Defend Trade Secrets Act (DTSA) and Other Legal Claims and Recourse to Protect Employers' Confidential Information and Trade Secrets

A Lexis Practice Advisor® Practice Note by
Bret A. Cohen, Nelson Mullins Riley & Scarborough, LLP, Amanda B. Carozza, and Nicholas W. Armington, Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

Bret Cohen

This practice note provides guidance on legal claims and recourse available to employers to protect their confidential information and trade secrets in the face of potential misappropriation by employees or others. Specifically, this practice note addresses the following issues:

- Recourse for Trade Secret Misappropriation under the Federal Defend Trade Secrets Act (DTSA)
- State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information
- The Economic Espionage Act of 1996 (EEA)
- The Computer Fraud and Abuse Act (CFAA)
- Common Law Tort Claims
- Common Law Contract Claims
- Employee Raiding

For information on the use of restrictive covenants to protect trade secrets and confidential information generally, see the Restrictive Covenants practice notes. For additional practice notes concerning trade secrets, see the Protecting Trade Secrets practice note page. For information on state laws on protecting trade secrets and confidential information, see Non-competes and Trade Secret Protection State Practice Notes Chart. For more information on protecting confidential information at hiring, see Trade Secrets and Confidential Information Protection upon Hiring Checklist. For more information on dealing with trade secrets and confidential information protection upon termination, see Trade Secrets and Confidential Information Protection upon Termination Checklist. For more information on cybersecurity measures to protect confidential information and trade secrets, see Cybersecurity Measures to Protect Employers' Confidential Information and Trade Secrets.

RECOURSE FOR TRADE SECRET MISAPPROPRIATION UNDER THE FEDERAL DEFEND TRADE SECRETS ACT (DTSA)

The Defend Trade Secrets Act of 2016 (DTSA), 130 Stat. 376, allows U.S. employers to protect against and remedy misappropriation of trade secret information in federal court. Before the enactment of the DTSA, in the absence of diversity jurisdiction, employers seeking redress had no choice but to sue in state court. While most states have adopted and codified some version of the Uniform Trade Secrets Act (UTSA), which provides uniform definitions and remedies for trade secret misappropriation, these laws nevertheless tend to differ from state to state both in the text of the laws themselves and in their application. (For information on state trade secret laws, see Non-competes and Trade Secret Protection State Practice Notes Chart.) Bringing suit under the DTSA

allows a party to avail itself of the federal courts, which can be advantageous since federal courts often are more adept at addressing highly complex technical issues arising in trade secret cases. However, bringing a claim under the DTSA can be a double-edged sword, as it can make a case that an employer wishes to keep in state court (for any number of strategic reasons, including taking advantage of more employer-friendly laws or procedures) removable to federal court by the defendant. As a result, employers should think strategically before including a claim under the DTSA, particularly where the employer may prefer to remain in state court.

The DTSA Does Not Preempt Existing State Trade Secret Law

While the DTSA provides trade secret owners with a new federal cause of action, it does not preempt existing state trade secret law regimes. Practically, this means that a trade secret owner can bring parallel state and federal claims for trade secret misappropriation in federal court. See, e.g., Panera, LLC v. Nettles, 2016 U.S. Dist. LEXIS 101473, *4, *10 n.2 (E.D. Mo. Aug. 3, 2016) (noting that, for purposes of analyzing plaintiff's likelihood of success at preliminary injunction stage, the court's analysis focused on the state trade secrets claim, but stating that an analysis under the DTSA would "likely reach a similar conclusion").

Because state trade secret laws may provide slightly different relief than the DTSA, it is important to consider bringing concurrent state and federal trade secret claims to avail the employer of all potential causes of action. When considering filing dual claims under the DTSA and state trade secret law, be cognizant that the definition of trade secret in the DTSA and state trade secret laws may differ. For information on an employer's recourse under state and common law for trade secret misappropriation see State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information, below.

Statutory Definitions: DTSA vs. UTSA

Before bringing a claim pursuant to the DTSA (or state or common law), it is important to understand the definitions of key terms to ensure the employer has a viable claim.

Definition of Trade Secret

A trade secret is generally any commercially valuable information that is not publicly known where reasonable effort is taken to preserve its confidentiality. The DTSA's definition of trade secret is broad, allowing a wide range of proprietary information to fall under its protection.

"Trade secret" is defined as:

> 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:
>
> - The owner thereof has taken reasonable measures to keep such information secret –and–
>
> - 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).

This definition is not significantly different from the definition for trade secret in the UTSA, and contains the familiar requirements of the UTSA that the trade secret "derives independent economic value, actual or potential, from not being generally known," and that the trade secret owner has undertaken reasonable efforts to keep the information secret.

The UTSA definition of trade secret, which is the basis for the definition of trade secret in most state trade secret statutes, is set forth below:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> - Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use –and–
>
> - Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy

Unif. Trade Secrets Act § 1(4).

For information on the UTSA and an employer's recourse for state and common law laws on trade secret misappropriation, see State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information, below.

Although minor, the differences in the definition of trade secret between the DTSA and UTSA is not necessarily insignificant, and litigants have already attempted to exploit these differences. See, e.g., RF Micro Devices, Inc. v. Xiang, 2016 U.S. Dist. LEXIS 91284, *10–13 (M.D.N.C. July 14, 2016) (defendant successfully argued that guilty plea to criminal charge of misappropriation cannot establish liability under state civil trade secret statute with different definition of trade secret). Thus, be sure to argue that the trade secrets at issue meet the definition of trade secret under all applicable statutes.

