



Trends in Trade Secret Litigation and 7 Tips for Employers in the Post-DTSA World

Insights

3.01.22

Over five years ago, the Defend Trade Secrets Act (DTSA) was signed into law, passing with broad bipartisan support and signaling a new frontier for employers seeking to protect their trade secrets. Since its adoption, the DTSA has changed the landscape of trade secret litigation, giving owners of trade secrets a private right of action and the ability to sue in federal court when their trade secrets have been misappropriated. Prior to the law's enactment, employers generally were restricted to filing suit in state courts, where the laws and available remedies differ widely from state to state. Employers with operations in multiple states may have found this lack of consistency to be particularly challenging. But the enactment of the DTSA altered those circumstances, providing a uniform set of standards and available remedies, and driving more and more cases involving trade secret claims to federal courts. This Insight will review the current state of trade secret litigation in light of the federal law and provide employers with seven tips on how to navigate the sometimes turbulent waters.

Federal Trade Secret Litigation is on the Rise

Now that more than five years have passed since the law's enactment, the trend for filing trade secret disputes in federal court remains strong. 7,732 lawsuits involving trade secrets claims have been filed in federal court since the DTSA's effective date of May 11, 2016. In 2021 alone, 1,253 new actions were filed. And in just the last two months – since the beginning of 2022 – at least 139 new trade secrets disputes have made their way into the federal court system.

Surprising as these numbers may seem, perhaps more incredible is the amount of damages that have been awarded in these cases. Although these actions are often resolved before trial, at least 118 damage awards have been entered in federal trade secrets cases in the last five-and-a-half years – amounting to nearly \$1 billion awarded to plaintiffs.

In light of the potential harm to a company whose trade secrets have been misappropriated, and the potential avenue that the DTSA can provide consistent with the ongoing trend to litigate these disputes in federal court, employers should familiarize themselves with the DTSA's provisions and take a close look at how they manage and protect their own trade secrets.

Back to the Basics

Given the ever-growing number of trade secrets lawsuits filed in federal court, revisiting the basics of the DTSA is a helpful first step for an employer to consider in evaluating whether it has appropriately protected its trade secrets.

What Is a Trade Secret Under the DTSA?

The DTSA's definition of a "trade secret" is broad and includes 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:

1. the owner thereof has taken reasonable measures to keep such information secret; and
2. 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.

What Constitutes Misappropriation Under the DTSA?

"Misappropriation" is defined as:

1. 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
2. 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 limited the use of the trade secret; or
 - 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.

What Remedies Are Available Under the DTSA?

What Remedies Are Available Under the DTSA?

The DTSA provides civil seizure in addition to equitable and monetary remedies to owners of trade secrets whose trade secrets have been misappropriated. Monetary damages include:

- actual damages;
- unjust enrichment “caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss;” or
- “in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator’s unauthorized disclosure or use of the trade secret.”

In addition, if the trade secret was willfully and maliciously misappropriated, the owner of the trade secret is also entitled to exemplary damages (two times the actual damages award) and reasonable attorneys’ fees.

What Should Employers Do? 7 Tips.

When it comes to protecting a company’s information, there are seven key steps that an employer should consider taking:

1. ***Perform a Trade Secret Audit.*** A common defense to a trade secret claim is that the employer did not take reasonable measures to keep their information secret, thereby destroying the information’s trade secret status. Whether or not reasonable measures have been taken often depends on the facts and circumstances of the specific case. However, conducting a trade secret audit can go a long way in eliminating any shortcomings in a company’s security measures. Such an audit might include a review of any physical security, electronic data security, and the protocols governing or limiting which employees can access highly confidential and proprietary information.
2. ***Limit Access to Those with a Business Need.*** A helpful argument in proving that reasonable measures have been taken to protect confidential business information is that the company has limited access to the information to those employees who have a legitimate business reason for doing so. This might include protecting databases with passwords or encrypting documents so that they cannot be accessed by employees who do not otherwise need the information to perform their jobs.
3. ***Implement Policies and Procedures for Trade Secrets.*** It is also important to look at the current employment policies to make sure that the company has adequately communicated to employees the company’s expectations with respect to confidential, proprietary, and trade secret information. These expectations should be identified early in the recruitment/onboarding process. Employers should consider incorporating such policies into their codes of conduct, handbooks, record retention procedures, and computer security policies. In addition, departing employees should be reminded of their confidentiality obligations at the time of their departure.

4. **Consider Confidentiality or Non-Disclosure Agreements.** In addition to robust policies and procedures relating to trade secrets, employers should also consider requiring employees with access to confidential and proprietary business information to sign a confidentiality or non-disclosure agreement.
5. **Monitor the Company's Systems.** In addition to reviewing security measures and adopting appropriate policies, the continued monitoring of the company's systems is also important. The implementation of programs that monitor computer usage and server/cloud access can be key in identifying potential trade secret misappropriation.
6. **Be Prepared to Identify Trade Secrets.** The identification of a trade secret is essential to a DTSA claim, and some courts require the designation of specific misappropriated trade secrets early in a lawsuit. For some employers who have only a few trade secrets, this might be an easy task. For others who deal in industries with considerably more proprietary information, this project may be more daunting. A great place to start this process is considering what information your company has that gives it an advantage over competing businesses.
7. **Monitor Changes in the Law.** The DTSA is a relatively new law with an ever-evolving body of case law interpreting it. Given the dynamic nature of trade secret litigation, it is important to be aware of changes in the law and what employers should do to ensure their trade secrets are protected.

Conclusion

Advancements in technology have – for better or worse – made it easier for employees to misappropriate their employer's trade secrets to use for their own purposes. The DTSA has given employers a means of remedying these misappropriations in federal court, and since the statute's inception, federal trade secret litigation continues to trend upward.

If you find yourself facing a trade secret misappropriation issue or have any questions, please contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our [Employee Defection and Trade Secrets Practice group](#). We will monitor developments in this area and provide updates as warranted, so make sure to [subscribe to Fisher Phillips' Insights](#) to get the most up-to-date information direct to your inbox.

Related People





Laura Bailey Brown

Partner

816.460.0208

Email

Service Focus

Employee Defection and Trade Secrets

Litigation and Trials