Navigating Trade Secret Identification During Discovery: Timing & Scope

A trade secret derives its value by being kept secret, yet a trade secret owner is required to identify its trade secret at some point during litigation to apprise the defendant as to what information was allegedly misappropriated. This creates an inherent tension between secrecy and disclosure that is not found in litigating other types of intellectual property rights (particularly patents). Neither the Uniform Trade Secrets Act (“UTSA”)—on which most state trade secret laws are based—nor the federal Defend Trade Secrets Act (“DTSA”) includes specific procedural requirements for the timing or scope of disclosure. Instead, the timing and scope of trade secret identification often varies by jurisdiction, and even by judge in the same jurisdiction. Timing can range from before the opening of formal discovery to throughout fact discovery. And the scope of disclosure deemed sufficient varies as well, with some jurisdictions providing a codified scope standard, whereas others have no working definition of what constitutes sufficient scope. Even with the passage of the DTSA in 2016, there is not a unified approach to the timing and scope of trade secret disclosure in federal courts. Thus, parties should carefully consider trade secret disclosure requirements generally followed in a jurisdiction, both before a case is filed and during litigation.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>STATE AND FEDERAL TRADE SECRET LAW</td>
<td>1</td>
</tr>
<tr>
<td>TIMING OF TRADE SECRET DISCLOSURE VARIES ACROSS JURISDICTIONS</td>
<td>1</td>
</tr>
<tr>
<td>SCOPE OF TRADE SECRET DISCLOSURE VARIES ACROSS JURISDICTIONS</td>
<td>2</td>
</tr>
<tr>
<td>EXAMPLES OF SUFFICIENT DISCLOSURE</td>
<td>2</td>
</tr>
<tr>
<td>EXAMPLES OF INSUFFICIENT DISCLOSURE</td>
<td>4</td>
</tr>
<tr>
<td>AMENDING DISCLOSURES</td>
<td>5</td>
</tr>
<tr>
<td>TAKEAWAYS</td>
<td>5</td>
</tr>
<tr>
<td>LAWYER CONTACTS</td>
<td>5</td>
</tr>
<tr>
<td>ENDNOTES</td>
<td>5</td>
</tr>
</tbody>
</table>
INTRODUCTION

The nature of a trade secret—which by definition derives its value from being kept secret—creates a tension between disclosure and secrecy that is not found in litigating other types of intellectual property rights. More specifically, what must a trade secret plaintiff disclose regarding its trade secret to its adversary and when?

A trade secret is information that provides an economic or competitive advantage over one's competitor and has been maintained in secrecy. But unlike patents, which have a publicly defined scope, trade secrets must be kept from public view to maintain protection. Courts have wrestled with the timing and scope of trade secret disclosure, along with competing policy concerns that impact these issues, for many years. As a result, the timing and the scope of the identification of trade secrets in litigation generally varies by jurisdiction, and even by judge in the same jurisdiction.

This White Paper explores a sample of cases from various jurisdictions to highlight the spectrum of trade secret identification requirements. While most of the cited cases are from federal courts, we note that federal courts may analyze both federal and state law in certain circumstances, as federal cases will often involve both federal and state trade secret misappropriation claims.

STATE AND FEDERAL TRADE SECRET LAW

Trade secret misappropriation cases may be brought under state law (usually a state’s version of the Uniform Trade Secrets Act (“UTSA”)) and under the newer Defend Trade Secrets Act (“DTSA”), which created a federal cause of action for trade secret misappropriation in 2016.

The UTSA was originally published in 1979 by the Uniform Law Commission in an effort to standardize trade secret law across states. To date, 49 states and the District of Columbia have adopted their own version of the UTSA. The desire to have a uniform federal law led Congress to pass the DTSA in 2016.1 Because the DTSA does not preempt state law, the majority of trade secret claims allege misappropriation under both the state’s trade secret law and the DTSA.

Neither the UTSA nor the DTSA includes provisions governing the timing and scope of trade secret disclosure in litigation. Many courts view the DTSA as substantially similar to the UTSA, and therefore tend to enforce the same timing and scope requirements under both the state and federal claim.2 Indeed, a district court in New Jersey recently stated, “courts in this district fold the DTSA analysis into the NJTSA review … [and] consider[] the two claims together.”3 Thus, although the DTSA created a federal cause of action, the application of the federal cause of action generally appears to be consistent with claims brought under state trade secret law.