Definition of Misappropriation

The definition of misappropriation under the DTSA does not differ from the definition for this term under the UTSA, and is as follows:

"Misappropriation" is defined in detail as follows:

- 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–
- Disclosure or use of a trade secret of another without express or implied consent by a person who:
  - Used improper means to acquire knowledge of the trade secret
  - At the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was:
    - Derived from or through a person who had used improper means to acquire the trade secret
    - 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–

- — 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–
- o Before a material change of the position of the person, knew or had reason to know that:
  - — The trade secret was a trade secret –and–
  - — Knowledge of the trade secret had been acquired by accident or mistake

18 U.S.C. § 1839(5); Unif. Trade Secrets Act § 1(2).

For information on the UTSA and an employer's recourse for trade secret misappropriation under state or common law, see State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information, below.

Drafting a DTSA Complaint

When filing suit under the DTSA, it is very important to explain in the complaint why the allegedly misappropriated information qualifies for trade secret protection. It is not enough to simply call something a trade secret in a complaint under the DTSA. Rather, a plaintiff must plausibly allege—at least in general terms—how the information qualifies as a trade secret. Where a plaintiff fails to do so, the complaint is susceptible to dismissal with prejudice. See, e.g., Raben Tire Co., LLC v. McFarland, 2017 U.S. Dist. LEXIS 26051, *5–7 (W.D. Ky. Feb. 24, 2017) (finding plaintiff's failure to set forth in the complaint any measures it took to protect the allegedly misappropriated trade secret information from disclosure fatal to plaintiff's claims, and dismissing the complaint with prejudice); but compare Mission Measurement Corp. v. Blackbaud, Inc., 216 F. Supp. 3d 915, 921 (N.D. Ill. 2016) (explaining that "at the pleading stage, plaintiffs need only describe the information and efforts to maintain confidentiality of the information in general terms," and that "trade secrets need not be disclosed in detail in a complaint alleging misappropriation for the simple reason that such a requirement would result in the public disclosure of the purported trade secrets.").

However, it is necessary to be guarded about how much information about the allegedly misappropriated trade secret the employer discloses during court proceedings. Thus, it is important to balance two important considerations. On the one hand, put a sufficient amount of detail into the complaint to (1) state a claim, (2) show that the allegedly misappropriated information qualifies as a trade secret, and (3) survive a motion to dismiss. On the other hand, limit the amount of detail the employer's trade secret in the pleadings, as public disclosure of a trade secret may cause the information to lose its protected trade secret status. This is an integral yet often difficult balance to strike.

The DTSA makes finding this balance easier by allowing employers to maintain the secrecy of allegedly misappropriated trade secrets during court proceedings. Specifically, the DTSA states:

> [A] court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential.

18 U.S.C. § 1835(b).

Under this provision, the DTSA gives trade secret owners an opportunity to identify what information is subject to trade secret protection and why that information should be shielded from public disclosure. Thus, if trade secret owners make a proper submission, they then have a tool at their disposal to protect trade secret information from disclosure during court proceedings.

DTSA Statute of Limitations

There is a three-year statute of limitations for claims under the DTSA. This period begins when "the misappropriation . . . is discovered or by the exercise of reasonable diligence should have been discovered." 18 U.S.C. § 1836(d). The DTSA generally applies to trade secret misappropriation that occurred on or after the date of the enactment of the Act (May 11, 2016) or began before the Act's enactment and continued after the Act took effect. See, e.g., Arms v. Unified Weapon Sys., 2016 U.S. Dist. LEXIS 132201, *17–19 (M.D. Fla. Sep. 27, 2016) (holding that a trade secret owner may recover under the DTSA when the misappropriation occurs both before and after the effective date if the entire misappropriation is within the three-year limitations period).

DTSA Civil Seizure

The DTSA provides for an ex parte civil seizure mechanism. See 18 U.S.C. § 1836(b)(2). Civil seizure is a preventative tool employed prior to a finding of misappropriation by which a court may "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." Using this tool, an employer aware of a potential misappropriation of its trade secrets may quickly prevent further dissemination of that information during the pendency of a formal DTSA case. Following issuance of a seizure order, the court must hold a seizure hearing where the party who obtained the seizure order has the burden to prove the facts underlying the order.

Civil seizure may be ordered only in "extraordinary circumstances" and requires the moving party to show all the following:

- An order pursuant to Fed. R. Civ. P 65 or other equitable relief would be inadequate.
- An immediate and irreparable injury will occur if seizure is not ordered.
- Harm to the applicant from denial of a seizure order (1) outweighs the harm to the person against whom seizure is ordered and (2) substantially outweighs the harm to any third parties by such seizure.
- The applicant is likely to succeed in showing that the person against whom the order is issued misappropriated or conspired to misappropriate a trade secret through improper means.
- The person against whom the order will be issued has possession of the trade secret and any property to be seized.
- The application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, the matter's location.
- The person against whom seizure is ordered would destroy, move, hide, or otherwise make such matter inaccessible to the court if on notice.
- The applicant has not publicized the requested seizure.

18 U.S.C. § 1836(b)(2)(a).

Only a handful of such requests have been made under the DTSA. As of this writing, we have not identified any request for civil seizure that a court has granted. See, e.g., OOO Brunswick Rail Mgmt. v. Sultanov, 2017 U.S. Dist. LEXIS 2343, at *4–5 (N.D. Cal. Jan. 6, 2017) (denying request for DTSA civil seizure order). Cases where an employee used external digital storage devices and/or cloud storage services to store misappropriated trade secrets may be candidates for use of the civil seizure mechanism, especially if it is clear that the employee may not fully comply with a temporary restraining order (TRO) or preliminary injunction. Regardless of the form of the misappropriated trade secret, to make civil seizure effective, be prepared to

quickly explain to the court what information was stolen, who stole it, and where it is being kept. A well-developed trade secret asset management plan—in which an employer takes proactive steps to identify, value, secure, and protect its trade secrets — will greatly assist in this process.

