GLOBAL TRADE SECRET UPDATE

KEY DEVELOPMENTS IN 2024

Introduction

This publication summarizes noteworthy 2024 legal developments in trade secret law in key centers of commerce throughout the world. Understanding these legislative and judicial developments can help trade secret owners maintain trade secret protection, guard against misuse of their trade secrets by others, and assert rights as necessary.

Table of Contents

KEY DEVELOPMENTS IN THE UNITED STATES

Identifying Trade Secrets

Federal Circuit Overrules Preliminary Injunction Order for Failure to Identify Any Trade Secret with Sufficient Particularity

Insulet Corp. v. EOFlow, Co. Ltd., 104 F.4th 873 (Fed. Cir. 2024)

Insulet Corp. ("Insulet") sued EOFlow, Co. Ltd. and EOFlow, Inc. (collectively "EOFlow") for, among other things, misappropriation of trade secrets under the Defend Trade Secrets Act ("DTSA") after Insulet learned that four of its employees joined EOFlow and that EOFlow was considering being acquired by another company.[1] Insulet sought a temporary restraining order and preliminary injunction enjoining all technical communications between EOFlow and its potential buyer.[2] The district court granted Insulet's request for a preliminary injunction and enjoined EOFlow "from manufacturing, marketing, or selling any product that was designed, developed, or manufactured, in whole or in part, using or relying on the Trade Secrets of Insulet" with some limited carve-outs.[3] EOFlow appealed.[4] Notably, the Federal Circuit issued an order one day after oral argument staying the preliminary injunction pending its then-forthcoming opinion.[5]

The Federal Circuit's ultimate opinion reversed the district court's grant of a preliminary injunction, including because it failed to appropriately consider EOFlow's statute of limitations defense, the irreparable harm and the public interest of the preliminary injunction, and whether the asserted trade secrets were protectable in the first place or misappropriated.[6] On the topic of identification, the Federal Circuit held that the district court abused its discretion when it broadly defined the trade secrets in its preliminary injunction order. That definition was "severely overbroad" because it defined the term "trade secret" for the preliminary injunction to include "any and all Confidential Information of Insulet" and "any information that

contains, derives from, or incorporates such Confidential Information."[7]

In reaching this conclusion, the Federal Circuit rejected the district court's position that "it would be unfair to require at this stage perfection as to the precise number and contours of the trade secrets at issue" and instead reaffirmed that at the preliminary injunction stage, a trade secret plaintiff is required "to establish the likelihood of its success on the merits for least one, specifically defined, trade secret."[8] Insulet had not done so. "Rather, it advanced a hazy grouping of information that the court did not probe with particularity to determine what, if anything, was deserving of trade secret protection."[9]

The Federal Circuit also held that the district court's lack of a tailored analysis as to what specific information actually constituted a trade secret undermined other aspects of the district court's analysis. This included the district court's analysis of whether Insulet took reasonable measures to protect its alleged trade secrets, whether the alleged trade secrets were generally known or readily ascertainable, whether the alleged trade secrets possessed independent economic value, and whether EOFlow misappropriated the purported trade secrets and knowingly benefited from them.[10]

On remand, this case ultimately proceeded to trial in November and December 2024. The jury found that EOFlow misappropriated several of Insulet's asserted trade secrets, and awarded $452 million in damages—$170 million in compensatory and $282 million in exemplary damages.[11] The jury also found that the statute of limitations did not bar Insulet's trade secret claims[12]—a key issue at trial that related to whether Insulet was on notice of the misappropriation in 2018, when EOFlow presented a prototype of its product at a conference, or in 2023, when Insulet acquired, disassembled, and inspected the product.[13]

Federal Court Grants Summary Judgment in Favor of Defendant Based on Plaintiff's Failure to Identify its Trade Secrets with Specificity

Danieli Corp. v. SMS Group, Inc., 21-cv-1716, 2024 WL 3791894 (W.D. Pa. Aug. 13, 2024)

Danieli Corporation and Danieli & C. Officine Meccaniche S.p.A (collectively "Danieli") sued SMS group Inc. and SMS group GmbH (collectively "SMS") alleging that SMS misappropriated aspects of its steel caster technology in a competing bid for a potential customer.[14] Danieli asserted trade secret misappropriation claims under the DTSA and Pennsylvania Uniform Trade Secrets Act and brought a claim for unjust enrichment.[15]

The court granted summary judgment in favor of SMS on all of Danieli's trade secret claims because Danieli "failed to identify its trade secret(s) with the requisite specificity."[16] The court recognized that, in the course of the litigation, Danieli had "taken multiple positions as to how SMS allegedly misappropriated its secret(s)," but that "[u]ltimately, it does not matter because Danieli is unable to sufficiently identify what trade secret(s) it contends SMS misappropriated."[17]

During discovery, SMS sought and the court ordered Danieli to provide a written description of its trade secrets to which Danieli would be bound absent compelling cause.[18] The court found the resulting 30-page "Trade Secret Statement" "identified a number of features of [Danieli's] technology and processes that may be included in its trade secret(s) but avoided being pinned down by never unequivocally stating that any specific technology or process is/are its trade secret(s) pertinent to its claims."[19] The Trade Secret Statement offered a "less than clear articulation of what Danieli claim[ed] to be its trade secret(s)" and was, as the court described it, "as clear as mud and every bit as malleable."[20] The court held the Trade Secret Statement did not identify a trade secret with sufficient particularity to survive summary judgment.[21]

The court also found that Danieli deviated from its Trade Secret Statement, both in its summary judgment briefing and during oral argument, without seeking leave to modify the Trade Secret Statement. These belated shifts in position only "emphasized" the "malleable nature of Danieli's identification of its alleged trade secret(s)" and undermined Danieli's assertions that it provided a specific identification of its alleged trade secrets.[22] Those late deviations, even if permitted, still failed to specifically identify any Danieli trade secret.[23]

Ultimately, the court concluded, "the only thing clear about Danieli's trade secret misappropriation theory is that it is unclear and remains evasive."[24]

Reasonable Measures and Protectability

Sixth Circuit Addresses Importance of Pleading Reasonable Measures and Explicitly Requesting Leave to Amend

In re Island Indus., Inc., 23-cv-5200, 2024 WL 869858 (6th Cir. Feb. 29, 2024)

Plaintiff Sigma Corporation ("Sigma") sued Island Industries, Inc., its president, CEO, and principal owner (collectively, "Island"), alleging that Island obtained Sigma's confidential supplier list, among other information, from a former employee. Sigma alleged trade secret misappropriation claims under the DTSA and the laws of both Tennessee and New Jersey.[25] The Western District of Tennessee dismissed Sigma's claims with prejudice, in part because Sigma failed to adequately allege that it took reasonable steps to protect its trade secrets.

The Sixth Circuit affirmed, despite acknowledging that "the question of whether a trade secret holder took reasonable measures to protect its trade secrets is fact-intensive, often rendering dismissal inappropriate."[26] The court agreed with Sigma's position that company policies providing for dissemination of information on a "need-to-know" basis, and the imposition of confidentiality agreements, can establish reasonable measures to protect trade secrets.[27] However, Sigma's failure to allege these facts in its complaint was fatal to its case.[28]

The court further emphasized that: (i) the mere existence of a common law fiduciary duty to maintain confidentiality does not circumvent the requirement that Sigma impose protective measures to maintain the secrecy of its trade secrets; (ii) the "fact that information is confidential reveals nothing about the measures taken to ensure it is not disclosed"; and (iii) vague allegations of a "partial restriction" of trade secrets is insufficient to state a claim for trade secret misappropriation."[29] The court further held that Sigma had forfeited the opportunity to amend its complaint by failing to request leave to amend in the district court.[30]

Circuit Courts Evaluate Protectability of Trade Secrets Related to Customer Information

James B. Oswald Co. v. Neate, 98 F.4th 666 (6th Cir. 2024)

Plaintiff James B. Oswald Company ("Oswald") sued several former employees who left for a competitor. Oswald sought a preliminary injunction and asserted trade secret misappropriation claims under both the DTSA and Ohio Uniform Trade Secrets Act, as well as a breach of contract claim.[31] The United States District Court for the Northern District of Ohio granted Oswald's motion for a preliminary injunction, in part because Oswald was likely to succeed on its trade secret claims.[32] Defendant Dennis Neate appealed. Neate argued that, as to Oswald's trade secret claims, the district court erred when it found that the client information at issue was protectable as a trade secret.[33]

The Sixth Circuit agreed with the district court's analysis of Oswald's trade secret claims.[34] Neate argued that "key . . . workforce and personnel contact information, customer contact information, needs and preferences, and other customer-related information" were not protectable trade secrets because: (i) Neate had known this information for years before his employment at Oswald; and (ii) the information could be gleaned from the clients themselves.[35] However, these arguments did not persuade the Sixth Circuit that the district court made a clear error.

