IP Litigator, *Trade Secrets: 2025 in Review*, (May 1, 2026)

IP Litigator

Trade Secrets: 2025 in Review

Gregory S. Bombard and Kurt A. Kappes

Gregory S. Bombard is a trial lawyer whose practice focuses on trade secret litigation and other IP and commercial disputes. Greg represents software, pharmaceutical, technology, and manufacturing companies in state and federal courts, as well as in arbitration proceedings throughout the United States. He regularly represents both plaintiffs and defendants in trade secret cases and related claims. Greg is a frequent writer and speaker on trade secret law and is the co-author of the book Protecting and Litigating Trade Secrets (2nd Edition), published by the American Bar Association.

Kurt Kappes is one of the key leaders of Greenberg Traurig's trade secret practice group, which has over 100 lawyers in the US and abroad. He regularly counsels and represents mid-size to Fortune 500 clients in litigation over trade secrets, employee mobility, computer fraud, non-competes and unfair competition. He frequently writes and speaks on these subjects, both in the US as well as in the UK, Asia and the Middle East. He can be contacted on +1 (916) 868 0650 or by email: kappesk@gtlaw.com.

The marked rise in the use of artificial intelligence has given rise to new types of claims and defenses. We see increasing claims related to AI engineers and technology. But AI is changing the nature of the cases, too. Reverse engineering of software is easier than ever before, thanks to AI, potentially warping the concept of information that is "readily ascertainable by proper means" in future cases. And at the same time, AI makes the development of new, competing software easier than ever before.

The following is a comprehensive analysis of some of the most significant trade secret decisions that shaped the 2025 legal landscape. One clear theme of 2025 was continued judicial skepticism of broad trade secret claims. Courts systematically rejected broad, sweeping claims about proprietary information, with decisions like *Sysco Machinery v. DCS USA* and *DeWolff Boberg v. Pethick* establishing that companies must identify alleged trade secrets with greater precision or risk automatic dismissal. This scrutiny requires companies to abandon generic references to "databases" or "confidential information" in favor of granular specificity.

With respect to the "reasonable measures" requirement, the case law was more mixed. On one hand, the Fourth Circuit's decision in *Samuel Sherbrooke Corporate v. Mayer* affirmed that simple confidentiality agreements might suffice as "reasonable measures" at the pleading stage, while the Tenth Circuit's *Snyder v. Beam Technologies* demanded multiple protective layers.

One of the year's most significant developments may prove to be the emerging circuit split on damages calculations. In *Computer Sciences Corporation v. Tata Consultancy Services,* the Fifth Circuit accepted unjust enrichment claims for avoided costs, splitting with the Second Circuit's *Syntel* decision from the end of 2024. Concurrently, the Federal Circuit's decision in *ams-OSRAM USA Inc. v. Renesas Electronics America* clarified that head-start periods are measured from when information could hypothetically have been reverse-engineered, not when defendants actually did so.

Looking ahead to 2026, we anticipate continued evolution in several key areas: courts may continue to develop nuanced standards for trade secret identification, often tied to the nature of the secrets themselves, the Supreme Court may be called upon to resolve the growing damages calculation splits, and the continuing rise of AI might force

courts to fashion trade secret law to new technological realities.

In-house counsel should take the opportunity to review and consider updating trade secrets.

Noteworthy 2025 Federal Cases

Reasonable Measures - Samuel Sherbrooke Corporate, Ltd v. Mayer, --- F.4th ---- (4th Cir. 2025)

Facts: Plaintiff is a so-called "captive" insurance company that insures nursing homes and other entities its majority shareholder owns. The company had only three shareholders, who served as directors with "complete, total, and formidable managerial control over [plaintiff] since its formation." In March 2022, plaintiff hired one of the defendants as chief technology officer to design, create, and maintain proprietary software that enabled plaintiff to incorporate medical records to predict risk values and price insurance contracts more effectively. All defendants signed employment contracts containing confidentiality agreements and invention provisions, making work-related creations exclusive property of plaintiff. Plaintiff alleges that around 2022, two defendants began preparing to create a competing insurance entity, with a third defendant later joining the scheme to use plaintiff's proprietary software for the competing business.

District Court Proceedings: Plaintiffs sued in the Eastern District of North Carolina in January 2024, alleging violations of the Defend Trade Secrets Act (DTSA) and various state law claims. Defendants moved for judgment on the pleadings under Federal Rule 12(c). The district court granted the motion, dismissing the DTSA claim for failure to adequately plead reasonable measures to protect secrecy, and declined to exercise supplemental jurisdiction over the remaining state law claims. Plaintiffs appealed.

Court of Appeals Holdings:

- **Trade Secret Secrecy Element**: The Fourth Circuit held that plaintiff adequately pleaded it took "reasonable measures" to maintain secrecy of its software code because of the allegation that it required its employees to sign confidentiality agreements and invention provisions in employment contracts. While defendants argued that the existence of confidentiality agreements alone was insufficient, the Fourth Circuit court emphasized the contextual nature of trade secret protection, ruling "Trade secrets take many forms and what may constitute 'reasonable measures' must be considered in light of the nature of the trade secret and the context in which it exists" (p. 4). The court ruled that at the pleading stage, such contractual protections were sufficient to state a claim that plaintiff employed reasonable measures to maintain secrecy.

- **Misappropriation Element**: The Fourth Circuit ruled that plaintiff plausibly alleged misappropriation. The court held the complaint sufficiently alleged one defendant created the proprietary software while the other two defendants, as shareholders and officers, knew about it, and that all three used it for their competing business. The court noted the practical reality of the alleged theft: "After all, what does one do with a stolen competitive pricing software except 'use' it, as alleged in this case, 'to assist with operating this new competing insurance entity'?" (p. 5).

The Fourth Circuit reversed and remanded, concluding that at the pleading stage, plaintiffs need only plead facts sufficient to plausibly allege trade secret misappropriation, which they had accomplished here.

Takeaways: This decision holds that confidentiality agreements in employment contracts may alone constitute sufficient "reasonable measures" to protect trade secrets under the DTSA, at least at the pleading stage. Furthermore, the case holds that factual allegations connecting defendants' access to proprietary information and

subsequent competitive use may satisfy misappropriation pleading requirements without requiring direct evidence of specific methods of use.