Seizures under Fed. R. Civ. P. 65

Where the extraordinary circumstances required for a DTSA civil seizure order are not present, litigants seeking redress for trade secret misappropriation have another option in Fed. R. Civ. P. 65. Under Rule 65, a judge may grant a seizure request as part of a TRO or preliminary injunction related to allegations of trade secret theft under the DTSA, and thus potentially avoid the "extraordinary circumstances" requirement of the DTSA civil seizure provision. See, e.g., Magnesita Refractories Co. v. Mishra, 2017 U.S. Dist. LEXIS 10204, *1 (N.D. Ind. Jan. 25, 2017) (court granted a TRO ordering seizure of a former employee's personal laptop because there was a strong likelihood that the employee was conspiring to steal the employer's trade secrets contained on the laptop and the seizure needed to be carried out immediately to prevent the impending harm).

Other Remedies under the DTSA

The DTSA also provides for several remedies other than seizure upon a finding that a party misappropriated a trade secret. See 18 U.S.C. § 1836(b)(3). For instance, a court may grant an injunction to prevent any actual or threatened misappropriation, provided that the injunction does not "prevent a person from entering into an employment relationship," and that any conditions placed on employment are based on "evidence of threatened misappropriation and not merely on the information the person knows." 18 U.S.C. § 1836(b)(3)(A)(i). Where appropriate, an injunction under the DTSA may require affirmative actions to protect the trade secret. 18 U.S.C. 1836(b)(3)(A)(ii). Further, in "exceptional circumstances that render an injunction inequitable," the court may condition future use of the trade secret on the payment of a reasonable royalty. 18 U.S.C. § 1836(b)(3)(A)(iii).

Following a finding of misappropriation, a court may also award damages. 18 U.S.C. § 1836(b)(3)(B). Where the trade secret is "willfully and maliciously misappropriated" a court may award exemplary damages of double the damage amount already awarded. 18 U.S.C. § 1836(b)(3)(C). A court may also award attorney's fees where the misappropriation or claim of misappropriation was in bad faith, or where a party makes or opposes a motion to terminate an injunction in bad faith. 18 U.S.C. § 1836(b)(3)(D).

Inevitable Disclosure Doctrine Unavailable

By requiring actual evidence of threatened misappropriation, the DTSA explicitly rejects the inevitable disclosure doctrine under federal trade secret law.

Inevitable disclosure is a common law doctrine by which a court can prevent a former employee from working for a competitor of his or her former employer where doing so would require the employee to depend upon his or her former employer's trade secret information. See, e.g., PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269–71 (7th Cir. 1995) (upholding injunction preventing former PepsiCo manager from working for Quaker Oats Company because, notwithstanding the fact that he did not take any physical trade secret information, he would inevitably rely on his knowledge of PepsiCo's trade secrets in his new position).

Notwithstanding that the DTSA proscribes application of the inevitable disclosure doctrine in a federal claim for Trade Secret misappropriation, Trade Secret plaintiffs can still allege misappropriation under the inevitable disclosure doctrine pursuant to a state law cause of action where the state common law allows application of the doctrine. Thus, because some states have adopted the inevitable disclosure doctrine and some have not, the choice of jurisdiction is very important for trade secret plaintiffs alleging misappropriation under the DTSA with a pendent state trade secret claim under a theory of inevitable disclosure.

Whistleblower Provision and Notice Provision

As discussed above, the remedies for employers suing former employees for trade secret misappropriation under the DTSA include punitive damages and attorney's fees. To take advantage of these remedies, however, an employer must advise its employees of the existence of the whistleblower immunity in any contract or other employment agreement entered into after the enactment of the DTSA. 18 U.S.C. § 1833(b)(3). As such, advise employer to strongly consider updating their employment policies and agreements going forward to include either the required notice, or a cross-reference to a policy document that includes a statement about the DTSA's whistleblower immunity.

The DTSA also includes a safe harbor for whistleblower employees that provides for immunity from criminal or civil liability under any federal or state trade secret law for disclosure of a trade secret in confidence to an attorney or governmental official "solely for the purpose of reporting or investigating a suspected violation of law," or in a filing in a lawsuit made under seal. See 18 U.S.C. § 1833(b). Employers should be acutely aware of the notice provision within the whistleblower immunity section of the statute because compliance with this notice provision may affect whether an employer can seek certain remedies under the statute.

Sample Notice Language

Below is sample notice language that employers may consider including in employment agreements entered into after enactment of the DTSA:

> Defend Trade Secret Act Trade Secret Disclosure Notice
>
> NOTICE is hereby given that this agreement does not affect any immunity under 18 U.S.C. §§ 1833(b)(1) or (2). For the purposes of these subsections only, which are reproduced below, individuals performing work as contractors or consultants are considered to be employees.
>
> (1) 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) 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.

