Insights, News & Events

A 5-STEP ACTION PLAN TO PLEAD YOUR TRADE SECRETS CASE: DANCING ON THE HEAD OF A PIN WITH POSSIBILITY, PLAUSIBILITY, AND PROBABILITY

Insights
Sep 30, 2022

Trade secret cases, by their inherent nature, require speed. For instance, a former employee may have stolen key data and gone to a competitor — and you need to move fast to protect your confidential information. But that does not excuse you from drafting a generalized legal pleading as you assert your claims in court. While you do not have to disclose a secret to protect it, you must put the defendants on sufficient notice regarding the identity of the trade secret, the reasonable measures you used to keep it secret, and how the trade secret was misappropriated (taken, disclosed, or used). Since the passage of the Defend Trade Secrets Act (DTSA) in 2016, federal courts have seen a significant increase in trade secrets cases — and this will not stop anytime soon. Filing a lawsuit may help you to recover stolen information, stop its use, and obtain damages. But what do you need to show the court? At the pleading stage, employers generally must provide a "short, plain statement of the facts." However, two U.S. Supreme Court rulings — the *Twombly* and *Iqbal* cases — seem to require something more. What do you need to know before you file a trade secret claim? This Insight provides you with a helpful five-step action plan.

The Heightened Pleading Standard

The U.S. Supreme Court decided the *Bell Atlantic v. Twombly* case in 2016 announcing a new, heightened pleading standard for antitrust cases. Two years later, in *Ashcraft v. Iqbal,* the Court applied this heightened standard to all civil cases.

Related People

David J. Walton, AIGP, CIPP/US

Partner

610.230.6105

Service Focus

Counseling and Advice

Employee Defection and Trade Secrets

Litigation and Trials

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

The heightened standard is based on "plausibility." As the Court explained, **plausibility** is something more than **possibility**. But, importantly, plausibility means something less than **probability**. So, what's the difference? Here's a quick summary:

- Generalized allegations that merely parrot the legal definitions show a mere **possibility** of a violation. Even when assumed to be true, general or conclusory allegations are not enough.
- **Probability** makes the court evaluate the weight of the evidence at the pleading stage. This is improper, because a plaintiff does not have to prove their case at the pleading level.
- **Plausibility** is somewhere in the middle. As *Iqbal* explained: "A claim has factual plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that the defendant has acted unlawfully."

Even so, many lawyers argue that the underlying facts are not plausible. But this conflates plausibility with probability. At the motion to dismiss stage, the trial court must still assume all well-plead (non-conclusory) facts are true. The court must then evaluate whether all those facts — taken together — state a plausible claim for legal relief. The court's evaluation must be limited to whether a legal claim is plausibly stated, not whether the underlying (non-conclusory) facts are plausible. In fact, *Twombly*, stressed that "a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable."

For **trade secret cases**, "plausibility" means that you must plead facts that showing "trade secret" and "misappropriation." It's not enough that the information is possibly a trade secret, or that there's a chance that something was misappropriated. You must plead facts that, if proven true, would show that the information is an actual trade secret:

1. It is subject to reasonable measures to keep it secret; and

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

2. It has independent economic value from not being generally known.

And you need to allege plausible facts for misappropriation – the information was taken, disclosed, or used.

A Real-World Example

Based on the inherent nature of trade secret cases, evaluating whether something is possible, plausible, or probable can feel like semantic gymnastics. But a recent decision provides a great illustration of the analysis of *Twombly/Iqbal* in a trade-secret case — even though the decision itself has little precedential effect (as it is a report and recommendation by a magistrate judge) — *Core SWX, LLC v. Vitec Group US Holdings, Inc.* 2022 WL 3588081 (E.D.N.Y July 14, 2022).

Like many trade secret cases, the facts underlying this decision are complicated. For us, it's enough the know that defendants asserted a counterclaim based on trade secret misappropriation under the DTSA and New York state law. The plaintiff filed a motion to dismiss the trade secret claims under *Twombly/Iqbal*.

Here, the plaintiff argued that the counterclaim-defendants failed to adequately plead the identity (or existence) of a trade secret and the fact of misappropriation. The magistrate judge agreed and recommended that the complaint be dismissed without prejudice.

Descriptions are not enough

First, the court looked at whether the existence of a trade secret under *Twombly/Iqbal* was plausibly plead. According to the counterclaim, the alleged trade secrets were "proprietary and confidential information, including detailed products plans and marketing strategy documents, and information concerning" two key products. These are category-based descriptions. The issue was whether these descriptions were enough. The court said they were not.

In doing so, the court looked at other cases where similar categorical descriptions were not enough. These included:

- Clinical methods;
- Growth initiatives;

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

- Data configuration protocols and methods;
- Data interpretation;
- Quality assessments and risks assessments;
- Analytics;
- Analytic tools and programming;
- Advertising methods;
- Methods for communicating with prospective customers; and
- Unique and proprietary processes.

These were all examples (from other cases) of category-based descriptions that were too abstract to meet the plausibility standard. In this sense, category-based descriptions are the same as parroting a legal standard – both establish the **possibility** of a legal claim not they do not meet the **plausibility** standard.