TIMING OF TRADE SECRET DISCLOSURE VARIES ACROSS JURISDICTIONS

While a plaintiff is required to allege in its complaint at least the general nature of the trade secrets that were misappropriated to survive a motion to dismiss, the plaintiff must later identify the asserted trade secrets with more specificity at some point after a protective order has been issued. Some courts have required a special procedure by which the plaintiff must identify the asserted trade secrets before discovery commences or at the inception of fact discovery, whereas others simply rely on the written discovery requirements in the Federal Rules of Civil Procedure. Federal courts are often influenced by their home state’s approach. There is no unified approach to the timing and scope of trade secret identification in litigation.4

The California and Massachusetts state legislatures have codified a procedure for state court actions that requires a trade secret plaintiff to disclose its trade secret prior to the onset of discovery, once a protective order has been entered.5 Judges in some other state and federal courts have chosen to impose a similar requirement.6

In some courts, however, early identification is not required. In those venues, plaintiffs typically identify the asserted trade secrets during discovery through interrogatory responses and supplements thereto.7

Federal courts that do not follow the California and Massachusetts approach generally analyze the issue under the discovery principles in Rule 26 of the Federal Rules of Civil Procedure. In doing so, courts have noted competing policy
concerns about whether to require a plaintiff to identify its trade secrets prior to discovery.

For example, some federal courts relied on at least three policy considerations when denying a defendant’s request for pre-discovery trade secret identification: (1) a plaintiff has a broad right to discovery under the Federal Rules of Civil Procedure; (2) the plaintiff may have no way of knowing what trade secrets have been misappropriated until it receives discovery showing how the defendant is operating; and (3) if the plaintiff is forced to identify its trade secrets at issue without knowing which have been misappropriated, the plaintiff is placed in a difficult situation of properly identifying the scope of the trade secret to capture the defendant’s activities.

On the other hand, some other federal courts have relied on other policy considerations that support pre-discovery identification: (1) if discovery on the defendant’s trade secrets were automatically permitted, lawsuits might regularly be filed as “fishing expeditions” to discover a competitor’s trade secrets; (2) until the plaintiff has identified the trade secrets at issue with some specificity, there is no way to know whether the information sought is relevant; (3) it is almost impossible for a defendant to mount a defense until it has some indication of the trade secrets allegedly misappropriated; and (4) requiring a plaintiff to state its claimed trade secret prior to discovery ensures that it will not mold its cause of action around the discovery it receives.

Despite these competing concerns, federal courts are increasingly requiring pre-discovery or early discovery identification of alleged trade secrets. Some judges adopt an early identification requirement because otherwise, it can be difficult to assess the relevance of the plaintiff’s discovery requests. The preference for early identification is also seen outside of court. The latest guidelines provided by The Sedona Conference recommend that “the plaintiff [] identify an asserted trade secret with reasonable particularity by the outset of merits discovery.”

SCOPE OF TRADE SECRET DISCLOSURE VARIES ACROSS JURISDICTIONS

There is also the separate question of scope of disclosure. In other words, what is considered sufficient detail to meet the disclosure requirement?

The answer to this question also varies across jurisdictions. Neither the UTSA nor the DTSA includes a specific identification scope requirement, but several states have implemented one. As mentioned previously, many district courts will analyze DTSA claims under the same specificity requirements as required under its home state’s trade secret act.

California state law requires a plaintiff to identify its trade secret with “reasonable particularity.” More specifically, the plaintiff must identify its trade secret “with sufficient particularity to limit the permissible scope of discovery by distinguishing the trade secrets from matters of general knowledge in the trade or of special knowledge of those persons … skilled in the trade.”

Courts in other jurisdictions have also adopted a “reasonable particularity” standard, although the specific terminology used to define “reasonable particularity” may differ across jurisdictions. For example, a judge in the District of Oregon defined it as “a description of the trade secrets at issue that is sufficient to (a) put a defendant on notice of the nature of the plaintiff’s claims and (b) enable the defendant to determine the relevancy of any requested discovery concerning its trade secrets.” A judge in the District of Utah has defined the standard as “requir[ing] a plaintiff to describe the trade secret at issue with adequate specificity to inform the defendants what is alleged to have been misappropriated.” Additionally, in cases brought in Florida, Georgia, North Carolina, and Delaware, the courts implemented a similar “reasonable particularity” standard.

However, not all courts have adopted an identification definition similar to that in California and Massachusetts, or have a defined “reasonable particularity” standard.

It should be noted that disclosure requirements do have limits. Courts do not require a trade secret owner to disclose every detail of its trade secret. In fact, requiring too much specificity can be found to be an abuse of discretion.

EXAMPLES OF SUFFICIENT DISCLOSURE

So how much disclosure is enough?