Overseas Application

The terms of the Economic Espionage Act, which the DTSA modified, allow employers to use the DTSA to address trade secret misappropriation where the theft occurred outside of the United States. Specifically, the EEA includes a provision indicating that the law applies to conduct occurring outside of the United States if:

- The offender is a citizen or permanent resident of the United States
- The offender is a United States corporation –or–
- An act in furtherance of the offense was committed in the United States

18 U.S.C. § 1837.

The option to apply the DTSA to overseas conduct will be immensely valuable because overseas trade secret theft continues to proliferate. The increased threat of trade secret theft overseas is a result of the lack of strong IP rights protection in many foreign countries. Overseas application will be especially useful to address economic and corporate espionage originating in China. See Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Trade Secrets in Cyberspace, Oct. 2011, at i-ii (stating that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."). Compounding this threat is the reality that "[s]ignificant structural and institutional impediments undermine effective IPR enforcement in China[, including] a lack of coordination among government agencies, insufficient resources for enforcement, local protectionism, and a lack of judicial independence." U.S. Int'l Trade Comm., China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy, Nov. 2010, at xiii. The DTSA's ability to address trade secret misappropriation overseas is valuable whether the theft occurs in China or another country with weak IP protections.

The DTSA at the International Trade Commission

The DTSA may also become the trade secret statute of choice to remedy trade secret misappropriation through a Section 337 investigation before the International Trade Commission (ITC) pursuant to 19 U.S.C. § 1337. The ITC is a quasi-judicial administrative agency with the authority to address unfair trade practices related to imports including the authority to exclude articles from importation into the United States. A complaint in Section 337 investigations related to trade secret misappropriation generally must show:

- Importation of an article into the United States related to an unfair method of competition or unfair act, namely the misappropriation of a trade secret
- Misappropriation of the trade secret at issue –and–
- Injury to a domestic industry that can be tied to the imported article

19 U.S.C. § 1337(a)(1)(A).

Notably, in a Section 337 investigation there is no requirement that the alleged trade secret theft take place in the United States. See Tianrui Group Co. v. ITC, 661 F.3d 1322, 1332 (Fed. Cir. 2011). Additionally, Section 337 investigations move very quickly, and the ITC typically reaches a final adjudication within 16 months of initiating the investigation. Thus, where an employer has been the victim of trade secret misappropriation overseas and the theft relates to articles being imported into the United States, strongly consider bringing a DTSA action before the ITC.

STATE AND COMMON LAW CLAIMS FOR MISAPPROPRIATION OF TRADE SECRETS OR THEFT OF CONFIDENTIAL INFORMATION

State laws by and large prohibit an employee from taking confidential information or trade secrets —shared by the employer with the employee during the course of the employment relationship—which are not generally in the public knowledge and from which the employer derives an economic advantage over its competitors. Such confidential information or trade secrets may include technical or nontechnical data, formulas, patterns, compilations, programs, devices, methods, techniques, drawing, processes, financial data, or lists of actual or prospective customers.

State Liability Standards for Misappropriation Claims

Most states have adopted and codified some version of the Uniform Trade Secrets Act (UTSA), which, among other things, provides a common definition for "trade secret" and "misappropriation" and a uniform remedy

scheme for misappropriation. For the UTSA's definitions of "trade secret" and "misappropriation" see "Statutory Definitions: DTSA vs. UTSA" in Recourse for Trade Secret Misappropriation under the Federal Defend Trade Secrets Act (DTSA), below.

Employers can utilize state laws that adopt a version of the UTSA to bring a claim against a former employee for misappropriation of an employer's trade secrets. To state a claim for misappropriation of trade secrets in state court, a party generally must show that:

- The information constitutes a trade secret
- The plaintiff took reasonable steps to preserve the secrecy of the trade secret –and–
- The defendant misappropriated the secret using improper means

See, e.g., Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1165 (1st Cir. 1994).

While some states may allow for common law claims alleging misappropriation of confidential information should the information stolen not rise to the level of trade secret, a majority of jurisdictions have determined that the UTSA preempts such claims. See, e.g., Embarcadero Techs., Inc. v. Redgate Software, Inc., 2018 U.S. Dist. LEXIS 1902, at *7–11 (W.D. Tex. Jan. 4, 2018) (collecting cases).

When drafting a complaint alleging state or common law violations, you should identify with specificity the exact confidential information or trade secrets that the former employee allegedly misappropriated, as general allegations are typically insufficient. To preserve the secrecy of information in public filings, you should seek to impound or seal the filings or attached documents you wish to keep secret pursuant to the local rules of your court. Such records can generally only be viewed by the clerk, the court, and the parties to the litigation. See, e.g., ALM Unif. Impoundment P. Rule 1. In addition, you will likely need to obtain from the employer hard forensic evidence demonstrating that the former employee is or was unlawfully in possession of the employer's confidential information or trade secrets.

Preliminary Injunctions in State Court

Where an employer's confidential information or trade secrets are at risk, consider making an immediate request for preliminary injunctive relief or a temporary restraining order to prevent the use and disclosure of the employer's trade secrets during the pendency of the litigation. Practically speaking, winning or losing at the injunctive relief stage often changes the way the litigation unfolds. While standards among states differ, to obtain a temporary restraining order or preliminary injunctive relief in state court, a plaintiff must typically demonstrate, at a minimum:

- A likelihood that the plaintiff will succeed on the merits of its claims –and–
- That the plaintiff will suffer irreparable harm if the injunctive relief is not granted

In many states, a plaintiff must also demonstrate that:

- The balance of equities favors the plaintiff –and—
- Injunctive relief advances the public interest

If an employer can prove at this preliminary stage—via critical forensic evidence—that the former employee has unlawfully stolen confidential information or trade secrets, there is a good chance that the court will grant an injunction, thereby preventing the defendant from revealing this critical information to his or her new employer.

For the elements of preliminary injunction claims in each state, see the section entitled "Preliminary Injunctions" in the practice notes contained in the "Restrictive Covenants" column of Non-competes and Trade Secret Protection State Practice Notes Chart.