Reasonable Measures - Snyder v. Beam Technologies, Inc., 147 F.4th 1246 (10th Cir. 2025)

Facts: Plaintiff, a former insurance industry employee, worked for a non-party life insurance company from 2006 to 2016, where he acquired a national customer list of over 40,000 insurance broker names. In February 2015, while still employed by the non-party, plaintiff downloaded this broker list to a spreadsheet and emailed it to his personal email account. After the non-party terminated his employment in August 2016, plaintiff remained unemployed until accepting a position with defendant in August 2018 as regional director of broker success. Plaintiff claims defendant promised to pay him "off the books" for providing the non-party's broker lists. When he started working for defendant, plaintiff created three state-specific derivative spreadsheets from the broker lists but accidentally included the complete list as a separate tab. He emailed the broker lists to multiple defendant employees. The emails were not marked confidential, password protected, or otherwise restricted. After discovering his mistake, plaintiff did not attempt to retrieve the materials or notify defendant that he considered the information confidential. Rather, plaintiff told defendant's CEO that he had purposefully shared the complete list. Defendant terminated plaintiff's employment in November 2018.

District Court Proceedings: Plaintiff sued in the District of Colorado in October 2020, alleging trade secret misappropriation under the DTSA and Colorado Uniform Trade Secrets Act (CUTSA), plus several state law claims. Defendant moved for partial summary judgment on the trade secret claims, arguing plaintiff failed to show ownership, reasonable secrecy measures, and that there was no misappropriation since plaintiff voluntarily shared the information. The district court granted summary judgment on the trade secret claims, finding insufficient evidence that plaintiff "owned" the broker list.

Court of Appeals Holdings:

- ***Trade Secret Claims- Reasonable Secrecy Measures***: The Tenth Circuit affirmed summary judgment on the trade secret claims, finding plaintiff failed to take reasonable measures to maintain secrecy. The court emphasized that reasonable measures require more than "normal business precautions," and noted: "In his summary judgment response, he admits that he did not label the state-specific lists as confidential, password protect the lists, require a confidentiality agreement to be signed by any [defendant] employees, or inform the [defendant] recipients that the broker names were confidential" (p. 1256). The court found that openly sharing the information with multiple employees without restrictions, failing to mark documents as confidential, and then ratifying the disclosure by telling defendant's CEO it was intentional, demonstrated unreasonable conduct that defeated trade secret protection.

Takeaways: This decision reinforces that trade secret protection requires affirmative steps to maintain secrecy beyond merely possessing information. Openly sharing alleged trade secrets without restrictions, confidentiality markings, or access limitations may defeat protection even if the disclosure was initially accidental.

TS Identification - Double Eagle Alloys, Inc. v. Hooper, 134 F.4th 1078 (10th Cir. 2025)

Facts: Plaintiff is a specialty metals distributor that buys and resells alloys for companies in the oil and gas industry. Defendant worked as an inside sales manager at the plaintiff for nearly five years before resigning to join a competitor (also a defendant). When leaving, the defendant took handwritten notes and downloaded 2,660 digital files from his

work computer to an external storage device. The files contained plaintiff's sales information, which plaintiff categorized into three types of alleged trade secrets: (1) pump-shaft-quality (PSQ) specifications that aggregate customer preferences and allow distributors to purchase material suitable to multiple customers, (2) pricing information including plaintiff's pricing model based on published surcharges, machining costs, material costs, and customer-specific target margins, and (3) customer drawings that customers routinely share with distributors to obtain price quotes for requested parts.

District Court Proceedings: Plaintiff sued defendants, alleging violations of the DTSA and Oklahoma Uniform Trade Secrets Act (OUTSA), plus state law claims for misappropriation of confidential business information and civil conspiracy. The parties cross-moved for summary judgment. The district court granted summary judgment to defendants on all claims, holding that plaintiff failed to identify its alleged trade secrets with sufficient particularity and failed to present evidence of the information's secrecy.

Court of Appeals Holdings:

- ***PSQ Specifications - Readily Ascertainable Information***: The Tenth Circuit affirmed, finding plaintiff's PSQ specifications were readily ascertainable through proper means and thus could not qualify as trade secrets. The court noted: "The undisputed evidence reveals that [plaintiff] publicly posted certain aspects of the 718 PSQ specification on its website, including a nearly identical chemical composition. [Plaintiff's] customers also have similar 718 and K500 PSQ specifications" (p. 1089-90). The court found widespread use of nearly identical specifications among distributors and customers, with the corporate defendant having developed its own specifications almost a year before the individual defendant even left plaintiff's employment. The court emphasized that plaintiff failed to distinguish which portions of its specifications might qualify as trade secrets from readily available information.

- ***Pricing Information - Insufficient Evidence of Competitive Advantage***: The court held plaintiff's pricing model failed to qualify as a trade secret due to insufficient evidence of uniqueness or competitive advantage. While acknowledging that "confidential data regarding operating and pricing policies can qualify as trade secrets," the court found: "[Plaintiff] describes its pricing as 'a function of the published surcharge, its machining costs, its material costs (which are highly confidential and fixed) plus customer-specific target margins'... But the problem here is that [plaintiff] cites meager evidence to support any claims about its pricing model" (p. 1093-94). The court noted the absence of evidence regarding the time, effort, expense, or competitive advantage of plaintiff's pricing approach.

- ***Customer Drawings - Ownership and Ascertainability Issues***: The court found customer drawings could not qualify as trade secrets under either statute. For the DTSA claim, the court noted the parties did not dispute that drawings came from customers, not plaintiff, defeating the ownership requirement. For the OUTSA claim, the court held: "[Plaintiff] fails to present sufficient evidence that these customer drawings were not readily ascertainable. [Plaintiff] cites no evidence that customers do not share drawings of requested parts with distributors like [plaintiff] and [defendant] or that it would be difficult to obtain the drawings from customers" (p. 1096). The court found that even where plaintiff had confidentiality agreements with some customers, this did not prevent third parties from obtaining drawings directly from those customers.

The Tenth Circuit affirmed summary judgment for defendants on all trade secret claims, finding plaintiff failed to establish the existence of protectable trade secrets.

