more on investigating a former employee's new employer when misconduct is suspected, see Preparing for Non-Compete Litigation on Practical Law).

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 to litigation. A cease and desist letter typically:

- Reminds the former employee of their contractual and other obligations to the employer.
- Advises the former employee to cease and desist from conduct that violates their obligations.
- Where appropriate, demands 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.

The employer should investigate and substantiate its allegations of trade secret misappropriation before sending a cease and desist letter. Otherwise, it may face a tortious interference claim from the employee or the employee's new employer (see *Preparing for Potential Counterclaims* below).

(For model cease and desist letters, with explanatory notes and drafting tips, see Restrictive Covenant Cease and Desist Letter to Former Employee and Restrictive Covenant Cease and Desist Letter to New Employer on Practical Law.)

CONTACTING LAW ENFORCEMENT

When an employer suspects criminal conduct, in addition to or instead of sending one or more cease and desist letters, it may contact law enforcement to investigate and prosecute trade secret theft. 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, foreign instrumentality, or 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 secret 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 avoid unnecessarily disclosing sensitive, confidential, or trade secret information. However, there remains a risk that the employer's trade secrets will be disclosed, purposefully or inadvertently, if disclosure would help the prosecution of the case.

FILING A LEGAL ACTION

Before commencing a legal action, counsel must consider several threshold issues.

FORUM SELECTION

Unless the employer and employee 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 (see *DTSA* below; for more on forum selection in DTSA cases, see Employment Litigation: DTSA Claims on Practical Law). Typically, the circumstances of the case help an employer determine the most advantageous option.

(For more on forum selection issues, see Choice of Law and Choice of Forum: Key Issues on Practical Law.)

CHOICE OF LAW

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

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

(For more on choice of law issues, see Choice of Law and Choice of Forum: Key Issues on Practical Law.)

DECIDING WHETHER TO NAME THE EMPLOYEE'S NEW EMPLOYER IN THE ACTION

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

- The former employee was acting under the new employer's direction when the employee misappropriated the former employer's trade secrets.
- The new employer agreed to indemnify the former employee for any liability arising out of the employee's:
  - transition 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.

DECIDING WHETHER TO NAME THIRD PARTIES IN THE ACTION

In addition to naming the former employee and the new employer in the complaint, an employer should consider naming any third parties who:

- Procured or assisted in the trade secret misappropriation.
- Received the trade secrets.

Naming third-party defendants in the lawsuit can help ensure the return of all copies or derivatives of the trade secrets. The employer may also be able to obtain discovery more easily than using the third-party subpoena discovery process (for a collection of resources on the subpoena process, see Subpoena Toolkit (Federal) on Practical Law).

COMMON CAUSES OF ACTION

An employer seeking to pursue litigation for trade secret misappropriation or the potential disclosure of trade secrets should consider various causes of action.

MISAPPROPRIATION OF TRADE SECRETS

The most common claim against an employee who uses or discloses an employer's 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.

With the exception of New York, all states and the District of Columbia have enacted a version of the model Uniform Trade Secrets Act (UTSA), and the elements for a misappropriation claim under the laws of those states are similar. Typically, to bring a claim under state law, an employer 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 new employer's business.
- The employer suffered or will suffer damages.

DTSA

The DTSA creates a private cause of action for civil trade secret misappropriation under federal law and provides certain protections for whistleblowers who disclose trade secrets to report suspected illegal conduct. The DTSA supplements — rather than preempts — state law remedies for trade secret misappropriation (18 U.S.C. § 1836(b); for more on how the DTSA affects existing state non-compete laws, see Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers on Practical Law). It applies only to misappropriation occurring on or after May 11, 2016.

(For more on the DTSA, see Employment Litigation: DTSA Claims and Expert Q&A on DTSA Seizure Orders on Practical Law.)

Key Terms and Available Remedies

The DTSA uses the definition of trade secret contained in the Economic Espionage Act of 1996 (EEA) (18 U.S.C. §§ 1831 to 1839). Under that definition, a trade secret is business or scientific information that:

- Derives independent economic value from not being generally known to or readily ascertainable 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 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 the person's material change in position:
  - knew or had reason to know that the information was a trade secret; and
  - acquired knowledge of the trade secret by accident or mistake. (18 U.S.C. § 1839(5).)

The term "improper means" includes:

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

However, the DTSA expressly states that "improper means" does not include:

- Reverse engineering.
- Independent derivation.
- Any other lawful means of acquisition. (18 U.S.C. § 1839(6)(B).)