Additional State Court Considerations

In considering where to file a misappropriation claim, an employer should examine potential venue options, including analyzing which venue or forum may allow the employer's case to be placed on the fastest track (which often puts the employee at a disadvantage). Prepare expedited discovery requests to serve at the earliest possible time, and instruct the employer to immediately begin compiling all evidence relating to both the employee's liability for theft of confidential information and trade secrets and the damages suffered by the employer as a consequence. For information on expedited discovery and other relevant discovery issues in trade secret cases, see Discovery on behalf of Plaintiffs in Trade Secret Misappropriation and Breach of Restrictive Covenant Actions.

The UTSA and many state statutes permit courts to award attorney's fees to prevailing parties where the misappropriation is willful and malicious, which can also be used to assert leverage for any potential settlement prior to trial. See, e.g., Unif. Trade Secrets Act § 4; Ky. Rev. Stat. Ann. § 365.886.

For more information on the various states' trade secrets laws, see Non-competes and Trade Secret Protection State Practice Notes Chart.

THE ECONOMIC ESPIONAGE ACT OF 1996 (EEA)

The Economic Espionage Act of 1996 (EEA), 18 U.S.C. § 1831 et seq., protects trade secrets by providing for criminal sanctions for the misappropriation of trade secrets, including fines, payment of restitution, and prison time (up to 10 years maximum). Specifically, Section 1832 of the EEA makes it a crime, punishable by fine or imprisonment for up to 10 years, to steal a trade secret for "the economic benefit of anyone other than the owner thereof" while "intending or knowing that the offense will injure any owner of that secret." 18 U.S.C. § 1832(a). The statute defines "trade secret" to mean "all forms and types of financial, business, scientific, technical, economic, or engineering information," provided that "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3). In addition to the criminal penalties referenced above, the statute also allows the attorney general to secure injunctive relief. 18 U.S.C. § 1836.

Before the enactment of the DTSA, employers could only bring civil actions for the theft of trade secrets under state law, and the EEA provided no private right of action. As discussed above, however, the DTSA amended the EEA to create a private cause of action for the misappropriation of trade secrets. With this tool at their disposal, employers will generally be satisfied taking civil action under the DTSA and state law against former employees who misappropriated trade secrets. Nevertheless, in certain circumstances, it may still be useful to notify and cooperate with the attorney general, U.S. Department of Justice, and/or FBI to seek criminal prosecution, as enabling such a prosecution can be a powerful deterrent against future thefts of an employer's trade secrets.

Before petitioning the government to bring criminal charges against a former employee, however, ensure that your client has seriously considered whether seeking to use the prosecutorial powers of the government is appropriate in this particular case. For one thing, once the federal government is prosecuting a matter under the EEA, an employer's civil claims are more likely to be stayed indefinitely during the pendency of the government investigation, or fall by the wayside entirely. Moreover, the prosecutor will have sole discretion

over what specific acts to prosecute and what evidence is necessary to be gathered to support the government's claims. Finally, some disclosure of an employer's trade secrets may occur during a criminal prosecution, where courts are more hesitant to limit public access to documents and court proceedings.

THE COMPUTER FRAUD AND ABUSE ACT (CFAA)

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, supplies an employer with the right to bring a civil cause of action against employees who steal trade secrets using their employer-issued electronic devices. Employers often utilize this statute for recourse against departing employees who misappropriate trade secrets or other confidential business information from the employer's computer systems by, for example, utilizing an external hard drive or portable USB device, or emailing the information to the employee's personal account. In some particularly egregious instances, employees may use data destruction or computer wiping software to disguise the theft.

The CFAA provides for a civil cause of action by anyone who has been injured by the wrongful access of a protected computer by someone without authorization or in excess of their authorization. The CFAA does not explicitly define authorization, but courts have held that an employee does not have authorization to access his or her work computer once the employee has violated his or her duty of loyalty to the employer (Intl. Airport Centers, LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006)) or where the employer has specific policies that prohibit accessing information for nonbusiness reasons (United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010)).

The CFAA provides some distinct advantages to employers who opt to utilize it. First, it does not require an employer to demonstrate that the information accessed and stolen by the employee was necessarily a trade secret. Because the CFAA focuses on how the employee wrongfully accessed the confidential information and not what information the employee stole, an employer may bring a claim for the theft of confidential business information that does not rise to the level of being a trade secret. Second, under the CFAA, employers can obtain injunctive relief, which can take the form of prohibiting the employee from starting or working for a competing business, barring the employee from using the unlawfully obtained information, and ordering the return of such information to the employer. Third, since the CFAA is a criminal statute, CFAA claims can be useful for deterring current employees from misappropriating trade secrets, as such claims highlight the severe consequences of an employee's wrongful misappropriation of an employer's valuable information. However, as with the EEA, invoking the government's powers under the CFAA, is perilous. Once the government is involved, the employer may lose control over the outcome of the litigation.

When bringing a claim against a departing employee and/or his or her new employer under the CFAA, include each of the following allegations:

- The employee accessed a protected computer that is used in interstate commerce.
- The employee was not authorized or exceeded his or her authorization when accessing the protected computer and relevant information.
- The employee violated the employer's policies by accessing the information, or the employee's actions violated a duty of loyalty owed to the employer.
- The employee's actions caused damages/loss in excess of $5,000 (to meet the jurisdictional requirements of the statute).
- If applicable, the employer hired a forensic consultant to investigate and attempt to recover data and information that was wrongfully accessed and/or destroyed.