Takeaways: This decision emphasizes that trade secret plaintiffs must provide specific evidence distinguishing allegedly secret information from readily ascertainable public information. Courts will not hunt through voluminous records to identify potential trade secrets when similar information is widely available in the industry. The case also

reinforces that pricing models require evidence of uniqueness, competitive advantage, or significant development effort to qualify for protection, and that information obtained from third parties (like customer drawings) faces additional hurdles in establishing both ownership and secrecy requirements.

Evidence of Misappropriation and Damages - Harbor Business Compliance Corporation v. Firstbase.io, Inc., 152 F.4th 516 (3d Cir. 2025)

Facts: Plaintiff is a Pennsylvania-based business compliance company that provides corporate formation and registered agent services. Defendant is a New York-based competitor that contacted plaintiff in February 2022 seeking a partnership where plaintiff would provide white-label services to support defendant's new "agent" product. The companies entered into a confidentiality agreement in March 2022 and a partnership agreement in May 2022. Plaintiff shared various business information with defendant, including workflow documents outlining information transfer processes, a jurisdictional database containing state-specific filing requirements and tips, application programming interface documentation, and plaintiff's entity manager dashboard. The partnership launched successfully in June 2022 but began deteriorating by August due to technical issues and disputes over additional charges. In September, a defendant employee boasted about convincing plaintiff to share annual filing deadlines, with defendant's lead responding "The more we can get from them the better, especially if we truly are going to go down the route of being our own [registered agent]." In November 2022, defendant terminated the partnership and took control of the product infrastructure, with internal communications indicating defendant no longer needed plaintiff's information because they had built their own system using the shared data.

District Court Proceedings: Plaintiff sued in the Eastern District of Pennsylvania, alleging trade secret misappropriation under the DTSA and Pennsylvania Uniform Trade Secrets Act, plus state law claims for unfair competition and breach of contract. After a 10-day trial, the jury found the defendant liable and awarded $1,090,271 for breach of contract, $11,068,044 for trade secret misappropriation, and $14,757,399 for unfair competition, plus $1 million in punitive damages. Defendant moved for judgment as a matter of law, a new trial, and remittitur. The district court denied all motions.

Court of Appeals Holdings:

- ***Misappropriation by Use - Sufficient Circumstantial Evidence***: The court affirmed the jury's finding of misappropriation by use, noting sufficient circumstantial evidence beyond mere similarities between the trade secrets and defendant's product. The court identified key "plus factors": "First, there were [defendant's] internal communications... around the time the partnership was fraying, a [defendant] employee bragged that he 'convinced [plaintiff] to share all the annual filings due date per state[,] lol[,] with that info, we can build the reminders logic ourselves without using their data'... Second, there was the accelerated nationwide launch of [defendant's] agent" (p. 531). The court found these communications and rapid expansion provided sufficient evidence that defendant used plaintiff's trade secrets to assist and accelerate product development.

- ***Damages - Impermissible Double Recovery***: The court reversed the district court's denial of remittitur, finding the jury impermissibly awarded the same profits twice under different theories. The court noted: "The jury awarded [plaintiff] $14,757,399 in compensatory damages for the unfair competition claim, the exact amount of [defendant's] profits as calculated by [plaintiff's] damages expert... The jury also awarded $11,068,044 for the trade secrets misappropriation claim, which was seventy-five percent of [Defendant's] profits" (p. 535-36). The court found clear evidence that both awards were based on disgorgement of the same profits, with the damages expert using identical calculations for both claims, making this "double recovery of the same remedy and not a coincidence."

The Third Circuit affirmed the denial of judgment as a matter of law and new trial motions but conditionally remanded with instructions to remit damages by $11,068,044, giving plaintiff the option to accept the reduction or elect a new trial on damages.

Takeaways: The case reinforces that circumstantial evidence of misappropriation may include communications showing intent to use competitor's information and accelerated product launches following access to trade secrets. The decision clarifies that plaintiffs cannot recover the same remedy twice under different legal theories, even when multiple claims are based on the same underlying conduct.

Head Start Damages - ams-OSRAM USA Inc. v. Renesas Electronics America, Inc., 133 F.4th 1337 (Fed. Cir. 2025)

Facts: Plaintiff manufactures ambient-light sensors used in electronic products to adjust screen brightness. In June 2004, plaintiff and defendant entered merger discussions covered by a confidentiality agreement expiring June 3, 2007. During due diligence, plaintiff shared confidential information about its ambient-light-sensor technology with defendant. When merger discussions ended in August 2004, defendant quickly began using the confidential information to develop competing products, including the ISL29003 and other related products. Plaintiff publicly released a product incorporating the previously secret information in early 2005 (Feb. 28, 2005). Defendant became an approved vendor of the ISL29003 for a major consumer electronics product in September 2006 and for a further product between January and March 2008, leading to substantial sales volumes to a major consumer electronics brand.

District Court Proceedings: Plaintiff sued in 2008 for patent infringement and state-law claims, including trade secret misappropriation and breach of contract. After multiple proceedings and appeals, the case was remanded for redetermination of trade secret damages. On remand, a jury found the trade secret became ascertainable by proper means to defendant in January 2006, determined a 26-month head-start period, and awarded $8,546,000 in disgorgement for ISL29003 sales plus $64 million in exemplary damages. The district court limited exemplary damages to $17,092,000 under Texas statute and awarded separate contract damages of approximately $7.25 million for other products.

Court of Appeals Holdings:

- ***Trade Secret Accessibility Date - Legal Standard***: The Federal Circuit reversed the district court's finding that the trade secret became accessible when defendant actually reverse-engineered it in January 2006, holding instead that accessibility occurs when reverse-engineering hypothetically could have been accomplished. The court explained: "Under Texas law, information that is generally known or readily available by independent investigation is not secret for purposes of trade secrecy... 'Information cannot be the subject of a trade secret if it is readily ascertainable without engaging in tortious behavior'" (p. 1347). The court found that because the plaintiff's product containing the trade secret was publicly available by February 2005 and could have been reverse-engineered in roughly a week through common industry practice, the proper accessibility date was Feb. 28, 2005, not when defendant actually performed reverse-engineering.