The court found that the information at issue was not publicly available or readily ascertainable by proper means, and thus was distinguishable from the cases Neate relied on for support.[36] This information was protected, including through password-protected systems and firewalls.[37] Further, the information had "evident economic value" because Oswald spent a significant amount of money buying Neate's book of business and helping him to further develop client contacts and relationships.[38] Therefore, the Sixth Circuit affirmed the district court's findings that Oswald was likely to succeed on the merits of its trade secret claims.[39] Thus, while the case was vacated and remanded for reconsideration of the reasonableness of the noncompetition agreement between Neate and Oswald, and the impermissibly vague injunction issued by the district court, the Sixth Circuit affirmed the district court's conclusions as to Oswald's trade secret claims.[40]

Jacam Chem. Co. 2013, LLC v. Shepard, 101 F.4th 954 (8th Cir. 2024)

Plaintiff Jacam Chemical Company 2013, LLC ("Jacam") sued its former employee, defendant Arthur Shepard Jr. ("Shepard"), and a competitor, GeoChemicals, LLC ("GeoChemicals"), after Shepard convinced some of his former coworkers to send him Jacam's customer proposals and pricing information, which he and GeoChemicals used to underbid Jacam and obtain its customers.[41] Jacam brought trade secret misappropriation, breach of contract, and tortious interference claims under North Dakota law.[42]

The District Court of North Dakota granted summary judgment in favor of Shepard on Jacam's trade secret misappropriation claim because Jacam did not take reasonable efforts to keep its information confidential.[43] Under North Dakota's version of the Uniform Trade Secrets Act, much like the DTSA, reasonable efforts to maintain secrecy "need not be overly extravagant, and absolute secrecy is not required."[44] The district court found that Jacam did not take reasonable measures because customer-pricing information was not branded as "confidential," and Jacam did not produce any confidentiality agreement between its customers.[45]

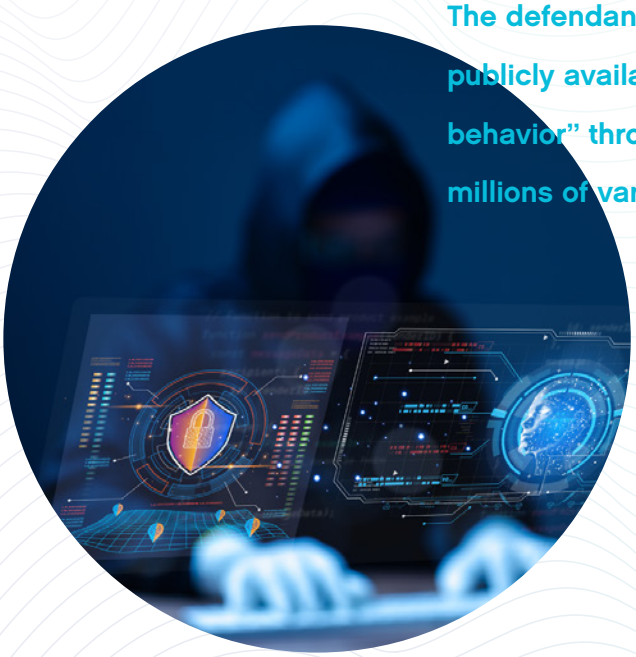
The Eighth Circuit affirmed.[46] The court reasoned that it is not enough to show that Jacam's employees—but not customers—were required to keep information confidential.[47] It also concluded that Jacam failed to show there was an implied obligation within the industry to keep information secret.[48]

Acquisition Through Improper Means

Eleventh Circuit Affirms Bench Trial Ruling on Misappropriation

Compulife Software, Inc. v. Newman, 111 F.4th 1147 (11th Cir. 2024)

Plaintiff Compulife Software, Inc. ("Compulife") sued four individuals with a competing website that generates life insurance quotes.[49] Compulife asserted trade secret misappropriation claims under the DTSA and Florida Uniform Trade Secrets Act ("FUTSA"), and a copyright claim.[50] After a bench trial, the Southern District of Florida ruled in favor of Compulife



The defendants "did not take innocent screenshots of a publicly available site," but rather engaged in "deceptive behavior" through a "scraping attack that acquired millions of variable-dependent insurance quotes."

on its trade secret claims but against Compulife on its copyright claim.[51] The Eleventh Circuit addressed both claims on appeal, as well as the district court's determination of joint and several liability.

The Eleventh Circuit analyzed Compulife's trade secret claim under the FUTSA but acknowledged that doing so also amounted to an analysis under the DTSA, given that the statutes are so similar.[52] The court confirmed that Compulife's database constituted a trade secret based on law-of-the-case doctrine.[53] A prior ruling already concluded that the district court's trade secret finding was not clearly erroneous, and the defendants failed to demonstrate that an exception to the doctrine applied.[54] The Eleventh Circuit also found no error in the district court's determination that defendants used improper means to acquire the trade secret.[55] The defendants "did not take innocent screenshots of a publicly available site," but rather engaged in "deceptive behavior" through a "scraping attack that acquired millions of variable-dependent insurance quotes."[56] Indeed, Compulife's revenue declined after the scraping attack, and the defendants obtained so much of the database that they posed a competitive threat to Compulife.[57]

The Eleventh Circuit also affirmed the district court's joint and several liability ruling, given that "[j]oint and several liability is the standard for trade secret claims, and that sort of liability ignores different degrees of wrongdoing."[58] However, the court ultimately reversed and remanded the district court's non-infringement ruling on Compulife's copyright claim because it failed to consider the copyrightability of the code's arrangement.[59] The petition for writ of certiorari is pending.

Trade Secret Damages

First Circuit Addresses Misappropriator's Profits as Unjust Enrichment

BioPoint, Inc. v. Dickhaut, 110 F.4th 337 (1st Cir. 2024)

BioPoint, Inc. sued Catapult Staffing, LLC and Andrew Dickhaut (collectively, "Catapult") for trade secret misappropriation claims under the DTSA and Massachusetts Uniform Trade Secrets Act.[60] The parties were both staffing agencies. BioPoint alleged that Catapult had improperly acquired its proprietary pay rates and candidate lists to place candidates in various roles, resulting in Catapult entering into a master services contract with Vedanta, a prospective BioPoint client.[61] At trial, the jury found that Catapult misappropriated trade secrets related to Vedanta and another BioPoint client.[62] At a bench trial for unjust enrichment resulting from the misappropriation, the court awarded treble damages jointly against Catapult and Dickhaut, totaling $5,061,444.[63]

On appeal, the First Circuit rejected Catapult's argument that the district court erred in awarding the entirety of the profits that it derived from its contract with Vedanta.[64] Catapult claimed that, because the jury found misappropriation related to only three out of the five candidates that BioPoint submitted to the jury, there was no basis to award all of the Vedanta profits as unjust enrichment.[65] The court explained that the trial court "did not err in finding that but for Catapult's misappropriation of BioPoint's trade secrets, it would not have had a business relationship with Vedanta, such that all of the Vedanta profits arose on account of Catapult's misappropriation and thus were recoverable as unjust enrichment."[66]

California Clarifies Elements of Damages Recoverable in Trade Secret Misappropriation Cases

Applied Medical Distribution Corp. v. Jarrells, 100 Cal. App. 5th 556 (2024)

In a case of first impression in California, the California Court of Appeal decided a novel issue related to the type of damages that are recoverable under the California Uniform Trade Secret Act in *Applied Medical Distribution Corp. v. Jarrells*. The court of appeal concluded that a plaintiff may recover as "damages" the costs incurred by a forensic computer expert to stop or mitigate misappropriation.

At the time of trial in the underlying case, no California case addressed whether "actual loss caused by misappropriation" under California's Uniform Trade Secret Act included costs associated with the work of a forensic computer expert. The trial court refused to allow the plaintiff to include, as part of its damages calculations, the fees paid to a computer forensics expert to determine the existence and extent of any trade secret misappropriation, or the fees incurred to stop and mitigate the misappropriation. The trial court reasoned: "expert fees traditionally and typically are not an item of damage that is recoverable in litigation, but rather, it's a cost of the litigation, which may or may not be recoverable at the end of the case by the prevailing party."

In reaching this conclusion, the trial court found that the "investigatory costs" were not damages but, rather, litigation expenses, because the investigatory costs were not necessary to determine what had happened or by whom. By excluding all expert costs as damages, the trial court failed to adopt the reasoning of other courts, which found that under the Uniform Trade Secrets Act, investigative costs *are* actual loss damages in connection with trade secret causes of action.

The California Court of Appeal disagreed with the trial court, holding that the trial court erred in excluding from the damages calculation the fees incurred by the forensic computer expert to *stop* or *mitigate* the misappropriation. In doing so, the court drew a line between the costs incurred to *stop* or *mitigate* the misappropriation of trade secrets, and the costs of investigating to determine *whether* and *how* any trade secret misappropriation occurred—the latter being not recoverable as damages under CUTSA.

To reach its decision, the court of appeal drew on cases from other states interpreting their respective Uniform Trade Secrets Act on the issue of whether expert fees are awardable as "actual loss" damages. The court specifically agreed with the court in *News America Marketing v. Marquis* (86 Conn. App. 2004) 862 A.2d 837, which held that expenses incurred while attempting to "mitigate and reverse" the harm caused by the misappropriation are recoverable as "damages," while the expenses incurred to investigate *whether* a plaintiff suffered an injury are not. Similarly, the court agreed with the reasoning in *Tank Connection, LLC v. Haight* (D.Kan. 2016) 161 F.Supp.3d 957, which concluded that the costs of a forensic expert's investigation into *whether* a theft of proprietary information occurred is not a recoverable expense. The court in *Tank Connection* also distinguished *21st Century Sys. v. Perot Sys. Govt. Svcs.* (Va. 2012) 726 S.E.2d 236, a case where expert investigatory costs to determine whether misappropriation occurred were recoverable as damages, because such expenses were incurred to staunch an ongoing misappropriation of company data.