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 or service 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 statutory or common law claims (for example, misappropriation of trade secrets, breach of a confidentiality or non-compete agreement, or unfair competition). A DTSA civil action may be brought in federal district court and must be commenced 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(c) and (d).)

Remedies under the DTSA are similar to those under the UTSA (see *Remedies Under the DTSA* below). Notably, the DTSA does not affect existing state law inevitable disclosure theories, except that the standard for obtaining injunctive relief may be different in federal than in state court (see *Inevitable Disclosure of Trade Secrets* below).

Whistleblower Protections

The DTSA provides criminal and civil immunity under any federal or state trade secret law to whistleblowers who disclose trade secrets if the disclosure is either:

- 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.
- Included in a complaint or other document filed under seal in a lawsuit or other proceeding (for more information, see Filing Documents Under Seal in Federal Court on Practical Law). (18 U.S.C. § 1833(b).)

The DTSA's whistleblower immunity may apply to claims asserted under state law but must be pled as an affirmative defense (see, for example, *Gatti v. Granger Med. Clinic, P.C.*, 529 F. Supp. 3d 1242, 1266-67 (D. Utah 2021)).

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

(For a model clause providing notice of whistleblower immunity under the DTSA, with explanatory notes and drafting tips, see Notice of Immunity Under the Defend Trade Secrets Act (DTSA) Provision on Practical Law.)

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 when the former employee cannot perform their new job without relying on their knowledge of the former employer's trade secrets or disclosing the trade secrets to the new employer. An employer alleging this type of claim may argue that it is inevitable that the former employee will:

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

Not every state recognizes claims for the inevitable disclosure of trade secrets. In jurisdictions that do recognize this cause of action, an employer should emphasize in its pleadings, as applicable, 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 other trade secrets.
- It would be impossible for the former employee to perform their new job without using or disclosing the trade secrets.
- Circumstances support or highlight the employer's concerns, such as the former employee being dishonest or misleading about their departure (*Prime Therapeutics LLC v. Beatty*, 354 F. Supp. 3d 957, 969-70

(D. Minn. 2018) (finding that the plaintiff failed to establish the likelihood of the employee's inevitable disclosure where the employee was forthcoming and the new employer made efforts to differentiate the employee's new role)).

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 Pepsi's strategic plans to gain market share.
- The high-level executive resigned from Pepsi to work for Quaker.
- It would have been impossible for the former executive to perform their job at Quaker in that same niche market without bearing in mind Pepsi's strategic plans.
- Pepsi's concern was well-founded because the former executive had been dishonest about the scope of their new position at Quaker when they left Pepsi. (54 F.3d 1262 (7th Cir. 1995).)

Put another way, an employer seeking application of the inevitable disclosure doctrine against a former employee should be able to demonstrate 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.

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 when the employee is not violating any contractual or other obligation.
- There is often no evidence that the employee misappropriated trade secrets or otherwise did anything wrong.

A court's application of the inevitable disclosure doctrine depends on a fact-specific analysis of factors, such as:

- The degree of competition between the former and new employers (for example, close rivals like Coke and Pepsi versus less directly competitive employers).
- The similarity between the employee's former and new positions.
- Any actions taken by the new employer to prevent the employee from using or disclosing the former employer's trade secrets. (*Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1140 (N.D. Ill. 2019) (finding a likelihood of success on the merits that the plaintiff would inevitably disclose trade secrets to the new employer), overruled in part on other grounds, *DM Trans, LLC v. Scott*, 38 F.4th 608 (7th Cir. 2022).)

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

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

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

However, other courts have reached contrary conclusions (see, for example, *Aon PLC v. Alliant Ins. Servs., Inc.*, 2023 WL 3914886, at *5 (N.D. Ill. June 9, 2023) (holding that the inevitable disclosure doctrine "appears to be foreclosed" under the DTSA); *IDEXX Labs., Inc. v. Bilbrough*, 2022 WL 3042966, at *3-6 (D. Me. Aug. 2, 2022) (ruling that "based on the plain language of the statute, the inevitable disclosure doctrine does not apply to claims brought pursuant to [the] DTSA"); *Kinship Partners, Inc. v. Embark Veterinary, Inc.*, 2022 WL 72123, at *7 (D. Or. Jan 3, 2022) (finding that the DTSA does not support an injunction based on the inevitable disclosure doctrine)).

(For more on the inevitable disclosure doctrine, see Non-Compete Agreements with Employees on Practical Law.)