- ***Head-Start Period Calculation***: The court affirmed the district court's 26-month head-start period determination, emphasizing the factual nature of this inquiry. The court noted: "The inquiry into a proper 'head-start period' is a practical inquiry focused on ensuring that one who prematurely used secret information gains no unfair advantage in the competitive marketplace—no 'head start' on the competition'—from that premature use" (p. 1348). The court found no clear error in the district court's determination that defendant provided insufficient evidence of how long it would have taken to realistically compete without the benefit of plaintiff's technology, while the record supported that defendant lacked relative experience and lagged behind competition

at the time of misappropriation.

- ***Disgorgement Scope - Design Win Analysis***: The court affirmed inclusion of profits from sales resulting from defendant's September 2006 "design win" (vendor approval), rejecting defendant's argument that post-head-start-period sales should be excluded. The court explained: "The district court found that . . . approval of [defendant] as a vendor in September 2006 was a necessary precondition to all the sales . . . at issue. That finding is not clearly erroneous" (p. 1349-50). However, the court affirmed that the exclusion of sales related to a second product because the necessary design win events occurred after the corrected head-start period ended in April 2007.

The Federal Circuit affirmed the monetary awards with one exception, reversing the accessibility date finding but leaving the disgorgement award unchanged, and remanded only on prejudgment interest calculations.

Takeaways: The Federal Circuit ruled that the proper measure of a "head start" period is measured using the date when the trade secret information hypothetically could have been obtained by a defendant through proper means, not when the defendant actually reverse-engineered the information. The case reinforces that head-start period calculations are highly fact-specific inquiries focused on restoring competitive balance.

TS Identification & Public Disclosure - Sysco Machinery Corporation v. DCS USA Corporation, 143 F.4th 222 (4th Cir. 2025)

Facts: Plaintiff is a Taiwanese manufacturer of rotary die cutting machines, and defendant is a North Carolina distributor. From 2017 to 2021, the companies worked together under a manufacturer-distributor relationship where defendant secured customers and identified technical requirements while plaintiff produced customized machines. In April 2021, a group of plaintiff's Taiwanese employees left to launch a competitor, allegedly "copying, stealing, and misappropriating confidential files and machine layouts" when they departed. After establishing the competitor, defendant arranged at least three transactions selling machines made by the competitor to customers who had previously purchased or expressed interest in plaintiff's machines. Plaintiff registered 23 technical drawings related to its rotary die cutting machines with the U.S. Copyright Office in July 2022, making them publicly available by default. This lawsuit represents the plaintiff's third attempt at litigation, having previously filed and dismissed suits in North Carolina federal court and Massachusetts federal court concerning the same underlying conduct.

District Court Proceedings: Plaintiff sued defendant in the Eastern District of North Carolina, alleging misappropriation of trade secrets under the DTSA and North Carolina's Trade Secrets Protection Act (TSPA), plus claims for copyright infringement, unfair and deceptive trade practices, and tortious interference. Defendant moved to dismiss under Rule 12(b)(6). The district court granted the motion, finding plaintiff's trade secret claims were stated in "broad, sweeping terms" lacking sufficient specificity. Plaintiff moved to alter or amend the judgment and for leave to amend its complaint, which the district court denied, citing plaintiff's pattern of bad faith pleading across multiple lawsuits.

Court of Appeals Holdings:

- ***Trade Secret Definition - Insufficient Particularity***: The Fourth Circuit affirmed dismissal, finding plaintiff's trade secret definitions failed to meet pleading requirements for specificity. The court noted plaintiff defined its trade secrets in three different ways: "first as [plaintiff's] compilation of machinery, software, and confidential information,' and then as [plaintiff's] proprietary and confidential information, including the Copyrighted Works, and technical, financial, operations, strategic planning, product, pricing vendor, and customer information'" (p. 228-29). The court found these definitions suggested "nearly [plaintiff's] entire business is a trade secret,"

making it "impossible for [defendant] to know what it has been accused of misappropriating or for the court to assess whether [plaintiff] has met the reasonable secrecy and independent economic value requirements."

- ***Copyright Registration Destroying Trade Secret Status***: The court held that any trade secrets plaintiff might have had in technical drawings were extinguished when the drawings were deposited with the U.S. Copyright Office without redaction. The court explained: "As a consequence of the reasonable secrecy requirement, a trade secret is 'extinguished' when it is disclosed 'to others who are under no obligation to protect the confidentiality of the information'... As a general matter, the U.S. Copyright Office is under no such obligation for documents that are deposited with it" (p. 229). The court found that copyright protection requires disclosure, making the copyrighted works incapable of trade secret protection, and plaintiff's inclusion of "Copyrighted Works" in its trade secret definition further demonstrated the inadequacy of its pleading.

- ***Failure to Allege Misappropriation***: The court found plaintiff failed to plausibly allege how defendant acquired, disclosed, or used any trade secrets. The court noted: "[Plaintiff] did not explain the manner in which fulfilling customer orders involved disclosing or using [plaintiff's] trade secrets. As the district court noted, '[Plaintiff did] not even allege that [defendant] [was] in possession of any of [plaintiff's] 'trade secrets.'' It is difficult to see how [defendant] could have acquired, disclosed, or used something it did not possess" (p. 230). The court emphasized that any information defendant possessed appeared to have been acquired lawfully through the ordinary manufacturer-distributor relationship, and plaintiff never alleged it informed defendant that such information contained trade secrets.

- ***Denial of Leave to Amend - Bad Faith Pattern***: The court affirmed the district court's denial of leave to amend, finding plaintiff engaged in a pattern approaching bad faith through its three civil actions. The court explained: "Here the district court found that [plaintiff] had engaged in bad faith, or something close to it, by filing three civil actions concerning the same underlying conduct and featuring substantially the same defendants and legal claims" (p. 231-32). The court noted that granting leave to amend would prejudice defendant, who had already been required to defend against substantially similar claims in multiple cases.

The Fourth Circuit affirmed dismissal of all claims and denial of post-judgment motions.

Takeaways: This decision reinforces that trade secret plaintiffs must identify their alleged secrets with sufficient particularity to enable defendants to understand what they are accused of misappropriating and courts to assess whether legal requirements are met. The case demonstrates that information disclosed through copyright registration may not simultaneously qualify for trade secret protection due to the fundamental incompatibility between disclosure requirements and secrecy. The decision also serves as precedent for a court to deny leave to amend when plaintiffs engage in repetitive litigation tactics across multiple jurisdictions involving the same conduct.