Again, it is worth noting the distinction between the necessary scope of disclosure for the trade secret in a complaint
(or counterclaim) and the scope of discovery required once a protective order is in place (governing how disclosures of a party's confidential information must be protected and sealed in court filings). What may be sufficient under the requisite pleading standards to state a claim successfully for trade secret misappropriation may not be sufficient to meet the disclosure requirement once a protective order is in place and the parties are to begin (or continue) discovery.

In one example, *Cisco Sys., Inc. v. Chung*, the court found that the plaintiff, Cisco, identified its trade secrets with sufficient particularity in the complaint. Cisco alleged its trade secrets included “market and strategy data, product strategy, financial data, information about Cisco’s Limited Restructurings, Cisco’s investment in emerging technologies, sales opportunities and customer lists, product pipelines, partner margins, and future plans for current products.” The Court noted that Cisco went a step further to include particular subject matter within these categories. For example, Cisco alleged that its trade secret information included a “redacted document containing a range on non-public financial information and a sales strategy named Project Liberator, as well as information about organizational changes at Cisco before they were made public, a discussion guide including Cisco product strategy and other financial data, details of a Cisco program named Project X, and Cisco’s future plans for particular collaboration products.” The court found Cisco’s disclosure to be sufficient because Cisco “narrowed the scope of information at issue in such categories to particular subjects mentioned in certain documents or communications...”

In another example, in *Quintara Biosciences, Inc. v. Ruifeng Biztech Inc.*, the court found that the plaintiff, Quintara, had sufficiently identified its trade secrets (customer profile and vendor databases) and could therefore proceed with discovery. In response to an order prior to the onset of discovery directing plaintiff to disclose its asserted trade secrets, Quintara identified its customer profile database as including “a relational database and many computer spreadsheets which were exported from the database and stored on local file servers. The database contains each customer's purchases and payment history over the years, including the products purchased, the dates of the purchases, the prices paid, and any customer feedbacks for the purchases,” and identified its vendor database to include “the contact and business information for these third-party service providers which are essential for Quintara’s business operations” along with “Quintara's purchasing plans with specific vendors and the financial arrangements between Quintara and such vendors.” The court noted that the descriptions were minimal but adequate to allow the parties to proceed to discovery, given that the identified trade secrets were not highly technical. Further, the court relied on the fact that the data from these databases was party specific, meaning the court could easily identify between plaintiff’s data and defendant’s data.

In *Opal Labs, Inc. v. Sprinklr, Inc.*, an Oregon federal district court found that the plaintiff, Opal Labs, sufficiently identified its trade secrets in its interrogatory response prior to a protective order. In its response, Opal Labs “provided an exhibit that contained additional details about the structure, functions, and capabilities that it claims are trade secrets and cited the transcripts of the depositions” of corporate witnesses describing the trade secrets. Thus, the court denied defendant’s motion to compel Opal Labs to supplement its response to the interrogatory.

In *Maxtech Consumer Products, Ltd. v. Robert Bosch Tool Corp.*, an Illinois district court evaluated the sufficiency of the trade secret disclosure at the close of discovery, denying the defendant’s motion for summary judgment. The court applied the Seventh Circuit’s disclosure standard and found that the plaintiff, Maxtech, identified its “shell packaging” trade secret with sufficient specificity. Over the course of discovery, Maxtech described the shell packaging trade secret in several, highlighted paragraphs of “patent applications relating to the cocoon technology, corresponding paragraphs of its own patent application, and an interrogatory response that, when read in conjunction with those patent applications, clarifies precisely which specifications of the described processes were secret.” In denying Bosch’s motion for summary judgment on the shell packaging trade secret claim, the court noted that the Seventh Circuit’s disclosure standard requires the plaintiff to identify particular documents or other sources of information reflecting its trade secrets and separate them from more generic information contained therein. “By highlighting portions of the patent applications, Maxtech indicated which particular aspects of Bosch’s process overlapped with its own, and its interrogatory response explains which specifications and settings it learned through trial and error would yield the best possible results.” This disclosure, the court found, was sufficiently concrete and comprehensible to withstand a specificity of disclosure challenge.
EXAMPLES OF INSUFFICIENT DISCLOSURE

General terms, vague categories, and catchall phrases may not be enough if additional details are not provided to limit the scope.