In rendering its opinion, the court struck a balance between providing for expert fees that stem from the misappropriation, i.e., an actual loss caused by misappropriation, and preventing the recovery of costs incurred only to *find proof* of a claim for misappropriation.[67]

Seventh Circuit Upholds Multimillion-Dollar Trade Secret Damages Win Based on Worldwide Sales

Motorola Sols., Inc. v. Hytera Commc'ns Corp. Ltd., 108 F.4th 458 (7th Cir. 2024)

Motorola Solutions, Inc. ("Motorola") sued Hytera Communications Corporation Ltd. ("Hytera") for trade secret misappropriation under the DTSA and Illinois Trade Secrets Act. Motorola alleged that Hytera hired engineers who brought Motorola's trade secrets to Hytera.[68] At trial, the jury found that Hytera had violated the DTSA, resulting in an award of $135.8 million in compensatory damages and $271.6 million in punitive damages.[69] The damages were based on Hytera's worldwide sales of products embodying the trade secrets.[70]

The key trade secret issue on appeal was whether damages can be awarded under the DTSA for sales outside of the United States.[71]

The Seventh Circuit explained that all federal statutes are subject to a presumption against extraterritoriality.[72] To determine whether, and to what extent, that presumption is rebutted, courts apply a two-step framework that was articulated by the Supreme Court in *RJR Nabisco, Inc. v. European Community*, 579 U.S. 325 (2016).[73] At the first step, courts ask "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially."[74] The Seventh Circuit explained that the DTSA does contain such a clear, affirmative indication.[75] Specifically, the DTSA provides that it "applies to conduct occurring outside the United States if . . . an act in furtherance of the offense was committed in the United States."[76]

Once it is determined that the presumption is rebutted, the scope of extraterritoriality "turns on the limits Congress has (or has not) imposed on the statute's foreign application."[77] With respect to the DTSA, the Seventh Circuit held that the only limit on the statute's reach is that an act in furtherance must have been committed in the United States.[78] Hytera argued that there was no domestic act in furtherance of its extraterritorial sales; thus, according to Hytera, profits from those sales should not have been awarded as damages under the DTSA.[79]

The Seventh Circuit rejected Hytera's argument. The court explained that trade secret misappropriation includes marketing goods that embody a stolen trade secret.[80] Hytera had advertised, promoted, and marketed products embodying the stolen trade secrets at numerous trade shows in the United States.[81] The Seventh Circuit held that the district court did not err by awarding damages based on worldwide sales of products furthered by Hytera's marketing efforts in the United States.[82]

District Court Vacates Nine-Figure Damages Award Following Remand from Second Circuit

Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Group, Inc., 15-cv-211, 2024 WL 1116090 (S.D.N.Y. Mar. 13, 2024)

The TriZetto Group, Inc. ("TriZetto"), a health insurance software developer, partnered with Syntel Sterling Best Shores Mauritius Limited ("Syntel") to offer TriZetto's software product to health care insurance companies.[83] After TriZetto was acquired by Syntel's competitor, Syntel sued TriZetto for breach of contract, misappropriation, and intentional interference with contractual relations.[84] In response, TriZetto filed counterclaims alleging misappropriation of trade secrets.[85]

At trial, a jury found that Syntel misappropriated TriZetto's trade secrets.[86] TriZetto's expert opined that TriZetto had lost profits of $8.5 million.[87] The jury awarded TriZetto nearly $285 million in unjust enrichment damages under the DTSA based on Syntel's avoided development costs.[88] In other words, the unjust enrichment award was based on the theory that Syntel avoided spending money on research and development by misappropriating technology instead of independently developing it. In this case, TriZetto's actual development costs were used as a proxy for Syntel's avoided costs.[89] The jury also awarded $142 million as a reasonable royalty for trade secret misappropriation under New York common law.[90] The jury awarded nearly $570 million in punitive damages.[91] The court remitted the punitive damages award to $284.9 million and entered a permanent injunction.[92]

On appeal in 2023, the Second Circuit affirmed Syntel's liability for trade secret misappropriation under the DTSA but vacated the $285 million DTSA damages award.[93] The court recognized that the DTSA may permit recovery of avoided costs as unjust enrichment damages.[94] But in this instance, the court determined that avoided costs were not available. The Second Circuit explained that DTSA damages are meant to be compensatory; thus, unjust enrichment damages must be tied to the compensable harm suffered by the trade secret owner.[95] The Second Circuit further explained that a trade secret's development cost may be a valid proxy for compensable harm if the misappropriator retained use of the trade secrets or destroyed their value through publication.[96] Here, the trade secrets were not destroyed and Syntel was enjoined from using them in the future.[97] Thus, TriZetto suffered no compensable harm beyond $8.5 million in lost profits.[98]

On remand in 2024, the district court vacated the New York common law reasonable royalty award.[99] The district court explained that, under New York law, reasonable royalties are

compensatory damages; therefore, a royalty must be related to the actual harm suffered by the trade secret holder.[100] The court held that the royalty award bore no reasonable relation to TriZetto's actual injury of $8.5 million in lost profits.[101] The court did not vacate the punitive damages award because that award was not within the Second Circuit's remand.[102] The district court further awarded attorneys' fees totaling almost $15 million.[103]

Virginia Court of Appeals Reverses $2 Billion Trade Secret Damages Award

Pegasystems Inc. v. Appian Corp., 81 Va. App. 433 (Va. Ct. App. 2024)

Appian Corporation ("Appian") sued Pegasystems Inc. ("Pegasystems") for trade secret misappropriation under the Virginia Uniform Trade Secrets Act ("VUTSA").[104] The parties were in competition to build complex software applications that automate business process functions such as fulfilling orders or opening new customer accounts.[105] Appian alleged that Pegasystems hired a consultant who had access to Appian's platform through his employer, which had licensed the platform from Appian.[106] At trial, the jury returned a record verdict in favor of Appian, awarding damages in excess of $2 billion.[107]

On appeal, Pegasystems argued: (i) the alleged trade secrets were not protectable trade secrets because Appian had not taken reasonable measures to keep the information secret; (ii) Appian failed to identify the trade secrets with sufficient particularity; and (iii) the trial court erred in excluding certain evidence and granting flawed jury instructions.

Pegasystems argued that Appian failed to protect its trade secrets because: (i) Appian had delegated to independent resellers complete discretion to disclose its software; (ii) Appian's agreements with its resellers did not contain strict confidentiality measures; and (iii) Appian shared its secrets with countless independent developers and end users without taking reasonable measures to guard its secrets.[108] The appellate court ruled against Pegasystems, explaining that sufficient evidence of protectability had been presented to the jury.[109] That evidence consisted of extensive expert testimony regarding Appian's measures to protect its trade secrets, including through employing terms of use and license agreements, restricting access to documentation, and using firewalls.[110] The court also noted that the lengthy record was devoid of any evidence that wholesale disclosures took place.[111]

Pegasystems also argued that Appian failed to identify its trade secrets with reasonable particularity.[112] The appellate court disagreed, explaining that Appian's expert witness provided testimony establishing the contours of Appian's five "architecture and design" trade secrets.[113]

Although Appian prevailed on the core trade secret issues, the appellate court ultimately reversed the judgment due to a series of evidentiary errors and instruction missteps by the trial court.[114] First, Pegasystems sought a jury instruction that its "wrongful conduct was the proximate cause of Appian's damages."[115] The trial court rejected that instruction and instead instructed the jury to apply a burden-shifting approach under which, upon proving a misappropriation of a trade secret, Appian's only further burden was to "establish[ ] by . . . greater weight of the evidence Pegasystems' sales."[116] This instruction failed to meet the VUTSA requirement that a plaintiff prove that unjust enrichment damages were caused by misappropriation.[117]

Second, the trial court erred in preventing Pegasystems from authenticating software that could have shown how its functions differed from Appian's. The trial court ruled that Pegasystems could only present the software on the same laptop used during discovery, which was not functional at the time of trial.[118] Pegasystems was barred from authenticating the software on a different physical laptop.[119]

Lastly, the trial court erred in ruling that the number of users with access to Appian's secrets was not relevant.[120] Pegasystems offered substantial evidence showing that thousands of users had access to the alleged trade secrets with varying degrees of restriction.[121] Although not dispositive, the appellate court explained that the number of users with access to Appian's information was relevant to "whether Appian took reasonable efforts in protecting its secrets and whether such secrets were generally known and readily ascertainable."[122]

Injunctive Relief

Ninth Circuit Reinforces Notion that Injunctions Are Not Meant for Stale Trade Secrets

Perrin Bernard Supowitz, LLC v. Morales, 23-cv-55189, 2024 WL 411714, at *1 (9th Cir. Feb. 5, 2024)

Plaintiff Perrin Bernard Supowitz, LLC., doing business as Individual FoodService ("IFS"), a supplier for food service products, sued two former employees for trade secret misappropriation under the DTSA and California Uniform Trade Secrets Act. On summary judgment, the district court found that several of IFS's claimed trade secrets did not actually constitute trade secrets.[123] However, the district court allowed IFS to proceed on trade secrets relating to IFS's customer order history.[124] The district court still denied IFS's request for a preliminary injunction, finding that there was no "real or immediate threat" of misappropriation.[125]

The Ninth Circuit affirmed on appeal.[126] The court acknowledged the district court's finding that the defendants "had not obtained any new information from IFS following their termination," and that any trade secrets they may still have had were "old and stale."[127] The Ninth Circuit reasoned that "a finding of staleness is sufficient to deny injunctive relief," because an injunction against misappropriation of trade secrets should only last as long as necessary to preserve the rights of the parties and eliminate a commercial advantage.[128]

New Challenges to Non-Competes

Federal Developments

New FTC Rule

On April 23, 2024, the Federal Trade Commission voted 3–2 to ban most non-competes, adopting a Final Rule set to take effect on September 4, 2024.[129] The Final Rule prohibits an employer from enforcing or entering into a non-compete clause with a "worker," defined to include employees and independent contractors.[130] The Rule makes a partial exception for so-called "senior executives" who earn an annual compensation greater than $151,164 and can make policy decisions for the business.[131] But even this exception is narrow. The Rule acknowledges the validity of non-competes for senior executives entered into on or before September 4, 2024, but bans them after that date.[132]

The Final Rule has encountered significant opposition, facing multiple lawsuits, and has been vacated nationwide in a ruling that is currently on appeal. Below are three prominent cases showing the divergent rulings reached by courts in these competing cases.