Trade Secret Identification - DeWolff, Boberg & Associates Incorporated v. Pethick, 133 F.4th 448 (5th Cir. 2025)

Facts: Plaintiff is a global management consulting firm that provides services to electronics, food, manufacturing, and defense contractors through a three-phase process of sales/marketing, analysis, and operations/implementation. The individual defendant worked as a regional vice president of sales from October 2018 until May 2020, when he resigned to join a competitor, the corporate defendant. During his employment, defendant had access to plaintiff's CRM database containing client information and signed non-disclosure, non-compete, and non-solicitation agreements. Plaintiff alleged that defendant diverted three prospective clients from plaintiff to the corporate defendant after his departure. Plaintiff claimed its trade secrets included confidential contact information, demographic and historical information about clients, meeting notes, and a compilation of defense industry prospects (the DOD List)

maintained in its databases.

District Court Proceedings: Plaintiff sued in a Texas state court for breach of contract and breach of fiduciary duty, which was removed to federal court. Defendants moved to dismiss under Rule 12(b)(6), which was granted in part. Defendants subsequently moved to exclude plaintiff's damages expert under *Daubert* and for summary judgment. The district court granted both motions, excluding the expert and dismissing all remaining claims, finding the trade secret claim failed due to lack of admissible damages evidence.

Court of Appeals Holdings:

- ***Trade Secret Identification - Overbroad and Unspecific Claims***: The Fifth Circuit affirmed summary judgment, finding plaintiff failed to identify specific trade secrets with adequate particularity. The court held that plaintiff's "labeling large swathes of database information trade secrets is 'vastly overbroad,' and that [plaintiff] failed to distinguish between the public information in its [CRM] Database and the non-public information" (p. 452). The court emphasized that plaintiff "has not identified what specific information within its database constitutes a trade secret," noting that while plaintiff generally described "confidential contact information" or "notes from prior meetings," it "nowhere is that information identified with specificity" (p. 452-53).

- ***Insufficient Evidence of Use or Disclosure***: The court found no evidence that defendants actually used or disclosed any alleged trade secrets. Despite plaintiff's claims about a suspicious timeline of client departures, the court noted: "the only evidence from [plaintiff] that [defendant] actually used or disclosed trade secrets is an email from [defendant] requesting a copy of the DOD List before leaving for the [corporate defendant] But... when [defendant] had his computer imaged by a forensic specialist to delete any [plaintiff] data, the DOD List was not even one of the documents on the computer" (p. 453). The court concluded that plaintiff "has failed to show [defendant's] or the [corporate defendant's] use of any alleged trade secret."

The Fifth Circuit affirmed summary judgment for defendants on alternative grounds without reaching the district court's *Daubert* ruling excluding plaintiff's damages expert.

Takeaways: This decision rejects sweeping claims about entire databases or information systems being trade secrets. Courts will not search through voluminous records to identify potential trade secrets when plaintiffs fail to distinguish between public and confidential information. The case also demonstrates that suspicious timing alone is insufficient to establish misappropriation without evidence of actual use or disclosure of specific trade secret information.

Trade Secret Identification and Evidence of Misappropriation - Crabar/GBF, Inc. v. Wright, 142 F.4th 576 (8th Cir. 2025)

Facts: Plaintiff is a subsidiary of a wholesale manufacturer that purchased defendant's folder business in September 2013 through an asset purchase agreement (APA) for $15 million. The APA transferred customer lists, databases, intellectual property, and confidential information, while prohibiting defendant from disclosing customer identities or confidential information, including trade secrets. After plaintiff moved operations out of state in late 2015, it lost 86 of 90 employees, and sales dropped significantly. In mid-2016, defendant launched a new folder business. Despite the APA's terms, defendant had retained "hundreds, maybe thousands" of spreadsheets containing folder-related sales data and customer lists on his personal laptop. Using this historical data, WPCO identified plaintiff's most-popular products and created an identical product line. Two of plaintiff's former employees, also defendants, aided defendant by providing 56 die template files of plaintiff's most-popular folders and a "die inquiry" spreadsheet containing

specific product information for over 4,500 of plaintiff's products. From July 2016 through January 2021, defendant sold over $20 million worth of folders, with roughly 84% of sales coming from products identical to plaintiff's top-selling items.

District Court Proceedings: Plaintiff sued all defendants under the DTSA and related claims, including breach of contract and unfair competition. After an 11-day trial, the jury found all defendants liable and awarded just over $5 million in compensatory and exemplary damages. The district court denied defendants' motions to exclude plaintiff's damages expert and for judgment as a matter of law, and after trial denied defendants' post-trial motions seeking judgment as a matter of law or new trial.

Court of Appeals Holdings:

- ***Trade Secret Identification - Folder Information as Protected Secrets***: The Eighth Circuit affirmed, finding sufficient evidence that the "folder information" constituted protectable trade secrets. The court noted that the jury heard testimony that the die inquiry spreadsheet contained "incredibly useful" information "for pretty much every folder product that Folder Express had ever made," and that "nowhere is [the Folder Express die template inquiry spreadsheet] in the public space" (p. 585). The court found that plaintiff's IT policies prohibited employees from downloading die-file information without permission, and that defendant itself had treated the folder information as confidential by requiring a non-disclosure agreement before the APA negotiations. The court concluded: "Based on this evidence, a reasonable jury could find that the folder information had independent economic value due to its secrecy and that [plaintiff] took reasonable steps to protect the secrecy of its folder information" (p. 585-86).

- ***Contractual Protections and Confidentiality Agreements***: The court held that plaintiff's confidentiality agreements with former employees were enforceable contracts under Nebraska law. Despite defendants' arguments that the agreements were merely "policies" and "did not survive termination of employment," the court found the language was "definite and certain" and noted that the agreements expressly stated, "I shall never, either during my employment with the Company or thereafter, directly or indirectly use ... confidential information acquired in the course of my employment activities" (p. 584).