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 by using alternative legal claims such as:

- Breach of contract.
- Common law torts.
- Violation of the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030). However, CFAA claims are less commonly asserted in trade secret misappropriation cases because:
  - the DTSA now provides a more direct path to federal court; and
  - the US Supreme Court has limited the scope of plausible CFAA claims in the employment context.

(For more on claims for breach of contract and common law torts, see Protection of Employers' Trade Secrets and Confidential Information on Practical Law; for more on CFAA claims, see Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation on Practical Law.)

Because the burden of proof and available relief differ across claims, an employer should consider asserting all applicable claims to maximize its chances of recovery. Additional claims may be available if an employer involves law enforcement to pursue claims of, for example:

- Conspiracy.
- Criminal trade secret theft under the EEA.
- Mail or wire fraud.

Breach of Contract

A breach of contract claim may be based on:

- A non-compete agreement, if the former employee is working for a competitor in violation of the agreement (for a model non-compete agreement, with explanatory notes and drafting tips, see Employee Non-Compete Agreement on Practical Law).
- A non-solicitation agreement, if the former employee is soliciting customers or employees in violation of the agreement (for a model non-solicitation clause, with explanatory notes and drafting tips, see Non-Solicitation Clause on Practical Law).
- A nondisclosure or confidentiality agreement, if the former employee disclosed confidential or trade secret information to the new employer or another party (for a model agreement between an employer and an employee concerning the appropriate handling of the employer's confidential information, with explanatory notes and drafting tips, see Employee Confidentiality and Proprietary Rights Agreement on Practical Law).

(For more on breach of contract claims, see Asserting Breach of Contract Claims on Practical Law.)

Tortious Interference with Contract

An employer should consider a tortious interference with contract claim against a former employee's new employer. This claim may apply if the new employer was aware that the 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 that agreement.

Often, an employer sends a cease and desist letter to the new employer before initiating legal action against it (for a model cease and desist letter that an employer may send to a former employee's new employer, with explanatory notes and drafting tips, see Restrictive Covenant Cease and Desist Letter to New Employer on Practical Law).

(For more on tortious interference with contract claims, see Tortious Interference: Asserting a Claim on Practical Law.)

Breach of Duty of Loyalty or Fiduciary Duty

Under the laws of most states, an employee owes a duty of loyalty to their employer during the employment relationship. An employer that discovers a former employee acted contrary to the employer's interests while employed may have a claim for breach of that duty.

Officers and directors of a corporation also owe a fiduciary duty to the entity. Many officers serve as employees involved in day-to-day business operations. Therefore, the employer may have a claim for breach of the duty of care against an officer or director who acts against the employer's interest, such as by using or misappropriating the employer's trade secrets for their own or another's benefit.

(For more on fiduciary duties, see Fiduciary Duties of Officers of Corporations and Fiduciary Duties of the Board of Directors on Practical Law; for more on fiduciary duty claims, see Breach of Fiduciary Duty: Asserting a Claim on Practical Law.)

Defamation

An employer 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.
- The employee's former coworkers in an attempt to recruit them.

(For more on defamation claims, see Defamation Claims in Employment and Defamation in Employment References State Law Chart: Overview on Practical Law.)

Tortious Interference with Business Relationships

An employer may have a claim for tortious interference with business relationships 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:

- Prospective economic advantage.
- Business expectancy.

(For more on tortious interference with business relationships claims, see Tortious Interference: Asserting a Claim on Practical Law.)

DISCOVERY

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

- The employee's skill set and duties.
- The nature and extent of the employee's access to confidential and trade secret information, including computer databases and files.
- Any agreements between the employer and employee, including restrictive covenants.
- The employee's acknowledgment of and agreement to the employer's policies.
- The employee's acts of misappropriation, including the information and materials misappropriated.

- Collaborative or conspiratorial conduct by the employee with 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 new employer's hiring of the employee.
- The new employer's policies and practices and any relevant acts.
- Records of the new employer's knowledge or use of the former employer's trade secrets, including existing and deleted computer files.
- Any indemnification by the new employer of the employee for claims arising from breach of restrictive covenants or trade secret violations.
- Social media posts and other electronic communications, for example:
  - posts and private messages on social media sites, such as Facebook, LinkedIn, and Instagram;
  - communications using workplace collaboration tools, such as chats on Microsoft Teams; and
  - communications using ephemeral messaging applications, such as Confide, Telegram, and Wickr (for more information, see Ephemeral Messaging: Balancing the Benefits and Risks on Practical Law).

An employer seeking injunctive relief should consider requesting that the court permit discovery on an expedited schedule in advance of the hearing and:

- Narrowly tailor discovery requests to the issues that are essential to the hearing on injunctive relief.
- Emphasize the potential harm that 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.