Challenges to the FTC Rule

Ryan, LLC v. FTC, 24-cv-00986, 2024 WL 3297524 (N.D. Tex. July 3, 2024); _Ryan, LLC v. FTC_, 24-cv-00986, 2024 WL 3879954 (N.D. Tex. Aug. 20, 2024)

The most substantial challenge to the FTC Rule came with a lawsuit filed by Ryan, LLC, a global tax services firm that uses non-competes with its shareholder principals and certain other employees with access to particularly sensitive business information.[133] In its complaint, Ryan, LLC alleged that the Rule contravenes the FTC Act, violates the Constitution, and is arbitrary, capricious, and otherwise unlawful.[134]

California's new non-compete laws went into effect on January 1, 2024, bolstering the state's existing protections against non-competes

On July 3, 2024, the court granted a preliminary injunction enjoining the Rule as to the plaintiffs, finding, in relevant part, that the plaintiffs were likely to succeed on the merits of their arguments that: (i) the FTC lacks substantive rulemaking authority under the FTC Act; and (ii) the Rule is arbitrary and capricious.[135]

Then, in an August 20, 2024, ruling blocking the Rule from taking effect, the court followed up on its earlier ruling and broadened it, holding that the FTC exceeded its rulemaking authority with respect to unfair methods of competition.[136] The court held that the non-compete Rule was "arbitrary and capricious" because it was overbroad and based on "inconsistent and flawed empirical evidence."[137] The ruling bars the FTC from enforcing the Final Rule nationwide.[138]

Like in the *Villages* case, on October 18, 2024, the FTC formally filed a notice of appeal in the Fifth Circuit.[139] The FTC Rule remains enjoined by the ruling of the district court while the appeal is still pending.

Props. of the Villages, Inc. v. FTC, 24-cv-00316, 2024 WL 3870380 (M.D. Fla. Aug. 15, 2024)

The U.S. District Court for the Middle District of Florida reached a different result. In *Properties of the Villages, Inc. v. FTC*, it temporarily blocked the Rule as to the plaintiff on August 15, 2024.[140] The plaintiff requested only relief for itself, not a nationwide injunction.[141]

At a hearing, the court explained its reasoning and addressed three key points. First, it addressed whether the plaintiff was likely to succeed on the merits of its argument that the FTC lacks the rulemaking authority it claimed.[142] The court found that the plaintiff was unlikely to do so, as "Congress gave the FTC authority to 'prevent' unfair methods of competition. . . ."[143]

Second, the court addressed whether the plaintiff was likely to succeed on the merits of its constitutional argument that the Rule violates the Commerce Clause. The court concluded that the plaintiff was not.[144]

Third, and critically, the court found that the plaintiff was likely to prevail on its argument that the Rule "presents a major question as defined by the Supreme Court," and that Congress did not render "a sufficiently clear expression . . . to authorize the final rule."[145] In light of this ruling, on September 24, 2024, the FTC filed a notice of appeal to the Eleventh Circuit.[146]

ATS Tree Servs., LLC v. FTC, 24-cv-1743, 2024 WL 3511630 (E.D. Pa. July 23, 2024)

In a case seemingly upholding the new FTC Rule, ATS Tree Services, LLC, a 12-employee tree-care company, sued the FTC, seeking to enjoin the FTC's Rule.[147] The court denied the plaintiff's motion for preliminary injunction, holding that the plaintiff failed to establish the irreparable harm required for an injunction and that it failed to establish a reasonable likelihood of success on the merits.[148] The plaintiff voluntarily dismissed its claims without prejudice on October 4, 2024.[149]

State Developments

California's new non-compete laws went into effect on January 1, 2024, bolstering the state's existing protections against non-competes.[150] SB-699 in particular provides that any contract void under California law (including non-competes) is unenforceable—regardless of where and when the employee signed the contract.[151] Employers can thus anticipate disputes with former employees who relocate to California at the behest of their new employer to avoid enforcement of their covenants by former employers.

The reach of the California law was tested when DraftKings, a Massachusetts company, enforced a non-compete against a former executive who joined Fanatics, a California company.[152] Notwithstanding the contract's choice of Massachusetts law, the employee argued that the non-compete provision should be evaluated under California law.[153] The First Circuit disagreed, holding that the employee failed to show, as required by Massachusetts law to avoid a contract's choice-of-law provision, that California had a "materially greater interest" in deciding the case than Massachusetts.[154] It is important, therefore, to stay aware of a given state's choice-of-law doctrine, as it can matter as much as the unique substantive law on non-compete provisions—the right contract enforced in the right forum may still fail if the wrong state's law is applied.

Like New York in 2023, the Maine legislature passed a non-compete ban that was vetoed by its governor. Governor Janet Mills vetoed the legislation (L.D. 1496) on March 29, 2024, informing legislators that the proposed law placed unnecessarily strict restrictions on non-competes.[155] Governor Mills defended the use of non-competes in certain circumstances, especially "when they are designed to protect a former employer's confidential information from disclosure to commercial competitors."[156]

On the federal front, it remains to be seen whether the FTC will continue to pursue its appeals and, if so, whether the FTC's Rule will be reinstated following appeal. And we expect to see additional state-level challenges to and restrictions on non-competes in 2025. Employers are encouraged to protect confidential information through alternative means, such as requiring and enforcing non-disclosure agreements and seeking redress under trade secret laws.

KEY DEVELOPMENTS IN CHINA

With the growing use of trade secrets in today's highly digitized landscape—where cross-border operations are the norm—we see rising disputes between U.S. and Chinese entities on trade secret misappropriations.

Chinese courts, however, will not recognize or enforce a judgment of a U.S. court. Thus, to obtain a trade secret judgment in China, a Chinese action for trade secret misappropriation must be instituted.

Luckily, recent reforms to Chinese trade secret laws have provided more legal certainty for litigation in China. For example, in June 2024, China's Supreme People's Court awarded a record-high damages of RMB 640 million (equivalent to US$88 million) in a trade secret misappropriation case.[157] Such high damages are likely to become even more common.

Serving the Complaint

Recent amendments to Chinese Civil Procedure Law allow for additional alternative means for service on foreign parties, which can help avoid time-consuming procedures under the Hague Convention—e.g., by serving a defendant's wholly owned subsidiary instead of the defendant itself.[158]

Making the Case as a Trade Secret Owner

Chinese trade secret law was amended in 2019, shifting the burden of proof and making it easier for the plaintiff to prove its case.[159]

Under current law, once evidence on trade secret misappropriation is produced, the defendant has the burden to disprove

that.[160] In addition, the plaintiff does not need to prove actual access to the trade secrets. Instead, the plaintiff only needs to show that the accused party had channels or opportunities to access the alleged trade secrets.[161]

Remedies

Injunctions and damages are both available remedies in China.

The maximum statutory damages recently increased from RMB 1 million to RMB 5 million.[162] A 2019 amendment also introduced punitive damages of up to five times in cases of willful and malicious misappropriation or repeated infringements.[163]

The damages rules are similar to patent cases. Damages are based on the actual loss suffered due to the infringement or the profits gained by the accused party. But because China lacks U.S.-style discovery, it is challenging to gather evidence of damages. As a result, courts award statutory damages in the majority of cases.

The Supreme People's Court has created a new system to address this problem. Under the new procedure, if the plaintiff has provided preliminary evidence of lost profits, the plaintiff may submit an application to order the defendant to provide its accounting books and records. If the defendant refuses to comply, the court may determine the lost profits based on the claims and evidence the plaintiff provided.[164]

This system significantly reduces the burden on the plaintiff, avoiding overreliance on statutory damages.

Indeed, in 2023, the Supreme People's Court awarded a record-high damages award in *Geely v. WM Motor*, about RMB 640 million (US$88 million), in a case related to electric vehicle technology.[165]

And in *Sennics Chemical v. Yuncheng Jinteng*, the Supreme People's Court relied on the plaintiff's actual loss report in a corresponding criminal case to order the defendant to pay more than RMB 200 million (about US$28 million).

Criminal Proceedings

Trade secret misappropriation can also be a criminal offense in China if the losses suffered by the trade secret owner exceed RMB 300,000 (approximately US$40,000).[166]

Criminal enforcement sends a strong message. It has become a preferred enforcement mechanism for victims of trade secret misappropriation because local enforcement authorities have more power to gather evidence and prove the misappropriation. As a result, public prosecutions doubled in 2023 compared to 2022.[167]

Commercial espionage, meaning espionage of trade secrets to the benefit of foreign parties, is a new crime in China.[168] The law bears some similarities to the Economic Espionage Act in the United States, but there are significant differences.