- ***Damages Expert Testimony - Lost Profits Calculations***: The court affirmed admission of plaintiff's damages expert testimony calculating lost profits based on defendant's sales data. While defendants argued that the expert's model made too many assumptions about customer behavior and plaintiff's production capacity, the court noted: "The fact that [the expert's] model relied on assumptions 'cannot be sufficient to mandate exclusion; otherwise, expert testimony on lost profits would rarely be admissible because every model relies on assumptions and no model can account for every conceivably relevant factor'" (p. 588). The court found that evidence of plaintiff's long-term customer relationships and operational recovery by mid-2016 supported the expert's assumptions.

The Eighth Circuit affirmed the jury verdict and damages award, rejecting defendants' arguments regarding waiver, trade secret validity, tortious interference, expert testimony admissibility, double recovery, and causation.

Takeaways: This decision reaffirms that compilations of customer data, product specifications, and manufacturing information may qualify as trade secrets when companies take reasonable measures to protect secrecy and the information derives independent economic value from not being generally known. The decision also shows that expert testimony on lost profits is admissible despite reliance on assumptions, provided the assumptions have some factual support in the record and can be challenged through cross-examination.

Password Trade Secrets - NRA Group, LLC v. Durenleau, 2025 WL 2449054 (3d Cir.

2025)

Facts: Plaintiff is a debt-collection firm with comprehensive data protection and computer use policies. In January 2021, while one employe was out sick with COVID and lacked remote access to company systems, an urgent licensing deadline arose requiring immediate action. One employee called a second employee and shared her login credentials so the second employee could access the first employee's computer from the office. The second employee logged into plaintiff's system as the first employee, accessed a spreadsheet containing the first employee's passwords for dozens of company systems and accounts, and the next day emailed the password spreadsheet to first employee's personal email account and work email. The spreadsheet contained passwords for systems that accessed consumer personally identifiable information and other private business information, but the spreadsheet itself contained no consumer data.

District Court Proceedings: Plaintiff sued defendants for violations of the DTSA and PUTSA, arguing that the passwords in the spreadsheet were trade secrets that defendants misappropriated by creating and emailing the document. The district court granted summary judgment for the defendants on all trade secret claims.

Court of Appeals Holdings:

- ***Trade Secrets - Passwords Lack Independent Economic Value***: The Third Circuit held, in a matter of first impression, that passwords protecting proprietary business information are not themselves trade secrets under federal or Pennsylvania law. The court found that while "[a] compilation of data that has independent economic value can be protected as a trade secret," [the employee's] password spreadsheet did not qualify because the passwords lacked the required independent economic value (p. 11). Relying on *State Analysis, Inc. v. American Financial Services Association*, the court explained that a password is "simply a series of random numbers and letters that is a barrier to" other proprietary material (p. 12). The court emphasized: "Although passwords may 'have economic value' if 'integral to accessing [proprietary information], they have no independent economic value in the way a formula or a customer list might have'" (p. 12).

- ***Distinction Between Passwords and Protected Information***: The court distinguished passwords from the valuable information they protect, noting that plaintiff did not allege "that the passwords were the 'product of any special formula or algorithm'" and that plaintiff "immediately remedied the problem by simply changing the passwords" (p. 12). The court concluded that "it is what the passwords protect, not the passwords, that is valuable," as the passwords were merely "numbers and letters" that "blocked the proprietary information that did have independent economic value: [plaintiff's] business records and customer databases" (p. 12).

The Third Circuit affirmed summary judgment for defendants, holding that passwords are not trade secrets under the DTSA and PUTSA.

Trade Secret Misappropriation and Maritime Law - Global Marine Exploration, Inc. v. Republic of France, 151 F.4th 1296 (11th Cir. 2025)

Facts: Plaintiff is an underwater exploration company that in 2015 received an exploration permit from the Florida Department of State to explore a three-square-mile area offshore of Cape Canaveral. The permit required plaintiff to submit detailed reports, including survey log sheets with site locations and GPS coordinates, and to immediately contact the Division upon discovering historic sites. In 2016, plaintiff discovered remains of la Trinité, a French ship that sank in 1565 during a hurricane while on a military mission to attack Spanish forces in Florida. Plaintiff contacted France about the discovery, offering to enter an agreement to recover artifacts. France refused any commercial arrangement and issued a diplomatic note claiming ownership of the ship as part of the French Royal Fleet. Under

permit requirements, plaintiff submitted reports to Florida, including a "Final Dig & Identify Report" that acknowledged the ship was likely la Trinité and that "France, Spain, England and other countries must be contacted." When Florida requested specific GPS coordinates for the archaeological sites, plaintiff initially resisted providing them due to concerns about public disclosure but ultimately acquiesced after Florida explained it had exemptions under public records law. France and Florida subsequently announced a joint venture to protect and recover la Trinité and other shipwrecks from the French fleet.

District Court Proceedings: After France successfully defended against plaintiff's *in rem* salvage action in a separate case, plaintiff filed this *in personam* action against France seeking salvage awards, unjust enrichment, misappropriation of trade secrets, and tortious interference. Plaintiff alleged that its "coordinate location data" for the shipwrecks constituted trade secrets that France misappropriated. France moved for summary judgment, arguing that the Sunken Military Craft Act barred salvage claims and that plaintiff's other claims failed as a matter of law. The district court granted summary judgment for France on all claims.

Court of Appeals Holdings:

- ***Trade Secret Misappropriation - No Evidence of Improper Acquisition***: The Eleventh Circuit affirmed summary judgment, finding no evidence that France misappropriated plaintiff's alleged trade secrets. The court noted that plaintiff's exploratory permit required the company to provide "Survey Log Sheets" with "site locations" to the Florida Department of State, and while plaintiff alleged that Florida used "coercion and deception" to obtain this location data, "that alleged coercion has nothing to do with France" (p. 1312). The court emphasized that plaintiff "failed to bring forth any evidence proving that France knew that the precise location data 'was improperly obtained' or that France itself 'used improper means to obtain it'" (p. 1312). The court found no connection between Florida's permit requirements and any wrongful conduct by France in acquiring the coordinate information.