(For more on discovery and preserving electronically stored information in trade secret litigation, see E-Discovery in Trade Secret and Restrictive Covenant Litigation Involving Former Employees on Practical Law.)

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.
- Monetary damages, comprised of any combination of:
  - lost profits;
  - the wrongdoer's unjust enrichment from 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.
- A seizure order under the DTSA.

INJUNCTIVE RELIEF

Typically, the first and foremost goal in filing a trade secret misappropriation lawsuit is to recover the trade secrets and prevent the misappropriation from inflicting additional (and often difficult-to-quantify) harm on the employer. This means that, in most cases, an employer asks the court to issue an injunction in addition to damages.

In a trade secret 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.

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 stronger showing in one factor to offset a weaker showing in another. Other circuits apply the traditional factors sequentially, requiring sufficient demonstration of all four factors before granting preliminary injunctive relief. (For a chart on the legal standard that each federal circuit applies when evaluating a motion for a preliminary injunction or TRO, see Standard for Preliminary Injunctive Relief by Circuit Chart on Practical Law.)

MONETARY DAMAGES

In addition to injunctive relief, several types of damages are typically recoverable for trade secret misappropriation. Employers often request compensatory damages that result from the misappropriation of trade secrets. Under Section 3 of the UTSA, damages may include both:

- The employer's actual loss caused by the misappropriation.
- To the extent the former employee or the new employer, or both, used misappropriated trade secrets,

the unjust enrichment caused by the misappropriation that is not accounted for 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, a court may measure damages for misappropriation by imposing 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 (for example, 765 ILCS 1065/4(b)). Similar damages are available under the DTSA.

To ensure that damages are calculated accurately under the circumstances, courts have the ability to:

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

(For more information, see Trade Secret Valuation on Practical Law.)

ATTORNEYS' FEES

In addition to damages, a prevailing employer may recover the attorneys' fees it incurs 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 misappropriation claim 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.

REMEDIES UNDER THE DTSA

Remedies under the DTSA, similar to those under the UTSA, 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 employment relationship are based on evidence of threatened misappropriation, 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 of up to two times the amount of the damages for willful and malicious misappropriation.
- Reasonable attorneys' fees for the prevailing party if:
  - the misappropriation claim was made in bad faith;
  - a motion to terminate an injunction was made or opposed in bad faith; or
  - the trade secret was willfully and maliciously misappropriated. (18 U.S.C. § 1836(b)(3); for more information, see Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist on Practical Law.)

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 it in extraordinary circumstances. A party seeking an ex parte seizure order must demonstrate as a threshold matter that an order granting injunctive relief under Federal Rule of Civil Procedure 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 on the civil seizure of property under the DTSA, see Expert Q&A on DTSA Seizure Orders on Practical Law.)

PREPARING FOR POTENTIAL DEFENSES AND COUNTERCLAIMS

Although defenses may vary by claim and circumstance, an employer can make a complaint less susceptible to attack by a defendant-employee (and new employer, if applicable) by anticipating several common defenses.

THE INFORMATION IS NOT A TRADE SECRET

Often, defendants' first line of defense is to claim that the information at issue is not a trade secret. An employer should take the steps discussed below in anticipation of that argument.

Do Not Overreach on What Is Claimed as a Trade Secret

Typically, defendants will 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.

An employer should only claim that information is a trade secret if it has evidence to support the claim and the alleged trade secret information is pertinent to the facts of the case. (For more on what constitutes a trade secret, see Protection of Employers' Trade Secrets and Confidential Information on Practical Law.)

Consider What Information Is Common Industry or Public Knowledge

Defendants also frequently try to undermine a trade secret claim by arguing that the alleged secret information is commonly known in the industry. To support that argument, defendants often seek testimony from peers at competitor companies indicating that they know this information. 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. An employer should consider what information may be known by its competitors when deciding what to assert as a trade secret.

Defendants also may claim that certain information is publicly available and therefore does not qualify for trade secret protection. While matters of public knowledge generally are not trade secrets, a compilation of public and non-public information may be protectable (see, for example, *Allstate Ins. Co. v. Fougere*, 79 F.4th 172, 189-90 (1st Cir. 2023) (finding trade secret protection for a spreadsheet containing customer names and addresses, premium rates, and renewal dates that, to the extent publicly available, "could only be recreated at immense difficulty")).