Whereas economic espionage laws in the United States are generally targeted toward the provision of trade secrets to foreign governments, Chinese commercial espionage laws are broader and apply against all foreign parties, regardless of whether they are government entities.

China punishes commercial espionage with up to five years of imprisonment. Criminal trade secret violations, by comparison, are punishable by up to three years in prison.

A version of this article first appeared in Law360 on October 4, 2024.

KEY DEVELOPMENTS IN AUSTRALIA

In Australia, there is no legislation that establishes a general regime of trade secret protection. Instead, a legal claim for misuse of confidential information can be brought either in contract or under the equitable doctrine of breach of confidence. Trade secrets are one category of confidential information that can be protected through a breach of confidence action. To establish the cause of action, the "owner" of the confidential information must:

- Identify the information in question with specificity (claims for breach of confidence in Australia often fail at this first hurdle, a good example being the recent decision in *Engadine Medical Imaging Services Pty Ltd atf Engadine Unit Trust v Ibrahim* [2024] NSWSC 1399);
- Establish that the information has the necessary quality of confidence;
- Establish that the information was received in circumstances by which an obligation of confidence was created; and
- Prove actual or threatened use or disclosure of the information without the owner's consent.

There are specific considerations for information developed by an employee in the context of an employment relationship—in some cases, information developed by an employee during the course of employment is considered to be "know-how" and may be used by the employee once an employment relationship ends (subject to any enforceable contractual restraint). Employees and executives may also be subject to equitable obligations arising from the fiduciary nature of the relationship between employer and employee. Australian corporations legislation also prohibits improper use of information obtained in this context.

A range of equitable remedies are available to the court—including *ex parte* search and preservation orders, injunctions, damages or an account of profits (at the applicant's election), and orders for delivery up or destruction of relevant materials. Over many years, *ex parte* search and/or preservation orders at the outset of proceedings have often proven to be an essential weapon in the arsenal of a trade secret owner. By this mechanism, the owner preserves vital evidence, and obtains a clear and early indication of the strength of its case. A recent high-profile decision provides a good example of the usefulness (and serious nature) of search orders in such cases.

Fortescue Limited v Element Zero Pty Limited (No 2) [2024] FCA 1157

Fortescue Limited ("Fortescue") is one of the world's largest producers of iron ore. One of Fortescue's ventures involves creating "green iron," which is iron ore converted into decarbonized iron through a proprietary electrochemical reduction process.

Fortescue alleged that, after providing their notices of resignation, three of its employees (Bartlomiej Kolodziejczyk, Bjorn Winther-Jensen, and Michael George Masterman) misappropriated its proprietary electrochemical reduction process and other confidential information relevant to designing, engineering, constructing, and operating an industrial pilot plant for manufacturing green iron. Fortescue alleged that this information was used to set up a green iron start-up company called Element Zero Limited ("Element Zero"), and also to apply to patent Fortescue's intellectual property under Element Zero's name.

Fortescue applied to the Federal Court of Australia for an *ex parte* search order (also known as an "Anton Piller" order) to enter, search, and remove documents and materials relevant to Fortescue's green iron intellectual property from the former employees' homes and Element Zero's company office. A search order is considered an extraordinary remedy designed to obtain and preserve evidence pending the final resolution of an applicant's claims.

At the *ex parte* hearing, Fortescue successfully established that:

- It had a strong *prima facie* case that its former employees had misappropriated Fortescue's confidential information;
- There was a very serious potential or real risk of loss to Fortescue if the order was not made;
- It had provided sufficient evidence that Element Zero and the former employees possessed the relevant material; and
- There was a real possibility that Element Zero and the former employees might destroy such material if the former employees were given notice of Fortescue's intention to bring an application for breach of confidence.

The Federal Court of Australia therefore granted the search order sought by Fortescue. In executing the search order, Fortescue's lawyers needed to ensure that independent lawyers were present at each premises that was searched pursuant to the order. Those independent lawyers were required to provide a report to the court regarding the execution of the search order and to thoroughly record the documents and other items that were copied or removed from those premises.

After the search order was executed, Element Zero, Kolodziejczyk, and Masterman challenged the granting of the search order, arguing that it should be set aside or varied on the basis that:

a. Fortescue's *prima facie* case was overstated and misrepresented the facts;
b. There was no real risk of destruction of the evidentiary material;
c. There was material non-disclosure by Fortescue when seeking the search orders;
d. Fortescue undertook unnecessarily intrusive surveillance of Element Zero and the former employees, which it deployed in evidence on the search order application; and
e. The form and scope of the search orders were inappropriately broad and resulted in excessive capture of information from Element Zero and the former employees.

The application to discharge the search order was dismissed on the grounds that the applicants could not factually substantiate claims (a) to (d), and could not legally substantiate claim (e).

KEY DEVELOPMENTS IN FRANCE

Trade Secrets Protection Under French Law

With the law of July 30, 2018, France implemented the European directive of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure, inserting new provisions into the French Commercial Code[169] allowing protection of trade secrets from misappropriation.

Requirements for Trade Secret Protection

Three cumulative conditions must be met in order to benefit from trade secret protection: (i) the information must be secret; (ii) it must have commercial value; and (iii) reasonable protection measures must have been put in place in order to keep said information secret.

Several recent rulings, discussed below, provide valuable insight on the conditions under which courts recognize the existence of trade secrets, and on the remedies that trade secret owners can request in the event of breach.

Domino's Pizza v. Speed Rabbit Pizza

The French Supreme Court issued an important ruling on June 5, 2024, in the *Domino's Pizza v. Speed Rabbit Pizza* case,[170] in which it was asked whether the Paris Court of Appeal was correct in holding that a document internal to Domino's Pizza—describing to franchisees how to manage a pizza restaurant and in particular to handle rush hours—was protected by trade secret.

In its decision, the Supreme Court approved the reasoning of the court of appeal as it had noted that the information in the document was not generally known, had a commercial value, and had been made available only to a limited numbers of persons within the franchise group. In addition, the Supreme Court reminded that the court of appeal rightfully found that

trade secrets had been misappropriated because the defendants who had had access to such document should have known that the document had been provided to them in violation of a contractual obligation.

The relevant part of the Supreme Court decision is as follows:

> Having noted, firstly, that Exhibit D3 was a point-of-sale evaluation guide for 2018, containing numerous tips to enable franchisees in the Domino's Pizza network to improve the quality of their management and the profitability of their point-of-sale, and secondly, that this guide had only been sent to members of this network and that it mentioned, at the bottom of each of its pages, its strictly confidential nature as well as the prohibition of any communication outside the network, the Court of Appeal held that this document was a vehicle for transmitting the franchisor's distinctive know-how, and deduced that the information it contained had actual or potential commercial value and was not generally known or easily accessible to people familiar with this type of information in the pizza manufacturing and takeaway sector.
>
> 9. In the light of these observations and assessments, which show, on the one hand, that Exhibit D3 was part of Domino's Pizza's trade secrets, and, on the other hand, that the (…) companies knew or ought to have known that this document had been given to them without Domino's Pizza's consent, and in breach of an obligation of confidentiality to which the companies belonging to the network headed by this franchisor were bound, the Court of Appeal (…) legally justified its decision.

A ruling issued by the Paris Court of Appeal on January 9, 2024,[171] provides another recent example of the similar assessment of the three conditions of trade secret protection:

> In view of the explanations given by the appellant and the nature of these documents, which the court has examined in their entirety, it appears that they qualify as trade secrets, in that they set out a recruitment method and tools consisting of a complex rating system, that they have an actual or potential commercial value and are not known to or easily accessible by third parties, and that they are subject to reasonable protection measures insofar as they are internal documents of [appellant], it being specified that this specific methodology is to be found in e-mails exchanged exclusively between employees of [appellant]: in fact, none of the disputed documents consists of exchanges with third parties or with prospective candidates.

Unlawful Act of Violation of Trade Secrets

French law prohibits the unlawful acquisition, use, and disclosure of trade secrets.

Exxia v. Arcade

The Montpellier Court of Appeal held, in the *Exxia v. Arcade* decision of June 6, 2023, that the mere possession by the defendants of confidential information relating to the claimant's customer database, obtained by former employees of the latter, amounted to unfair competition and violation of trade secret, regardless of the lack of proof that the defendants actually used the misappropriated database.

SAERT v. ROCA

Similarly, in its ruling issued on April 3, 2024, in the *SAERT v. ROCA* case,[172] the Colmar Court of Appeal considered that the mere possession of a former employer's files constituted an act of unfair competition, regardless of the lack of use of the misappropriated information, and assessed damages at €15,000.

This is confirmation of the principle set in three decisions of the French Supreme Court in 2022.

In two other recent rulings, French courts denied trade secret protection because the information was generally available:

- The Paris First Instance Court on December 20, 2023,[173] held that information that could be accessed by merely subscribing to a free software trial could not be considered to be secret; and
- The Paris Court of Appeal on November 29, 2023,[174] held that financial information, such as on a company's investments or corporate bonds, cannot be protected as a trade secret because in this particular case, they were available on the internet and in the management report of the company available on the "Infogreffe," "Pappers," and "Hello Crowdfunding" websites.