- ***Unjust Enrichment and Tortious Interference Claims***: The court also affirmed dismissal of plaintiff's unjust enrichment claim, finding no evidence that France "requested Global Marine's services or that it knowingly and voluntarily accepted the benefits" of plaintiff's efforts, noting that France had publicly opposed commercial salvage activities since 2004 and refused plaintiff's services when contacted (p. 1311). For the tortious interference claim, the court held that France's actions were justified under Florida's "protection privilege," as France did "nothing more than protect its economic and financial interests in a permissive way" by asserting ownership of la Trinité and establishing a relationship with Florida (p. 1313).

The Eleventh Circuit affirmed summary judgment for France on all claims.

Takeaways: The facts of this case are unusual, involving a foreign sovereign and obscure treaties covering the salvage of military vessels. Still, the case interprets U.S. trade secret law to find that regulatory compliance by third parties cannot establish misappropriation by defendants who had no involvement in the disclosure process. Coordinate location data and similar technical information might qualify as potential trade secrets under different facts, but plaintiffs must still prove the elements of misappropriation with specific evidence of wrongful conduct by defendants.

Unjust Enrichment Damages - Computer Sciences Corporation v. Tata Consultancy Services Limited, --- F.4th ---- (5th Cir. 2025)

Facts: Plaintiff provides IT services and business solutions software, including two software platforms. Defendant developed its own competing software platform. In 2013, defendant signed a contract to maintain a customer's

implementation of plaintiff's software platforms. In 2014, plaintiff signed a contract addendum permitting defendant to use plaintiff's software "solely for the benefit" of the customer. In 2016, the customer awarded the defendant a new, $2.6 billion software contract despite defendant's software not being ready for the U.S. market at the time. During the bidding process and subsequent development, defendant used plaintiff's confidential information and trade secrets to develop a competing software and prepare its winning proposal. Discovery revealed that defendant had been sharing excerpts of plaintiff's source code and technical manuals with its development team.

District Court Proceedings: Plaintiff sued defendant under the DTSA, alleging misappropriation of trade secrets. After an eight-day trial with an advisory jury, the district court found defendant liable and awarded $56 million in compensatory damages based on unjust enrichment (avoided development costs), $112 million in exemplary damages, and imposed a permanent injunction barring defendant from using plaintiff's trade secrets or the version of the competing software defendant developed using the misappropriated material.

Court of Appeals Holdings:

- ***Contractual Authorization - Third-Party Access Limitations***: The Fifth Circuit affirmed that defendant's use of plaintiff's confidential information was not authorized under the contractual addendum. The court held that the phrase "solely for the benefit of [the customer]" must be read to mean "exclusively for the benefit of [the customer] and no one else," rejecting defendant's argument that it could benefit from accessing the information beyond ordinary compensation for services. The court explained: "Although [defendant] may, of course, be paid for its services by [the customer], it may not additionally access and use [plaintiff's] confidential information for its own benefit, as that benefit is reserved 'solely' for [the customer] under the Third-Party Addendum" (p. 13). The court found that using plaintiff's trade secrets to prepare a competing bid and develop a competing platform exceeded the scope of authorized access under the agreement.

- ***Unjust Enrichment Damages and Injunctive Relief - Duplication Analysis***: The Fifth Circuit addressed but ultimately rejected the Second Circuit's restrictive approach to unjust enrichment damages under the DTSA in *Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Group, Inc.* The court disagreed with *Syntel's* requirement that plaintiffs prove "compensable harm" beyond lost profits to recover unjust enrichment damages, finding this interpretation "divorced from the text of the DTSA and from traditional understandings of the 'unjust enrichment' remedy" (p. 29). The court explained that *Syntel's* "general rule that a secret holder can never be awarded unjust enrichment damages under the DTSA where it 'suffers no compensable harm beyond its lost profits or profit opportunities'" was problematic because "the DTSA authorizes damages 'for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss.' It does not separately require a compensable, quantifiable injury suffered by the secret holder" (p. 29).

The Fifth Circuit emphasized that unjust enrichment focuses on benefits to the defendant rather than harm to the plaintiff, noting: "if misappropriating trade secrets allows a misappropriator to avoid $1 million in costs for trade secrets they continue to leverage, requiring that misappropriator to pay $1 million in avoided-costs damages simply puts them in the same financial position they would have been in had they not misappropriated trade secrets at the secret holder's expense" (p. 31). However, the court agreed with *Syntel's* core concern about duplication between remedies, finding that "if a misappropriator has been precluded from benefitting from the trade secrets by virtue of an injunction, there is no longer any unjust benefit. Imposing both an injunction and an unjust enrichment damages award in those circumstances would be duplicative and therefore punitive" (p. 31-32). Rather than vacating the damages award, the court chose to modify the injunction to eliminate the prohibition on defendant's use of its competing software while maintaining the bar on access to plaintiff's trade secrets.

Takeaways: This decision is an example of how contractual language may affect whether information is acquired by a defendant by "improper means." The case rejects the Second Circuit *Syntel* test, which requires proof of separate "compensable harm" to the plaintiff to recover unjust enrichment damages under the DTSA. Nevertheless, the court narrowed the relief awarded to avoid potential duplication between monetary awards and injunctive relief.

Noteworthy 2025 State Cases

Preemption and Conspiracy Liability - Coe v. DNOW LP, 718 S.W.3d 338 (Tex. App.—Houston [14th Dist.] 2025)

Facts: Plaintiff is a pump seller. In January 2022, 13 former plaintiff employees began planning to leave for a competitor. The employees copied extensive confidential information and trade secrets from plaintiff, with the copied materials filling 32 boxes. Between April and June 2022, approximately 30 plaintiff employees departed for the competitor in what plaintiff characterized as a "mass exodus." Three employees were particularly active in the scheme: one copied his hard drive to flash drives, a second sent 645 proprietary drawings to his personal email, and a third also copied information and later admitted lying under oath about his conduct. The departing employees used plaintiff's confidential information to assist the competitor in recruiting additional employees and competing directly with plaintiff.

District Court Proceedings: Plaintiff sued the 13 former employees under the Texas Uniform Trade Secrets Act (TUTSA) for conspiracy to misappropriate trade secrets, under the Texas Theft Liability Act for civil theft, and four employees for breach of fiduciary duty. A jury found various defendants liable under all three causes of action and awarded actual and exemplary damages for conspiracy to misappropriate trade secrets, ordered forfeiture of compensation for breach of fiduciary duty, and held all defendants jointly and severally liable for attorney fees. Defendants appealed.

