2023 Year-End Review: Key Trade Secret Developments

WHITE PAPER | By Kelsey I. Nix, Shameka C. Rolla and Dani B. Dobosz

A trade secret is any information used in one's business that derives independent economic value from not being generally known. Trade secrets, unlike patents, are protected indefinitely for as long as they remain a secret. Due in large part to enactment of the Defend Trade Secrets Act in May 2016 which made trade secret misappropriation a federal cause of action, trade secrets have become an increasingly attractive form of intellectual property for businesses to protect their innovations.

This White Paper summarizes and explains noteworthy decisions in trade secret law over the past year. Each of these decisions has meaningful implications for trade secret owners, defendants, and practitioners alike.

Contents

Pleading Standards for Trade Secret Cases

EIGHTH CIRCUIT RULES THAT, IN SOME CIRCUMSTANCES, IT IS SUFFICENT TO PLEAD TRADE SECRET MISAPPROPRIATION ON INFORMATION-AND-BELIEF

Ahern Rentals, Inc. v. EquipmentShare.com, Inc., 59 F.4th 948 (8th Cir. 2023)

Ahern is a large national company that rents construction equipment.[1] EquipmentShare was founded in 2014 and became a top competitor to Ahern.[2] As it expanded, EquipmentShare hired many former employees from Ahern.[3] Ahern sued EquipmentShare and several individual defendants in 2019 alleging that EquipmentShare recruited Ahern employees to steal trade secrets before leaving to work at EquipmentShare.[4] The federal causes of action were consolidated as a multidistrict litigation (MDL).[5] In 2020, Ahern initiated a new suit against EquipmentShare and another company, EZ.[6] EZ allows users to make money by renting out their own equipment through EquipmentShare.[7] EquipmentShare and EZ thus have a close business relationship.[8]

Ahern's suit alleged, based on "information and belief," that EZ was using trade secrets obtained illegally by EquipmentShare with knowledge that the information was ill gotten.[9] EZ moved to dismiss Ahern's claims, which the district court granted, noting that all claims alleging EZ's involvement and knowledge were pled solely upon information and belief.[10] The district court held that "allegations pled only on information and belief do not nudge the claim[s] across the line from conceivable to plausible as required by *Iqbal* and *Twombly*."[11]

On appeal, the Eighth Circuit considered the sufficiency of Ahern's complaint against EZ, noting that "we have never fully articulated when plaintiffs may use upon-information-and-belief pleadings in a complaint to satisfy Twombly's plausibility requirement."[12] But the court reasoned that "where the proof supporting the allegation is within the sole possession and control of the defendant or where the belief is *based on sufficient factual material that makes the inference of culpability plausible*," allegations pled only on information and belief "are not categorically insufficient to state a claim for relief."[13]

The court then analyzed Ahern's complaint under this framework and concluded that (1) "Ahern adequately alleges the existence of protectable trade secrets," but (2) it is a "closer question . . . whether Ahern plausibly alleges that EZ has 'misappropriated' those trade secrets."[14] Misappropriation under the DTSA and Missouri law includes an element of knowledge that the trade secret was "derived from or through a person who had used improper means to acquire the trade secret."[15] The court concluded that because the "detailed allegations, taken as true, make clear that EquipmentShare's programs were at the core of EZ's operations . . . it is entirely plausible to infer that EZ knew it was using programs developed through the exploitation of trade secrets."[16] The Eighth Circuit thus reversed EZ's dismissal and remanded to the district court.[17]

Standards to Qualify as a Trade Secret

FIRST CIRCUIT AFFIRMS SUMMARY JUDGMENT AGAINST FORMER INSURANCE AGENTS WHO MISAPPROPRIATED CUSTOMER INFORMATION

Allstate Insurance Co. v. Fougere, 79 F.4th 172 (1st Cir. 2023)

Allstate Insurance Company ("Allstate") sued two former independent agents and the insurance agency operated by one of the agents for breach of contract and trade secret misappropriation under common law and the Defend Trade Secrets Act ("DTSA").[18] The defendants denied wrongdoing and filed various counterclaims against Allstate.[19]

During discovery, the defendants produced spreadsheets containing the names of thousands of Allstate customers, along with their renewal dates, premiums, types of insurance, Allstate policy numbers, driver's license numbers, home addresses, phone numbers and email addresses.[20] Following discovery, both sides filed partial motions for summary judgment.[21] The district court determined that the spreadsheets retained by the defendants constituted Allstate's confidential and trade secret information and granted summary judgment for Allstate on its claims for breach of contract and misappropriation of trade secrets.[22] The district court denied defendants' motion for reconsideration.[23]