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 its employees to sign nondisclosure or confidentiality agreements.
- The employer did not train its employees on:
  - its confidentiality policy; or
  - the 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 conduct exit interviews.
- Employees shared confidential information with clients or competitors. (Compare *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 898 (N.D. Ill. 2019) (denying a preliminary injunction because the plaintiff did "virtually nothing to protect" its trade secrets) with *Vendavo, Inc.*, 397 F. Supp. 3d at 1136-38 (granting injunctive relief and noting all of the steps the plaintiff took to protect its trade secrets).)

An employer's complaint should detail all efforts made to protect the secrecy of its trade secrets, including all policies, training, access restrictions, and restrictive covenants used to protect the information. (See, for example, *Insulet Corp. v. EOFlow Co. Ltd.*, 104 F.4th 873, 881-82 (Fed. Cir. 2024) (reversing the district court's grant of an injunction where the plaintiff had not taken reasonable steps to keep its information secret and the information could be derived from reverse engineering); *Jacam Chem. Co. 2013, LLC v. Shepard*, 101 F.4th 954, 964-66 (8th Cir. 2024) (holding that pricing information was not entitled to trade secret protection because the plaintiff failed to make reasonable efforts to keep the information secret and customers were under no obligation to keep the information secret).)

(For model documents addressing the appropriate handling of the employer's confidential information, with explanatory notes and drafting tips, see Confidential Information Policy and Employee Confidentiality and Proprietary Rights Agreement on Practical Law; for more on efforts to maintain secrecy that courts have deemed reasonable or sufficient for trade secret protection, see Protection of Employers' Trade Secrets and Confidential Information on Practical Law.)

THE INFORMATION WAS NOT MISAPPROPRIATED

Defendants often argue that they did not misappropriate any information. The employer must provide evidence of misappropriation and may not rely on mere speculation (see, for example, *Morgan Stanley Smith Barney LLC v. Takahashi*, 2025 WL 35134, at *2 (D. Nev. Jan. 6, 2025)).

An employer's initial investigation is often key to demonstrating that information was misappropriated. An employer, therefore, should ensure that its initial investigation includes reviewing any records concerning access to the physical work environment (for example, swipe card access), 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 and examining a forensic image of the hard drive of the former employee's work computer and reviewing the former employee's emails for evidence of inappropriate activities can help an employer successfully demonstrate that the employee misappropriated the employer's information. Such a review might reveal files e-mailed to a personal e-mail account, mass copying via a USB device, or access to databases unrelated to work performed on or around the date of such access. Conversely, an employee's forensic evidence that they deleted or did not access the alleged trade secrets may defeat a misappropriation claim (see, for example, *CAE Integrated, L.L.C. v. Moov Techs., Inc.*, 44 F.4th 257, 262 (5th Cir. 2022)).

(For more on preserving electronically stored information, see Preparing for Non-Compete Litigation on Practical Law.)

PREPARING FOR POTENTIAL COUNTERCLAIMS

Before initiating litigation, an employer should consider the possibility that a defendant may file counterclaims. Various counterclaims could potentially be asserted, such as claims of:

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

A defendant also may assert tortious interference claims or counterclaims arising from cease and desist letters. To minimize the risk of a tortious interference claim, an employer should avoid sending a cease and desist letter if the allegations of trade secret misappropriation may be deemed baseless. (For more on the potential risks of sending a cease and desist letter, see Restrictive Covenant Cease and Desist Letter to New Employer on Practical Law.)

MAINTAINING CONFIDENTIALITY DURING LITIGATION

An employer that files a lawsuit concerning trade secrets should take appropriate steps to prevent its trade secrets from being publicly exposed. The UTSA and many states' trade secret laws specifically authorize courts to take appropriate steps to protect alleged trade secrets. These may include:

- Granting a protective order in connection with discovery proceedings (for a collection of resources on motions for protective orders, see Discovery Motions in Federal Court Toolkit on Practical Law).
- Holding in camera hearings.
- Sealing the records of the action (for more information, see Filing Documents Under Seal in Federal Court on Practical Law).
- Ordering persons involved in the litigation not to disclose an alleged trade secret without prior court approval. (Unif. Trade Secrets Act § 5.)

Typically, an employer protects its trade secrets by requesting that the court enter a protective order. In general, courts are familiar with and typically willing to enter protective orders in trade secret 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). When a 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)).
- The person against whom seizure is ordered from publicity (18 U.S.C. § 1836(b)(2)(C)).
- The confidentiality of seized materials unrelated to the trade secret information that was ordered seized (18 U.S.C. § 1836(b)(2)(D)(iii)).