Court of Appeals Holdings:

- ***TUTSA Preemption - Conspiracy Theory Barred***: The court of appeals held, as a matter of first impression, that TUTSA preempts claims that rely on the same facts as trade secret misappropriation claims, including conspiracy theories of liability. The court adopted the "compare-the-facts" test used by the majority of jurisdictions, ruling: "if proof of some other theory of liability would also prove misappropriation of a trade secret, then the claim is preempted" (p. 353). The court found that conspiracy liability conflicts with TUTSA because it allows recovery from persons who may have no responsibility for causing actual losses, explaining that under the conspiracy theory "all who conspire in another's misappropriation of a trade secret are jointly and severally liable with the tortfeasor, even if the conspirators' conduct caused no damage or did not itself violate the Act" (p. 355).

- ***Damages - Limited Evidence of Causation***: The court found legally insufficient evidence to support most damage categories, holding that plaintiff's damages expert failed to link damages to trade secret misappropriation rather than mere employee departures. The court noted: "[Defendant's] damages expert . . . attempted to link [plaintiff's] damages only to the resignations of thirty employees, not to the misappropriation of trade secrets" (p. 357). However, the court found sufficient evidence to support retention bonus damages of $225,000, as there was evidence that the competitor wrongfully used plaintiff's trade secret rate information to obtain a master service agreement with a customer, which enabled the mass hiring of plaintiff's employees.

- ***Breach of Fiduciary Duty - Partial Preemption***: The court ruled that TUTSA preempts breach of fiduciary duty claims only to the extent they rely on trade secret misappropriation, but not claims based on misappropriation of confidential information that lacks the economic value required for trade secret protection. The court found

sufficient evidence of fiduciary breaches by other means but reversed due to erroneous jury instructions that failed to properly define the scope of fiduciary duties owed by employees.

The court of appeals reversed most of the judgment, limiting plaintiff's recovery to 5% of retention bonus damages ($11,250) against one defendant, and remanded for a new trial on fiduciary duty claims with correct jury instructions.

Takeaways: This decision establishes that Texas courts may apply the majority "compare-the-facts" test for TUTSA preemption, barring conspiracy theories of liability that rely on the same conduct as trade secret misappropriation. The case demonstrates that damages must be causally linked to trade secret misappropriation, specifically, not merely to employee departures or competition.

Evidence of Misappropriation and Damages - Military and Veteran Counseling Center, LLC v. Feller Behavioral Health PLLC, 575 P.3d 1098 (Utah 2025)

Facts: Plaintiff is a behavioral healthcare practice, operating as Freedom Counseling, that employed four therapists in 2019. The therapists began exploring job opportunities with a competitor. The competitor requested that the therapists share copies of their employment agreements with plaintiff and information about their clients, including names, insurance information, member ID numbers, co-pay amounts, and deductibles. All of the therapists had signed confidentiality agreements with plaintiff that defined confidential information to include "client information" and prohibited disclosure to outside parties. The competitor explained he needed the employment agreements to ensure he covered his "legal bases" regarding non-compete issues, and he sought client information to help "build a bridge" for client transitions. The competitor used the client information to determine therapist compensation, telling one therapist that "the panels you are credentialed with and [reimbursement rates] affect compensation," and that her requested compensation would "work, taking into consideration what you are bringing." The competitor hired all four therapists, and at least 49 clients followed them from plaintiff to the competitor. Plaintiff subsequently closed its business.

District Court Proceedings: Plaintiff alleged that the defendant misappropriated trade secrets by requesting and using client information to facilitate client onboarding, set therapist compensation, and prepare for insurance billing. Plaintiff sought damages for actual losses and unjust enrichment. Both parties moved for summary judgment, with plaintiff seeking partial summary judgment on liability and defendant seeking full summary judgment. The district court granted plaintiff's motion on liability, finding that trade secrets existed and that defendant had misappropriated them, and denied defendant's motion for summary judgment. Defendant petitioned the Utah Supreme Court for interlocutory review.

Supreme Court Holdings:

- ***Causation Requirement for Damages***: The Utah Supreme Court held that plaintiff failed to establish the required causal connection between defendant's misappropriation of client information and plaintiff's alleged losses. The Court emphasized that under the Uniform Trade Secrets Act, "the plaintiff's damages must be 'caused by' the defendant's 'misappropriation,'" and noted: "If a plaintiff cannot show that the defendant caused damages to the plaintiff through misappropriation, the claim fails" (p. 1103). The Court found that while plaintiff lost clients to defendant, "those clients left for reasons other than [defendant's] receipt of their personal information. The most straightforward reason is that their trusted therapists moved to [defendant]" (p. 1104).

- ***Insufficient Evidence of Actual Use***: The court found no evidence that the defendant actually used the client information to solicit clients, despite plaintiff's argument that the information gave defendant the opportunity to "solicit and poach" clients. The court noted: "the complaint never alleges that [defendant] actually used the

client information to solicit or poach clients. Nor does the evidence support such a claim" (p. 1104). Plaintiff's CEO admitted she was unaware of any communications from defendant to plaintiff's clients and that no client had reported being contacted by defendant.

- ***Rejection of Speculative Causation Theory***: The court rejected plaintiff's argument that defendant would not have hired the therapists without receiving the client information, finding this inference speculative rather than reasonable. The court explained that defendant's hiring decisions were based on "how many clients a therapist might bring and whether the therapist was credentialed with the clients' insurers," and not on personal client details (p. 1105). The Court noted that when one therapist initially provided only client initials and insurer names, defendant responded positively without requesting additional personal information, and that defendant's compensation decisions were based on client numbers by insurer rather than personal client details.

The Utah Supreme Court reversed the district court's denial of defendant's summary judgment motion and reversed the partial summary judgment in favor of plaintiff.

Takeaways: This decision reinforces that trade secret plaintiffs must establish actual causation between the defendant's misappropriation and the plaintiff's damages, not merely temporal correlation or speculative theories of harm.

https://prod.resource.cch.com/resource/scion/document/default/(%40%40PZG01%20WK-JSTORY20260501-2)5b74c8dedc8f421eb5238bcd5896c8cb?cfu=Legal&cpid=WKUS-Legal-Cheetah&uAppCtx=cheetah