Freedom of the Press as an Exception to Trade Secret Protection

Under Article L. 151-8 (1°) of the French Commercial Code, trade secret protection is not enforceable when the acquisition, use, and disclosure of information is required in order to exercise freedom of the press.

Rebuild, SNJ v. Altice Group

The Versailles Court of Appeal[175] applied this exception in its ruling of January 19, 2023, issued in the *Rebuild, SNJ v. Altice Group* case, deciding that the publication by a journalist of an organizational chart allegedly revealing the claimant's development strategy and some of its holdings could not be prohibited. The court ruled that the information benefits from this exception, because the information merely illustrated the points made in the article and/or reinforced the reliability of the information reported on.

Legitimate Holder of Trade Secrets Developed by Employees

The European and French provisions on trade secrets contain no provision regarding identification of the legitimate holder of trade secrets, in particular when they were developed by an employee.

SAERT v. X, ROCA

The Colmar Court of Appeal, on April 3, 2024, in the *SAERT v. X, ROCA* matter, held that trade secrets developed by an employee, in the course of his or her employment contract, belong to the employer.

Remedies in the Case of Trade Secret Breach

Judges can order several measures in the case of violation of trade secret, first and foremost an injunction and damages.

Exxia v. Arcade

In a ruling handed down on June 6, 2023, by the Montpellier Court of Appeal in the *Exxia v. Arcade* case,[176] the court found that trade secret violation had not resulted in any financial damage, but it ordered the destruction of the documents under a daily penalty, prohibited the use of the information, and awarded €50,000 as moral damage based on unfair competition.

LOOKING AHEAD

With more and more trade secret violation cases being filed before French courts, case law continues to expand and develop nuances.

One of the most noteworthy aspects to monitor in this respect is the balance between trade secret protection and the right to evidence, with proportionality emerging as a key criterion.

KEY DEVELOPMENTS IN GERMANY

Germany's Company Secret Act ("GeschGehG"), which was promulgated in 2019 and reported on in Jones Day's 2020 *White Paper*, is now well established and frequently applied to resolve disputes on trade secrets, which has resulted in ample jurisprudence.

Among developments in trade secret protection standards and appropriate security measures to be applied by the secret holder, obtaining a court order for procedural trade secret protection under the GeschGehG is a frequently requested measure in court proceedings and an ongoing source of legal dispute, especially in the context of preexisting nondisclosure agreements ("NDAs").

Higher Court of Düsseldorf, 2 U 102/22 (November 3, 2022)

The Higher Court of Düsseldorf reversed a ruling by the District Court of Düsseldorf that granted a court order for protection of certain information classified as a trade secret.

The Higher Court stressed that the information had been subject to a pre-trial NDA between the parties. The classification of information as a trade secret does not by itself guarantee a court order for protection pursuant to §§ 16 *et seq*. GeschGehG. It remains at the court's discretion whether such order is required. This decision must be made through a balancing of interests and the circumstances at hand, including the terms of NDAs made prior to litigation.

As a result of such balancing of interests, the Higher Court lifted the court order for protection rendered in the first instance. The Higher Court pointed out that, if the parties already had

come to a pre-dispute NDA, using their contractual freedom, it would be an unfair restriction of that freedom to alter the contractual agreement one-sidedly in favor of the plaintiff by way of a court order. Limitations agreed upon within the NDA, such as temporal limitations, are to be respected by the court. This is under the presumption that the preexisting NDA is not evidently inadequate to guarantee confidentiality and that the plaintiff cannot bring forth another compelling argument for additional protection.

District Court of Mannheim, 7 O 91/22 (April 14, 2023), and Higher Court of Karlsruhe, 6 U 122/22 (October 10, 2023)

Similarly, the District Court of Mannheim ruled that there is no justified interest for additional protection of trade secrets by a procedural order in cases where the defendant has already contractually undertaken to keep the information confidential, e.g., within the framework of an NDA.

The district court stated that an additional interest in protection of the secret holder against disclosure by third parties involved in the dispute, such as judges and clerks of the registry, does not justify an application for protection pursuant to §§ 16 *et seq*. GeschGehG. It was pointed out that those personnel were already bound to confidentiality by other laws concerning their professional standards and duties, and their obligation to confidentiality by the GeschGehG was merely a legal consequence thereof, not an individually enforceable claim of the secret holder.

The Higher Court of Karlsruhe, however, lifted this decision. It ruled that the need for legal protection by way of an order under § 16 *et seq*. GeschGehG is not precluded by the fact that the parties have already contractually agreed to keep the information confidential. The Higher Court recognized the secret holder's interest in establishing confidentiality toward other persons involved as well, in particular to bind court personnel to confidentiality via the GeschGehG. The court pointed out that it was required to bind the court personnel by a court order limiting or prohibiting immediate and future file access, as this appropriate protection would exceed their standard professional duties of confidentiality. And such protection also exceeded the confidentiality created by the NDA constructed between the parties.

This ruling does not directly contradict the ruling of the Higher Court of Düsseldorf, which pointed out that a case-by-case consideration is required. However, the different views on the need for additional protection via a court order under §§ 16 *et seq*. GeschGehG may result in a decision of the German Federal High Court mapping out the requirements for such a protective order in more detail, particularly in cases involving preexisting NDAs.

Higher Court of Schleswig, 6 U 39/21 (April 28, 2022)

The Higher Court of Schleswig ruled on whether a description of the content and a reference to an Excel sheet was sufficient to determine the relevant trade secrets subject to the legal action.

The defendant argued that the plaintiff's application for injunctive relief does not meet the principle of certainty according to German procedural law, since neither the Excel sheet in question nor its specific content had been made available to the court and the defendant, thereby not revealing to the defendant which action or use of information he was to refrain from. The Higher Court, however, held that the application for injunctive relief just describing the content of a specific Excel sheet may be admissible even if the trade secret is neither mentioned in the application nor part of the court files. The application for relief meets the principle of legal certainty as long as the defendant can reasonably identify the relevant document in question. This was found to be the case here, since the plaintiff had given a sufficiently detailed description of the Excel sheet and its content, and the defendant could not reasonably claim to possess any similar documents in danger of confusion.

Furthermore, the court ruled that the plaintiff applied appropriate confidentiality measures within the meaning of the GeschGehG. The court held that such confidentiality measures must be evaluated from an objective *ex ante* perspective, i.e., whether they objectively had the potential to ensure confidentiality of the information. And the court held that "appropriate" also means that less valuable trade secrets require a lower level of confidentiality measures. The court confirmed that, taking into account the value of the trade secret at hand, TLS encryption of emails, and a proper selection of the recipients were sufficient even though the persons acting on behalf of the secret holder had not entered into explicit confidentiality agreements regarding the trade secrets in question and contractual confidentiality clauses were invalid.

KEY DEVELOPMENTS IN THE UNITED KINGDOM

New National Security Legislation Criminalizes the Theft or Unauthorized Disclosure of Trade Secrets on Behalf of a Foreign Power

The National Security Act 2023 introduced new measures to protect UK national security against the growing threats of foreign interference, corporate espionage, and sabotage. Section 2 of the Act focuses on trade secrets. The Act came into force in December 2023, expanding government powers to monitor and regulate the commercial conduct of both national and foreign actors operating in the United Kingdom.

Section 2(1) of the Act provides that a person commits an offense if they: (i) obtain, copy, record, retain, or disclose a trade secret; or (ii) provide access to a trade secret without authorization—knowing, or reasonably knowing, that their conduct is unauthorized—or on behalf of a foreign power.

The Act adopts a broader definition of "trade secret" than the United Kingdom's principal Trade Secrets (Enforcement, etc.) Regulations 2018. Significantly, Section 2(2) provides that trade secrets encompass information with "*actual or potential* industrial, economic, or commercial value" that could "reasonably be expected" to be kept confidential irrespective of whether that information is actually subject to confidentiality restrictions.

Moreover, the Act adopts an expansive view of what it means to act on behalf of a foreign power, as clarified by Section 31, "the foreign power condition." Specifically, Section 31(1) establishes that an individual can act on behalf of a foreign power if they know, or if they reasonably ought to have known, they were doing so. Section 31(3) clarifies that the individual's relationship to the foreign power could be direct or indirect and provides an example of a relationship through one or more companies. Connection via financial "or other assistance" is also identified as a factor that would establish a connection between an individual and a foreign actor.

This broad approach speaks to the Act's efforts to bolster legal protections against corporate espionage, in an era of increasing overlap between multinational corporations and state actors.

Applications for Amending Pleadings in Litigation Must Be Clear and Specific When Dealing With a Breach of Confidence Case

Illiquidx Ltd v Altana Wealth Ltd [2024] EWHC 2191 (Ch)

Illiquidx Ltd alleged that Altana Wealth Ltd committed a breach of confidence and compromised its trade secrets when it publicized information about distressed Venezuelan sovereign debt. The claimant contended that the information it had shared with the defendant, about the existence of this sovereign debt and associated business opportunities, was itself confidential.

Over the course of the claim, Illiquidx filed for permission to re-amend a confidential annex to the particulars of its claim. Specifically, it sought to plead further detail and clarify certain points to address the defendants' complaints. This application followed previous rounds of amendments, which the parties had agreed among themselves.

The court rejected Illiquidx's application. It held that the proposed amendments did not meaningfully outline why the new information was confidential. In turn, it maintained they would be largely irrelevant.