See 18 U.S.C. § 1030(a); 18 U.S.C. § (e)(2)(b); Intl. Airport Centers, LLC, 440 F.3d at 420–21; Rodriguez,

628 F.3d at 1263–64.

For more information on the CFAA, see Cybersecurity Measures to Protect Employers' Confidential Information and Trade Secrets — What Are the Benefits of Bringing Claims under the Computer Fraud and Abuse Act? and the "Computer Fraud and Abuse Act (CFAA)" section of Counterclaims or Separate Lawsuits against Plaintiff Employees — Types of Claims against Employees. In addition, note that several states have some iteration of the CFAA or similar statutes that prohibit computer tampering or unauthorized computer access, which employers can also utilize to protect trade secrets.

COMMON LAW TORT CLAIMS

State Law Preemption of Tort Claims

In many states (particularly those where the state has adopted some version of the Uniform Trade Secrets Act (UTSA)), state statutes prohibiting the theft of trade secrets preempt common law tort claims against a former employee. See, e.g., Enreach Tech., Inc. v. Embedded Solutions, Inc., 403 F. Supp. 2d 968, 978 (N.D. Cal. 2005) (common law Trade Secret misappropriation claim preempted); Stolle Mach. Co., LLC v. Ram Precision Indus., 605 Fed. Appx. 473, 485–86 (6th Cir. Mar. 16, 2015) (claim for tortious interference with business relationships preempted); Putters v. Rmax Operating, LLC, 2014 U.S. Dist. LEXIS 51520 (N.D. Ga. Apr. 14, 2014) (breach of fiduciary duty claim preempted); T.D.I. Int'l, Inc. v. Golf Press., Inc., 2008 U.S. Dist. LEXIS 7427, *16 (E.D. Ky. Jan. 31, 2008) (conversion claim preempted); Cmty. Ties of Am., Inc. v. NDT Care Servs., LLC, 2015 U.S. Dist. LEXIS 14990 (W.D. Ky. Feb. 9, 2015) (unfair competition claim preempted); Health Alliance Network, Inc. v. Cont'l Cas. Co., 354 F. Supp. 2d 411 (S.D.N.Y. 2005) (unjust enrichment claim preempted).

However, some jurisdictions allow common law tort claims to proceed where there are material distinctions between the wrongdoings alleged in the tort claim and the statutory misappropriation of trade secrets claim. For instance, in a Florida case, the court allowed the plaintiff's tortious interference claim to proceed where it was based not merely on trade secret theft, but also on the plaintiff's attempted solicitations of her former employer's customers and employees. Allied Portables, Ltd. Liab. Co. v. Youmans, 2016 U.S. Dist. LEXIS 7109, *11–12 (M.D. Fla. Jan. 6, 2016). In addition, where the information protected is not a trade secret, but nonetheless constitutes confidential business information, some courts may be less likely to dismiss tort claims as being preempted by the relevant state's trade secret statute. See, e.g., Advanced Fluid Sys., Inc. v. Huber, 28 F. Supp. 3d 306, 325 (M.D. Pa. 2014) (tort claims not preempted where it was yet to be determined whether information constituted trade secrets); Orca Cmmc'ns. Unlimited, LLC v. Noder, 236 Ariz. 180, 185 (2014) (Arizona's trade secret statute does not displace tort claim if information falls outside definition of trade secret). Accordingly, research state law to determine what claims you can bring in conjunction with state statutory trade secret misappropriation claims.

Tortious Interference

Employers should consider bringing claims for tortious interference with contractual relationships, business relationships, or prospective economic advantage whenever a former employee uses misappropriated trade secrets or confidential information to the advantage of a competing business. Note that a plaintiff alleging tortious interference must demonstrate that the defendant did not engage in legitimate competitive activity, but instead acted tortiously, using some improper motive or means. Be sure to plead these claims carefully and include specifics to avoid dismissal, including the existence of the contractual or business relationship with an identified third party and a detailed description of the defendant's actions that allegedly constitute interference. To prevent confidential information from being released to the public through court filings, you should seek to seal or impound any documents you wish to remain secret pursuant to the procedure set forth in the court's local rules. Also consider bringing this claim against any competitor employer that engaged in tortious interference by raiding

the employer's staff. See "Combatting Employee Raiding Once It Has Occurred" in Employee Raiding, below.

For detailed information on tortious interference with contract or business relations claims, including elements of the claim, see Tortious Interference with a Third Party, Business Torts § 11.03, and Business Torts § 11.07. For detailed information on tortious interference with prospective economic advantage claims, including elements of the claim, see Tortious Interference with a Third Party, Business Torts § 12.03, and Business Torts § 12.07.

Breach of Duty of Loyalty

Generally, absent a non-compete agreement, employees are free to plan and prepare to compete against their current employer before ending their employment. However, if the employee's actions go beyond mere planning or preparation, and instead move into the realm of actual competition or aiding a competitor—including by misappropriating or misusing an employer's confidential information and/or trade secrets —the employer may have a claim against the employee for breach of the duty of loyalty. See, e.g., Navigant Consulting, Inc. v. Wilkinson, 508 F.3d 277, 284 (5th Cir. 2007). Thus, before bringing a claim for breach of the duty of loyalty, ensure the employee did not merely plan and prepare to compete, but actually engaged in competitive activity or used the employer's confidential information against it while still employed.

Moreover, consider the former employee's position and the scope of his or her duty of loyalty to the employer. While the duty of loyalty generally applies to all employees regardless of position, class, or salary, and even in the absence of a written non-compete or confidentiality agreement, non-officer employees are often held to a lesser fiduciary duty than officers of the employer. See, e.g., Enterprise Recovery Systems, Inc. v. Salmeron, 401 Ill. App. 3d 65, 80–81 (2010).