Beyond mere categories of trade secrets

The court then then looked at several other district-court-level decisions in the Second Circuit where descriptions that — at first blush — appear categorical-based, actually passed the plausibility standard. These decisions, it noted, all contained something beyond mere categories of trade secrets. These examples included:

- Data and design of a specific phone charger;
- Specifically identified documents that contained trade secrets;
- Technical data, internal pricing, work product, research, and engineering designs;
- Source Code for zero-latency transmission software; and
- Categorical descriptions of information that were tied directly to specific algorithms.

The difference, in the court's view, was categorical descriptions must be linked to something more specific. Here, the court distinguished between categorical descriptions connected to two different products (not

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

plausible) versus categorical descriptions connected to specific documents, a specific algorithm, or specific portion of a product.

The difference between categories aligned with a product versus categories aligned with specific parts of products seems minimal, at best. But this (minor) distinction illustrates the importance of linking general category-based descriptions like “product design information” and “marketing information” to something specific, like specific documents.

Showing that reasonable measures were taken to keep the information safe

The court also found that the counterclaim failed to properly plead that reasonable measures were taken to keep the information safe. Here, the counterclaim alleged that its information was stored and maintained in a secure electronic system, it was accessible only by people who helped developed the products (or were involved in marketing the product), and that person who alleged stole the trade secret “understood” the proprietary and confidential nature of the information. The court said this was not enough. In doing so, it focused on the lack of information that the alleged mis-appropriator signed a confidentiality agreement (as an employee) and was subject to an employee handbook that explained the confidential nature of the information. The court also believed the allegations regarding the “secure electronic system” were too general because they did not state if this “system” was encrypted or password protected and needed more detail about who had access to the system.

Plausibly pleading misappropriation

Additionally, the court found that the counterclaim did not plausibly plead misappropriation. Here, the allegations were that a former employee resigned and took information to a competitor — and his new employer then copied and sold a battery product that was remarkably like one developed by the counterclaim-defendant.

The allegations stated only in general terms that the trade secret must have been taken because only a few people had access to the information and the new employer developed a very similar product. The court found that these

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

"circumstantial datapoints" were not enough for two reasons:

1. The allegations regarding access to the information were too vague because they did not explain who had access to the information, how the information could be accessed, and the number of people who had access to the information.

2. The court stressed the absence of allegations regarding how the former employee specifically took the alleged trade secrets or how he acquired them.

Your 5-Step Action Plan

There's a lot to digest here. But there are five key steps you should consider taking when protecting your trade secrets in court:

1. **Anticipate breaches** – If you work in-house, anticipate that you will have an employee leave and take trade secrets. This has especially been true since the COVID-19 pandemic began and remote work became the norm. Treat it like a table-top exercise. Identify your trade secrets and be prepared to state specifically why they are trade secrets (as opposed to confidential or important non-public business information).

2. **Be careful when using category-based descriptions** — As the federal courts see more and more DTSA cases, there will be more backlash against general, category-based descriptions for trade secrets. When you plead trade secrets claims, think about due process — giving the other side notice of what they need to specifically defend against. Link the category-based descriptions to something specific, like a document, an algorithm, or a specific aspect of a product. As several courts have said, you don't need to publicly disclose a secret to protect it. But using a general category to describe your trade secrets may not meet the plausibility test.

3. **Consider filing under seal** – If you cannot adequately describe your trade secrets without disclosing their secret nature, then file your trade secrets under seal. Also, you can file a document describing each trade secret in particularity under seal, like many California practitioners do.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

4. **Focus on the elements** – A trade secret can be any business information that is subject to reasonable measures of secrecy and derives independent economic value by not being generally known or readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information. There are two major concepts here: **reasonable measures** and **economic value**. When alleging these, be as specific as you can. When alleging reasonable measures, you should consider:

   - Quoting confidentiality agreements, handbooks, policies, and agreements;
   - Discussing security measures in detail; and
   - Identifying the who, what, when, where, and why of access.

   When alleging misappropriation, be specific as you can. If you have a forensic examination, include the details in the complaint. Put the other side on notice of specially what they did to take, disclose, or us the information.

5. **Don't forget these six factors** — In a pre-DTSA world, six key factors were developed to guide courts to analyzing trade secrets:

   1. The extent to which the information is known outside of the business;
   2. The extent to which it is known by employees and others involved in the business;
   3. The extent of measures taken by the business to guard the secrecy of the information;
   4. The value of the information to the business and its competitors;
   5. The amount of effort or money expended by the business in developing the information; and
   6. The ease or difficulty with which the information could be properly acquired or duplicated by others.

The factors do not control the definition of a trade secret, and a party is not required to allege all of these factors to establish a trade secret. But these factors are still important

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

to the courts and still guide their analysis in a post-DTSA world. Thus, when drafting your trade secret complaint, use these factors as a checklist. Don't just parrot their language, but to the extent that you can, include as many specific facts as possible that meet these factors.

Conclusion

Protecting your company's trade secrets is becoming more difficult in today's environment. We will continue to monitor the latest developments, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have questions, please contact the author of this Insight, your Fisher Phillips attorney, or any attorney in our Employee Defection and Trade Secrets Practice Group.

Shelby Garland contributed to this Insight.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.