Confidentiality Over Documents Relied Upon in Litigation Is Relative and Fact-Specific

IBM UK Ltd v LzLabs GmbH [2024] EWHC 423 (TCC)

The claimant, IBM UK Ltd, alleged that the LzLabs (the first defendant) had conspired with the second defendant, an IBM licensee, to develop software using confidential information obtained from IBM through its licenses. Given the commercial sensitivity of the documents, the parties had initially agreed upon a confidentiality ring.

However, the claimant subsequently requested that the parties reconsider the various confidentiality designations. In turn, the court was asked to decide how confidential information should be defined and ringfenced for the purposes of this exercise.

The court relied on established legal authority to rule that confidential information comprised private information outside the public domain and not accessible by the public. Rather than giving a specific set of rules, it reinforced that confidentiality is fact- and context-specific and must be approached in a relative way.

High Court Maintains that "Open Justice [Must] Take Second Place to the Preservation of Trade Secrets" and Endorsed Extensive Redactions of Confidential Information in a Judgment

Optis Cellular Technology LLC v Apple Retail UK Ltd [2024] EWHC 197 (Ch)

The parties to the case were allowed to voluntarily redact a court judgment, before it was made public, to protect confidential information about their third-party licenses.

The Court was not involved with the process but, after receiving the final redactions, became concerned about the possibility of over-redaction. The question was decided in a subsequent judgment on consequential matters handed down in February 2024.

The Court held that the protection of trade secrets must be prioritized over open justice. In its judgment, it reflected on the notion that "open justice must give way to a greater principle, which is justice itself"—including how courts will cede ground to confidentiality when arranging trade secret hearings. In turn, it maintained that the heavy redactions to the judgment could remain.

When Considering if an Employee Had Committed a Breach of Confidence, the High Court Outlines the Factors that Could Lead to an Implied Duty of Confidentiality Extending Beyond an Employment Contract

Titan Wealth Holdings Ltd v Okunola [2024] EWHC 2718 (KB)

Titan advanced claims against the defendant in breach of confidence, among other causes of action.

Following the termination of an employment contract with the claimant (Titan), the defendant had sent emails and made social media posts containing confidential information. The Court was asked to decide whether the employee had committed a breach of confidence—specifically considering whether they had an enduring "obligation of confidence," despite the termination of their employment.

The Court found that the defendant had committed a breach of confidence, because of an implied duty of confidentiality extending beyond the employment contract. In the judgment, it outlined the factors that needed to be weighed when establishing whether the implied duty of confidentiality continued. These were:

- The nature of the work being carried out;
- The information to which the employee had access;
- The market reputation of the employer;
- The security of the employer's information and management systems;
- The employer's previous success in maintaining client confidentiality;
- The nature of the information being disclosed; and
- Whether the employer had impressed on the employee their implied duty of confidentiality after the end of their employment relationship.

Employers should take note of the above when formulating or updating their employment policies and contracts. They may wish to include express provisions in employment contracts outlining employees' duty of confidentiality after termination and implement procedures to re-communicate this duty to outgoing employees, through exit interviews or written reminders.

In addition, employers may wish to put in place regular training programs on their confidentiality expectations and systems. Over time, these will continue to "impress" on employees their post-employment confidentiality duties and may serve as compelling evidence in any court proceedings.

Individuals Can Commit Breach of Confidence Even if They Are Not Aware of What They Are Doing or Aware It Is a Legal Wrong

Kieran Corrigan & Co Ltd v Timol [2024] EWCA Civ 1233

In the UK Court of Appeal, the appellant (Kieran Corrigan & Co) appealed against the dismissal of its claims for breach of confidence against the respondent (Bashir Timol). The appellant had approached two tax advisers who worked for a company, of which the respondent was a director and minority shareholder, about a possible joint venture.

The appellant shared significant information about its trade over the course of negotiations; however, the joint venture never materialized. Shortly after, the company altered its structure based on a tax proposal put forward by the appellant during negotiations. The appellant therefore pursued the company (as well as the tax advisers and Timol in their personal capacities) for breach of confidence.

At first instance, Timol was found to have no liability since he had not been involved in developing the structure, had no understanding of its technical workings, and was unaware that it used the appellant's confidential information.

On appeal, the first instance decision was overturned and a retrial of Timol's liability was ordered. The court drew from *Paymaster (Jamaica) v Grace Kennedy Services* [2017] UKPC 40 to reaffirm that "conscious plagiarism was not a necessary component of breach of confidence." The fact that Timol had merely signed off on the new corporate structure, even without an understanding of its technical nature, was not enough to prevent him being liable.

Similarly, the court held it did not matter for the purposes of establishing a breach of confidence that Timol had not: (i) directly received the confidential information; and (ii) was not aware that approving the corporate structure would amount to misuse. It reaffirmed that as long as an individual uses the relevant information, it is possible for him to commit a breach of confidence without being aware he is committing a legal wrong.

This case will be of particular interest to company directors, who may wish to seek legal advice before implementing proposals constructed in collaboration with other legal entities.

LAWYER CONTACTS

Jeffrey Baltruzak
Pittsburgh
+1.412.394.7909
jbaltruzak@jonesday.com

Thomas Bouvet
Paris
+33.1.56.59.39.39
tbouvet@jonesday.com

Mark E. Earnest
Irvine
+1.949.553.7580
mearnest@jonesday.com

Margaret C. Gleason
Pittsburgh
+1.412.394.7235
mcgleason@jonesday.com

Michael A. Gleason
Washington
+1.202.879.4648
magleason@jonesday.com

Jakob Guhn
Düsseldorf
+49.211.5406.5500
jguhn@jonesday.com

Richard Hoad
Melbourne
+61.3.9101.6800
rhoad@jonesday.com

Haifeng Huang
Hong Kong/Beijing
+852.2526.6895/+86.10.5866.1111
hfhuang@jonesday.com

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

Randy Kay
San Diego/Silicon Valley
+1.858.314.1139/+1.650.739.3939
rekay@jonesday.com

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

Kristin Berger Parker
Minneapolis
+1.612.217.8847
kparker@jonesday.com

Robert N. Stander
Washington
+1.202.879.7628
rstander@jonesday.com

Rebecca Swindells
London
+44.20.7039.5845
rswindells@jonesday.com

Steven M. Zadravecz
Irvine/Los Angeles
+1.949.553.7508/+1.213.243.2195
szadravecz@jonesday.com

The following associates contributed to this White Paper: Kezia Adams, Colin Devinant, Michael B. Gallagher, Kevin Ganley, Nicholas Hodges, Rachel McKenzie, Ryan T. Nelson, Alyssa M. Orellana, Shane Padilla, Connor G. Scholes, Daniel C. Sloan, Tova Werblowsky, and Ariana Shaina Wilner.

ENDNOTES

1 *Insulet Corp. v. EOFlow, Co.*, 104 F.4th 873, 877–78 (Fed. Cir. 2024).
2 *Id.*
3 *Id.* at 878.
4 *Id.*
5 *Insulet Corp. v. EOFlow, Co.*, 2024-cv-1137, 2024 WL 2115888 (Fed. Cir. May 7, 2024).
6 *Insulet*, 104 F.4th at 880–884.
7 *Id.* at 881.
8 *Id.*
9 *Id.*
10 *Id.* at 881–83.
11 Jury Verdict at 4–5, 10–11, *Insulet Corp. v. EOFlow, Co.*, 23-cv-11780 (D. Mass. Dec. 3, 2024), ECF No. 833
12 *Id.* at 4.
13 Summ. J. Order at 12, 19–21, *Insulet*, 23-cv-11780 (D. Mass. Oct. 31, 2024), ECF No. 753.
14 *Danieli Corp. v. SMS Group, Inc.*, 21-cv-1716, 2024 WL 3791894, at *1 (W.D. Pa. Aug. 13, 2024).
15 *Id.*
16 *Id.* at *13.
17 *Id.* at *2.
18 *Id.* at *1, *7.
19 *Id.* at *12 (emphasis removed).
20 *Id.*
21 *Id.* at *12 (citing *Mallet & Co. v. Lacayo*, 16 F.4th 364, 381 n.19 (3d Cir. 2021)).
22 *See id.* at *11.
23 *Id.* at *10–13.
24 *Id.* at *13.
25 *In re: Island Indus., Inc.*, 23-cv-5200, 2024 WL 869858, at *2 (6th Cir. Feb. 29, 2024); 18 U.S.C. § 1836(b);.N.J. Stat. ann. § 56:15-1, *et seq.*; tenn. Code ann. § 47-25-1701, *et seq.*

26 *Id.* at *3, 6 (recognizing that "sister circuits in recent years have affirmed dismissal for failure to adequately plead reasonable measures of trade secret protection.").

27 *Id.* at *4.

28 *Id.*

29 *Id.* at *5.

30 *Id.* at *6.

31 *Id.*; 18 U.S.C. §§ 1836–39; Ohio Rev. Code Ann. § 1333.61.

32 *James B. Oswald Co. v. Neate,* 98 F.4th 666, 671–72 (6th Cir. 2024).

33 *Id.*

34 *Id.* at 677.

35 *Id.* at 675–76.

36 *Id.* at 676 ("[W]hen Neate quotes *Gallagher* saying 'customer information' is not a trade secret if it is 're-creatable from public sources on the internet *or from customers themselves*,' . . . this assertion only applies directly to publicly available information." (citation omitted)).