In addition, research whether a court in your jurisdiction would dismiss a breach of duty of loyalty claim as duplicative of a claim for breach of a restrictive covenant. See, e.g., J.K. Dental Lab Servs., Inc. v. Manno, 967 N.Y.S.2d 867, 867 (Sup. Ct. 2013) (dismissing breach of duty of loyalty claim as duplicative of breach of contract claim in case alleging theft of confidential information).

Finally, consider what relief to request due to the breach. An employer suing for breach of duty of loyalty may generally recover money damages or disgorgement of an employee's compensation, sometimes without even having to prove it sustained economic loss as a result of the breach. See, e.g., Kaye v. Rosefielde, 223 N.J. 218, 220 (2015).

For more information on breach of duty of loyalty claims, see Trade Secrets § 3.04, subsection 8.

Breach of Fiduciary Duty

A fiduciary duty is an obligation to act in the best interest of another party. In the context of employer-employee lawsuits relating to an employee's misappropriation of confidential information or trade secrets, some courts treat a breach of fiduciary duty claim as synonymous with a claim for breach of the duty of loyalty (especially when the employee is a high-level employee). See, e.g., Saye v. Old Hill Partners, Inc., 478 F. Supp.2d 248, 269 (D. Conn. 2007) (in a case involving a defendant executive officer, court stated that Connecticut likely does not recognize a duty of loyalty apart from a fiduciary duty claim). Employers may seek to protect trade Secrets using either claims of breach of fiduciary duty or loyalty, but generally not both. In many states, breach of fiduciary duty claims should be reserved for employees who are true fiduciaries, such as officers or directors of a company who participate in management of the company and have discretionary authority in that capacity. In asserting this claim, allege that the departing employee, who held a fiduciary obligation to act in the best interests of his or her

employer, instead acted in a manner that harmed the company or benefitted a competitor. If the departing employee is not a fiduciary, however, consider instead bringing a breach of duty of loyalty claim, which an employer may bring against former employees who were not fiduciaries of the company.

For more information on breach of fiduciary duty claims, see 1–5 Milgrim on Trade Secrets § 5.02 and Trade Secrets § 3.04, subsection 8.

Other Common Law Tort Claims

Where an employee has misappropriated an employer's confidential information or trade secrets, consider also bringing the following claims:

- Unfair competition. For detailed information on unfair competition claims, see Business Torts § 17.09[5].
- Conversion. For detailed information on conversion claims, see Business Torts § 17.09[4] and Milgrim on Trade Secrets § 13.03[2][c].
- Unjust enrichment. For detailed information on unjust enrichment claims, see Business Torts § 17.09[3] and Milgrim on Trade Secrets § 13.03[2][a].

COMMON LAW CONTRACT CLAIMS

Breach of Restrictive Covenants

Where the departing employee engaging in the unlawful use or theft of an employer's confidential information or trade secrets is subject to a non-compete agreement or other restrictive covenants regarding the use of the employer's confidential information, assert a breach of contract claim in the complaint. For more information on breach of contract claims in trade secret cases, see Milgrim on Trade Secrets § 13.03[1].

You should also consider the following issues when preparing to litigate and litigating a breach of a restrictive covenant claim.

- What steps to take when preparing for a restrictive covenant litigation, including drafting cease and desist letters and issuing litigation hold notices. For information on best pre-litigation practices, see Pre-litigation Steps in Trade Secret Misappropriation and Breach of Restrictive Covenant Cases and Restrictive Covenants: Enforcement Tips.
- Whether to move for a preliminary and permanent injunction to enjoin the former employee (and his or her new employer) from using the employer's confidential information for a competitive advantage. For information on preliminary injunctions, see section above called "Preliminary Injunctions in State Court" in State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information, the section entitled "Obtaining Temporary Injunctive Relief" in Restrictive Covenants: Enforcement Tips — Enforcing Restrictive Covenants in Court, and the section entitled "Preliminary Injunction Standards" in the practice notes contained in the "Restrictive Covenants" column of Non-competes and Trade Secret Protection State Practice Notes Chart.
- How to conduct discovery in breach of restrictive covenant cases, including engaging in expedited discovery, serving written discovery, and taking depositions. For best practices in conducting discovery, see Discovery on behalf of Plaintiffs in Trade Secret Misappropriation and Breach of Restrictive Covenant Actions.
- How to successfully enforce the employer's restrictive covenant and win your case in court. For more information on enforcing restrictive covenants in court, see Restrictive Covenants: Enforcement Tips — Enforcing Restrictive Covenants in Court.
- What issues to consider under state law. For detailed information on the various states' restrictive covenant

laws, see the column entitled "Restrictive Covenants" in Non-competes and Trade Secret Protection State Practice Notes Chart. See also Non-competes and Trade Secret Protection State Practice Notes Chart.

For additional information on restrictive covenants generally, including considerations for drafting and implementing restrictive covenants, see the practice notes in Non-competes and Trade Secret Protection—Restrictive Covenants. For sample restrictive covenant agreements and clauses, see the forms in Non-competes and Trade Secret Protection—Restrictive Covenants.