In You Map, Inc. v. Snap Inc., a Delaware court at the pleading stage granted the defendant's motion to dismiss the plaintiff's DTSA claim for failure to identify its trade secrets with sufficient particularity. The plaintiff's complaint listed various "technologies" relating to an app that were allegedly misappropriated by the defendants. The trade secrets identified included "the technology to visualize stories on a map" and "the technology to analyze social cues and display those cues as aggregated social patterns," but the complaint did not define "technology." Within the context of the complaint, technologies could refer to source code, algorithms, architecture or framework, visual design, or functional aspects of the app's user interface, yet the complaint did not specify which technology, or if it was all of them, that was allegedly misappropriated. Further, the court noted that the lack of details regarding the identity of the trade secrets rendered the court "unable to determine if the complaint plausibly alleges that defendants misappropriated them." Thus, the court found that the plaintiff's vague trade secrets were insufficient "to put defendants on notice of what they are accused of misappropriating and for this court to determine whether any misappropriation occurred.

In A&P Tech., Inc. v. Lariviere, an Ohio court found that the plaintiff had not identified its trade secrets with reasonable particularity under the protective order prior to discovery. Here, in response to a motion for pre-discovery identification of trade secrets, the plaintiff identified its trade secrets as "proprietary technology, engineering, research and development procedures and materials, braiding machinery, source code, processes, industry tools, and marketing materials, processing technology, design technology, pricing models, industry research, and customer lists, and the applications for A&P's unique process for placing fibers in a reinforcement form that is optimized for carrying the loads that a part will see in service in the aerospace, military, marine, infrastructure, energy, transportation, prosthetic and orthotic, and recreation industries." The court noted the list "is not a list of actual trade secrets but rather a list of categories of business information that for the most part is no way unique to [the plaintiff]." The court further commented on the use of the generic terms, stating, "[t]erms such as engineering, research development procedures and materials, and marketing materials could be applied to almost any corporation in existence, and do not in any way allow defendants to properly craft a defense around the alleged misappropriation of trade secrets." The court held that, only once the plaintiff specifically identifies its trade secrets allegedly misappropriated will the court require defendants to disclose their own trade secrets through discovery.

In another example, Vesta Corp. v. Amdocs Mgmt. Ltd., an Oregon court found the plaintiff insufficiently disclosed its trade secrets in response to an interrogatory and would not proceed with any discovery until the plaintiff identified its trade secrets with particularity. In this case, the plaintiff responded to the defendants' interrogatories requesting trade secret identification with reasonable particularity by providing a list of categories of information that were considered trade secrets: "omni-channel payment processing methods, mobile user fingerprinting, channel-specific credential and authentication management strategies, idempotent communication protocols, bifurcated funds capture, edge-case management strategies, best practices scorecard and recommendations, text-to-pay strategies, and proprietary management tools." The court found this list insufficient, noting that the plaintiff's responses "are too general and generic to satisfy the reasonable particularity standard. Plaintiff's disclosures do not specify any trade secrets, but rather reveal the end results of, or functions performed by, the claimed trade secrets." Further, the court remarked that the "[p]laintiffs must explain how the combination of much of what appears to be generally known information can constitute a trade secret. It is simply not sufficient for plaintiffs to identify a trade secret as a 'method' without some explanation of why that 'method' could be considered a legally protectable trade secret." Additionally, the degree of particularity that is considered reasonable will often differ depending on the alleged trade secrets at issue in the case. Trade secrets in highly specialized fields may require a more exacting level of particularity to distinguish the alleged trade from matters already known to persons skilled in that field.
AMENDING DISCLOSURES

It should also be noted that, once a disclosure is made, it may be possible to amend that disclosure. As a general rule, discovery is an iterative process, and Rule 26(e) of the Federal Rules of Civil Procedure allows a party to supplement a disclosure upon learning that the disclosure or response is incomplete or incorrect. For example, if the plaintiff learns during discovery that additional trade secrets may have been misappropriated, then the plaintiff may seek to amend its disclosure.

Nonetheless, the right to amend is limited. Many courts only allow plaintiffs to amend its disclosure upon a showing of good cause.

TAKEAWAYS

Parties should carefully consider the timing and scope of a jurisdiction's trade secret disclosure requirements, both before a case is filed and during the litigation. A plaintiff with questions regarding the information misappropriated may try to avoid filing suit in early disclosure jurisdictions. Similarly, a defendant should research the specific requirements of the jurisdiction in which they have been sued to develop a defense strategy, including understanding when and how hard to press for disclosure. Overall, a trend appears to be for courts to require a plaintiff to identify its trade secret with some level of detail prior to the commencement of fact discovery (or at least near the outset of fact discovery).