37 *Id.*

38 *Id.*

39 *Id.* at 677.

40 *Id.* at 679.

41 *Jacam Chem. Co. 2013, LLC v. Shepard*, 101 F.4th 954, 960 (8th Cir. 2024).

42 *Id.*

43 *Id.* at 965.

44 *Id.* at 964.

45 *Id.* at 965.

46 *Id.* at 966, 969.

47 *Id.* at 965.

48 *Id.*

49 *Compulife Software, Inc. v. Newman*, 111 F.4th 1147, 1153 (11th Cir. 2024).

50 *Id.* at 1153, 1160 n. 1.

51 *Id.* at 1154.

52 *Id.* at 1160 n.1.

53 *Id.* at 1161–62.

54 *Id.*

55 *Id.* at 1162.

56 *Id.* at 1163.

57 *Id.*

58 *Id.* at 1154.

59 *Id.*

60 *BioPoint, Inc. v. Dickhaut*, 110 F.4th 337, 343 (1st Cir. 2024).

61 *Id.* at 342–43.

62 *Id.* at 345.

63 *Id.* at 346.

64 *Id.* at 347–50.

65 *Id.* at 349.

66 *Id.* at 349–50.

67 The court did not address whether expert costs incurred in stopping or mitigating misappropriation, or any other broader set of expert costs, would be recoverable under a breach of contract theory; the issue is left open for further clarification going forward.

68 *Motorola Sols., Inc. v. Hytera Commc'ns. Corp. Ltd.*, 108 F.4th 458, 469–70 (7th Cir. 2024).

69 *Id.* at 471.

70 *Id.* at 484.

71 *Id.* at 472.

72 *Id.* at 472–73.

73 *Id.* at 473.

74 *Id.* (quoting *RJR Nabisco, Inc. v. European Community*, 579 U.S. 325, 337 (2016)).

75 *Id.* at 480.

76 *Id.*

77 *Id.* (quoting *RJR Nabisco*, 579 U.S. at 337–38).

78 *Id.* at 483.

79 *Id.*

80 *Id.* at 484.

81 *Id.*

82 *Id.*

83 *Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Grp., Inc.*, 68 F.4th 792, 796–797 (2d Cir. 2023), *cert. denied*, No. 23-306, 2023 WL 7117087 (U.S. Oct. 30, 2023).

84 *Id.* at 797.

85 *Id.* at 797–798.

86 *Id.* at 799.

87 *Id.* at 798.

88 *Id.* at 799.

89 *Id.* at 798–799.

90 *Id.* at 799.

91 *Id.*

92 *Id.*

93 *Id.* at 806–07, 814.

94 *Id.* at 809.

95 *Id.* at 811.

96 *Id.* at 811–12.

97 *Id.* at 811–14.

98 *Id.*

99 *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Grp., Inc.*, 15-cv-211, 2024 WL 1116090, at *1 (S.D.N.Y. Mar. 13, 2024)

100 *Id.* at *3.

101 *Id.*

102 *Id.* at *1 n.2.

103 *Id.* at *8.

104 *Pegasystems Inc. v. Appian Corp.*, 81 Va. App. 433, 448 (2024).

105 *Id.* at 449.

106 *Id.* at 450–51.

107 *Id.* at 448.

108 *Id.* at 468.

109 *Id.* at 469–70.

110 *Id.*

111 *Id.* at 470.

112 *Id.* at 470.

113 *Id.* at 472–75.

114 *Id.* at 508.

115 *Id.* at 477.

116 *Id.* at 461.

117 *Id.* at 502–08.

118 *Id.* at 459–60.

119 *Id.* at 497–98.

120 *Id.* at 501.

121 *Id.* at 503.

122 *Id.* at 504.

123 *Perrin Bernard Supowitz, LLC v. Morales*, 22-cv-02120, 2023 WL 1415572, at *7–13 (C.D. Cal. Jan. 31, 2023), *aff'd*, 23-cv-55189, 2024 WL 411714 (9th Cir. Feb. 5, 2024)

124 *Id.* at *13.

125 *Id.* at *14 (quoting *Hynix Semiconductor Inc. v. Rambus Inc.*, 609 F. Supp. 2d 951, 968 (N.D. Cal. 2009)).

126 *Perrin Bernard Supowitz, LLC v. Morales*, No. 23-55189, 2024 WL 411714, at *2 (9th Cir. Feb. 5, 2024).

127 *Id.*

128 *Id.* (*see Whyte v. Schlage Lock Co.*, 125 Cal. Rptr. 2d 277, 284–85 (Cal. Ct. App. 2002)).

129 U.S. Fed. Trade. Comm'n, "FTC Announces Rule Banning Noncompetes" (Apr. 23, 2024).

130 16 C.F.R. §§ 910.1–.2 (2024).

131 *Id.*

132 16 C.F.R. § 910.2.

133 Complaint at 4, *Ryan, LLC v. FTC*, 24-cv-00986 (N.D. Tex. Apr. 23, 2024), ECF No. 1.

134 *Ryan*, *LLC*, 2024 WL 3297524, at *4 (N.D. Tex. July 3, 2024).

135 *Id.* at *7–12.

136 *Ryan, LLC*, 2024 WL 3879954, at *12 (N.D. Tex. Aug. 20, 2024).

137 *Id.* at *13–14.

138 *Id.* at *14.

139 Notice of Appeal, *Ryan*, *LLC*, 24-cv-00986 (Oct. 18, 2024), ECF No. 213.

140 *Props. of the Villages, Inc. v. FTC*, 24-cv-00316, 2024 WL 3870380, at *1 (M.D. Fla. Aug. 15, 2024).

141 *Id.* at *2; *see also* Proposed Order on Motion for Preliminary Injunction, *Villages*, 24-cv-00316, 2024 WL 3870380 (M.D. Fla. Aug. 15, 2024), ECF No. 25-2.

142 *Villages*, 2024 WL 3870380 at *3–5.

143 *Id.* at *5.

144 *Id.*

145 *Id.* at *8–11.

146 *See* Notice of Appeal, *Villages*, 24-cv-00316, 2024 WL 3870380 (M.D. Fla. Sep. 24, 2024), ECF No. 64.

147 *ATS Tree Servs., LLC v. FTC*, 24-cv-1743, 2024 WL 3511630, at *1 (E.D. Pa. July 23, 2024).

148 *Id.* at *11, *19.

149 *See* Notice of Voluntary Dismissal at 1, *ATS Tree Servs., LLC v. FTC*, 24-cv-1743 (E.D. Pa. Oct. 4, 2024), ECF No. 92.

150 Cal. Sen. Bill No. 699 (Sept. 1, 2023); *see* Cal. Bus. & Prof. Code § 16600.5.

151 Cal. Sen. Bill No. 699 Sec.§ 2 (Sept. 1, 2023); *see* Cal. Bus. & Prof. Code § 16600.5(a).

152 *DraftKings Inc. v. Hermalyn*, 118 F.4th 416, 418 (1st Cir. 2024).

153 *Id.* The employee's attempt was predictable, and his success or failure potentially dispositive: "Everyone seems to agree (at least for present purposes) that if the noncompete is enforceable, Hermalyn breached it by joining Fanatics. Not surprisingly then, DraftKings asked the district judge to use Massachusetts law and Hermalyn asked her to use California law." *Id.*

154 *Id.* at 420.

155 Veto Letter from Governor Janet T. Mills, L.D. 1496, at 1 (Mar. 29, 2024).

156 *Id.*

157 *Geely v. WM Motor*, the Supreme People's Court, case number: (2023) Zui Gao Fa Zhi Min Zhong No. 1590.

158 Article 283, Civil Procedure Law of the People's Republic of China (2023 Amendment).

159 Article 32, Anti-Unfair Competition Law (amended 2019) (China).

160 *Id*.

161 *Id.*

162 Article 17, Anti-Unfair Competition Law (amended 2019) (China).

163 *Id.*

164 Articles 24 and 25, Several Provisions of the Supreme People's Court on Evidence in Civil Procedures Involving Intellectual Property Rights.

165 *Geely v. WM Motor*, the Supreme People's Court, case number: (2023) Zui Gao Fa Zhi Min Zhong No. 1590.

166 Notice by the Supreme People's Procuratorate and the Ministry of Public Security of Issuing the Decision on Amending the Criteria for Launching Formal Investigation into Criminal Cases of Infringement upon Trade Secrets (2020).

167 Jerry Xia, Ning Dong, and Yulu Wang, Trade Secrets 2024: China, Chambers and Partners, April 25, 2024.

168 Criminal Law art. 219-1 (China).

169 Articles L. 151-1 *et seq.* of the French Commercial Code.

170 French High Court, June 5, 2024, *Domino's Pizza v. Speed Rabbit Pizza*, Docket No 23-10.954.

171 Paris Court of Appeal, January 9, 2024, Docket No 22/17869.

172 Colmar Court of Appeal, April 3, 2024, *SAERT v. ROCA*, Docket No 22/01026.

173 Paris First Instance Court, December 20, 2023, Docket No 21/07924.

174 Paris Court of Appeal, November 29, 2023, *Cap Investissements et al. v. X*, Docket No 22/04955.

175 Versailles Court of Appeal, January 19, 2023, *Rebuild, SNJ v. Altice Group*, Docket No 22/06176.

176 Montpellier Court of Appeal, June 6, 2023, *Exxia v. Arcade*, Docket No 21/04644.