EMPLOYEE RAIDING

Steps for Preventing Employee Raiding

Employee raiding, in which a competitor hires away an employer's employees—often to acquire the confidential information known by those employees—is a significant threat to employers' trade secret protection. Although it is impossible for an employer to completely prevent employee raiding by a competitor, consider advising the employer to take the following measures to curb such raiding and help the employer retain its employees and its confidential information:

- Utilize non-compete agreements that prohibit employees with access to confidential information from competing against the employer during the term of their contract and for a reasonable time after their contract expires. In addition, implement non-solicitation agreements that prohibit former employees from soliciting the employer's current employees for a reasonable time after departing the employer. For more information on restrictive covenants, see "Breach of Restrictive Covenants" in Common Law Contract Claims, above.
- Where key employees are subject to non-at will employment agreements, consider implementing a longer than standard notice period in the contract, which makes the employee less attractive to a competitor or recruiter. Requiring the employee to give the employer notice of any solicitation or offer of employment by a competitor may also discourage employee raiding.
- Pay bonuses at year-end, rather than monthly, or condition the earning of the bonus on remaining employed at the time of payment, so that employees are incentivized to remain employed until the bonus is paid out. For information on rules on conditions for employees to earn bonuses, see Bonus Agreements: Key Drafting Tips.
- Implement an electronic communications policy stating that the employer has the right to access, inspect, and copy any communications, including voicemails and text messages, on devices connected to or supported by the employer's IT infrastructure. This access can provide valuable evidence when an employer takes legal action in response to an employee raid. For information on drafting electronic communication policies, see Communications System, E-mail, Network, and Internet Policies: Key Drafting Tips, and Computer, Mobile Phone, and Other Electronic Device Policies: Key Drafting Tips. For corresponding annotated policies, see Communications Systems, E-mail, Networks, and Internet Policy, and Computers, Mobile Phones, and Other Electronic Devices Policy.

No-Hire Agreements

Employers should be aware that "no-hire" arrangements—wherein competitors agree not to poach each other's employees—may or may not be enforceable as restraints on trade under the Sherman Act, 15 U.S.C. § 1. Where such agreements not to compete for employees are ancillary to and reasonably limited in scope for a lawful business contract (e.g., when the language is included in confidentiality agreements between competitors considering a merger who need to exchange information regarding key employees during the diligence process), they are typically deemed valid. See, e.g., Global Telesystems v. KPNQwest, N.V., 151 F. Supp. 2d 478 (S.D.N.Y. 2001) (granting preliminary injunction to a company against a competitor that allegedly violated a confidentiality agreement by hiring the plaintiff company's former CFO).

However, where these no-hire agreements are not ancillary to a legitimate contract or reasonably limited in scope, then they are viewed as naked restraints on trade that are per se illegal. See, e.g., United States v. Adobe, Inc., 75 Fed. Reg. 60, 820 (DOJ Sept. 24, 2010) (Department of Justice obtained a settlement agreement from several technology companies—including Google, Apple, Adobe Systems, Intel, Intuit, and Pixar—after challenging their agreements not to solicit, recruit, or otherwise compete for each other's employees).

Combatting Employee Raiding Once It Has Occurred

When an employer learns a competitor is raiding its business for employees, it is prudent to seek expedited forensic investigation of employees' electronic devices. Employers can often use a review of employee electronic devices to obtain valuable data regarding who was involved in coordinating the employee raid and how they implemented their plan.

The employer should immediately send cease and desist letters to the competitor and its departing employees, reminding former employees of their contractual and common law obligations, including the obligation to protect the employer's confidential information and trade secrets. For more information on drafting cease and desist letters, see Pre-litigation Steps in Trade Secret Misappropriation and Breach of Restrictive Covenant Cases — Step 3: Send Continuing Obligations or Cease and Desist Letters to the Former Employee and New Employer and Restrictive Covenants: Enforcement Tips — Drafting Cease and Desist Letters. See also Cease and Desist Letter (Employer to Former Employee) (Post-employment Restrictions) and Cease and Desist Letter (Former Employer to New Employer) (Post-employment Restrictions).

Most states do not recognize a cause of action for employee raiding. Rather, plaintiffs more commonly bring claims for employee raiding against competitors in the form of unfair competition, misappropriation of trade secrets or confidential information, and/or tortious interference causes of action. Where a competitor intentionally raids a rival employer and induces the resignations of key employees to gain access to the employer's trade secrets and other confidential information, consider alleging these claims. For more information on such claims, see Common Law Tort Claims, Recourse for Trade Secret Misappropriation under the Federal Defend Trade Secrets Act (DTSA), and State and Common Law Claims for Misappropriation of Trade Secrets or Theft of Confidential Information, above.

For additional information on employee raiding claims, see Milgrim on Trade Secrets § 7.02[4], Trade Secrets (ALM) § 6.02 (see subsection [2][f]), and Labor and Employment Law § 265.03[4][b].

Bret Cohen
Partner, Nelson Mullins Riley & Scarborough LLP

Bret Cohen is a partner in Nelson Mullins Riley & Scarborough LLP's Boston office where he co-chairs the Labor and Employment Practice. His practice covers a range of industries in the drafting and enforcement of non-compete, confidentiality, and other employment-related agreements throughout the United States. He has also represented individual employees, typically high-level executives, in such matters on behalf of the companies who seek to hire them. Mr. Cohen's practice has also regularly involved advising public company executives on terminations and employment issues and providing advice on a range of matters involving employment agreements, termination of high level executives, worker classification, deal diligence, and hiring oversight and best practices. His practice covers both the negotiation and drafting of relevant agreements and the regular enforcement in litigation of the claims of employers seeking to enforce those agreements.

Mr. Cohen writes and presents on employment law issues and has authored a range of articles relating to the Defend Trade Secrets Act. He frequently lectures on practice before the Massachusetts Commission Against Discrimination and on practice before state and federal courts. Mr. Cohen has served as a contributing author for the Employment Litigation chapter of the Annual Review of Developments in Business and Corporate Litigation, American Bar Association, for a number of years.