LAWYER CONTACTS

Nathaniel P. Garrett  
San Francisco  
+1.415.875.5731  
ngarrett@jonesday.com

Andrea W. Jeffries  
Los Angeles  
+1.213.243.2176  
ajeffries@jonesday.com

Michael A. Oblon  
Washington  
+1.202.879.3815  
moblon@jonesday.com

Cary D. Sullivan  
Irvine  
+1.949.553.7513  
carysullivan@jonesday.com

Ryan K. Walsh  
Atlanta  
+1.404.581.8487  
rkwalsh@jonesday.com

Laura M. Kanouse and Parth H. Matalia, associates in the Atlanta Office, assisted in the preparation of this White Paper.

ENDNOTES


Kalencom Corp. v. Shulman, No. 17-5453, 2018 WL 1806037, at *5 (E.D. La. Apr. 17, 2018) (requiring plaintiff to identify its trade secrets pre-discovery);

5. See CAL. CIV. PROC. CODE § 2019.210 (West 2021); MASS. GEN. LAWS ch. 93, § 42D(b) (2018).

DynCorp Int'l v. AAR Airlift Grp., Inc., 664 F. App’x 844, 848 (11th Cir. 2016) (noting Florida courts adjudicating FUTSA cases require plaintiffs to identify trade secrets with reasonable particularity prior to discovery).

9 See DeRubeis, 244 F.R.D. at 680–81 (describing four policies supporting pre-discovery trade secret identification); Newmark, 2018 WL 5886531, at *5 (same); BioD, 2014 WL 3864658, at *4–5 (same); StoneEagle Servs., 2013 WL 9554563, at *2 (same); J.J Plank Co. v. Bowman, No. 3:18-CV-00796, 2018 WL 3545319, at *5 (W.D. La. July 23, 2018) (finding this to be "one of the principal policy considerations noted by other courts requiring pre-discovery identification").


13 E.g., Sentry Data Sys., Inc. v. CVS Health, 361 F. Supp. 3d 1279, 1292 (S.D. Fla. 2018) (analyzing the DTSA claim under the same specificity requirement as the FUTSA).


16 Vesta Corp., 147 F. Supp. 3d at 1155 (analyzing the claim under Oregon's state trade secret laws).


19 See e.g., A&P Tech., 2017 WL 6606961, at *10 (analyzing the claim under the Ohio Uniform Trade Secret Act); Stollerusa, Inc. v. AgriScience Techs, LLC, 2019 U.S. Dist. LEXIS 11173, at*8 (S.D. Tex. Jan. 24, 2019) (analyzing the claim under the Texas Uniform Trade Secrets Act); StoneEagle Servs., 2013 WL 9554563, at *4 ("Courts have not specifically defined what constitutes 'reasonable particularity' but have been descriptive about what will not satisfy the requirement.").


23 Id. at 1049.

24 Id.


26 Id. at *4–5.

27 Id. at *4.

28 Id. at *5–6.


30 Id. at *5.

31 Id. at 1.


33 Id.

34 Id.

35 Id.

36 Id. at 860.


38 Id. at *17–18.

39 Id. at *18.

40 Id.

41 Id. at *20.

42 Id. at *21–22.


44 Id.

45 Id.

46 Id. at 9.

47 Vesta Corp., 147 F. Supp. 3d at 1154.

48 Id. at 1155.
49  Id. at 1156.
50  Id.
52  See Advanced Modular Sputtering, 132 Cal. App. 4th at 836.
53  See IntelClear, LLC v. ETC Global Holdings, Inc., 978 F.3d 653, 662 (9th Cir. 2020) (“Discovery provides an iterative process where requests between parties lead to a refined and sufficiently particularized trade secret identification.”).
54  See, e.g., StoneEagle Servs., 2013 WL 9554563, at *5 (noting the court’s order will not prevent a plaintiff from seeking to amend or supplement its alleged trade secret list in the future); Dura Global Techs., Inc. v. Magna Donnelly Corp., No. 2:07-cv-10945-SFC-MKM, 2011 WL 4527576, at *9-10 (E.D. Mich. Sept. 29, 2011) (allowing the plaintiff to bring additional trade secrets into the case in a timely fashion upon learning about additional alleged misappropriation through discovery).
55  See Par Pharm, 2019 WL 959700, at *3 (detailing that many courts permit trade secret plaintiffs to amend or supplement their disclosures based on information gained through discovery upon a showing of good cause); Neothermia Corp. v. Rubicor Med., Inc., 345 F. Supp. 2d 1042, 1044–45 (N.D. Cal. 2004) (cautioning the plaintiff that it must show good cause to amend its trade secret identification in the future).