Allstate opted to dismiss its remaining claims and was awarded nominal damages (amounting to $2.00 for both of its contract claims), an award of attorneys' fees and a permanent injunction enjoining the defendants from using, processing or having access to Allstate confidential information.[24] Defendants appealed.[25]

Focusing on Allstate's claims for trade secret misappropriation under the DTSA and Massachusetts common law and in breach of the agents' exclusive agency agreements with Allstate, on appeal the First Circuit concluded that the spreadsheets at issue qualified as trade secrets.[26] First, the court determined that, although the spreadsheets included some information that could have been obtained from public sources, the spreadsheets – which listed thousands of Allstate customers along with their personal and policy information – were still trade secrets.[27] The court explained that "the inclusion of some information in compilations which could have been obtained from public sources does not mean the compilations were not trade secrets, and that trade secrets may be found, even as to that information, when it would have been *immensely difficult* to collect and compile it in the form in which it appeared in the compilation."[28] Second, relying on the exclusive agency agreements' statement that misuse of the company's confidential information would cause irreparable damage that could not be adequately compensated or remedied by any monetary award or damages, the First Circuit concluded that the spreadsheets had independent economic value.[29] Third, in deciding that Allstate took reasonable steps to protect its trade secrets, the First Circuit looked to (a) the confidentiality provisions in the exclusive agency agreements; (b) Allstate only granting access to the information to agents; (c) Allstate restricting the availability of the information through the use of passwords; (d) upon termination, revoking access by former agents; and the fact that (e) the information was not in the public domain or readily ascertainable.[30]

The First Circuit also concluded that Allstate owned the spreadsheets, stating that any role that the agents played in compiling the spreadsheets was irrelevant for the purposes of determining ownership because the exclusive agency agreements established Allstate as the owner of the customer information included in the spreadsheets.[31]

Finally, the First Circuit concluded that there was sufficient evidence in the record to conclude that both former agents misappropriated Allstate's trade secrets and, by settling for nominal damages instead of proceeding to trial on actual damages, Allstate took the scope, but not the question, of the agent's liability off the table.[32] Accordingly, the First Circuit affirmed the district court's grant of summary judgment to Allstate on liability for its trade secret and contract claims against the defendants.[33]

DISTRICT COURT GRANTS SUMMARY JUDGMENT BECAUSE TRADE SECRETS WERE TOO VAGUE AND/OR WERE ACCESSIBLE BY COMPUTER-SAVVY USERS

***Card Isle Corp. v. Farid*, -- F. Supp.3d --, 2023 WL 5618246 (N.D. Ga. 2023)**

Card Isle Corp. ("Card Isle") is a small technology company that provides coding systems and technology infrastructure to enable companies to sell personalized greeting cards on their websites.[34] In 2019, Card Isle contracted with Edible Arrangements, LLC ("Edible Arrangements") and its founder, Tariq Farid, to provide the "infrastructure and support" for Edible Arrangements to launch a new, customizable greeting card product.[35]

After entering into three contracts related to the proposed business relationship, Edible Arrangements backed out of the deal and halted its plans to launch Card Isle's program.[36] Edible Arrangements alleged it was concerned about Card Isle's offerings and worked with a different vendor instead. In response, Card Isle argued that Edible Arrangements and its replacement vendor copied its copyrighted code and trade secrets in rolling out its alternate product.[37]

Card Isle sued Edible Arrangements and Netsolace, Edible Arrangements' replacement vendor, for breach of contract, misappropriation of trade secrets and copyright infringement, seeking damages and an injunction halting the use of Card Isle's trade secrets and copyrighted code.[38] The parties filed cross motions for summary judgment.[39]

Card Isle defined its three asserted trade secrets as: (1) its "E-Commerce Integration Blueprint," which is "an explanation of the relevant components of Card Isle's technology and a unique block of code written for the specific retailer's website," (2) "the underlying functionality" referred to by Card Isle's JavaScript libraries, and (3) a "combination of unique pieces," including Card Isle's technical know-how, approach to solving problems and organization of individual pieces of technology.[40]

Edible Arrangements argued that Card Isle's alleged trade secrets were "available to the public" and therefore not entitled to trade secret protection.[41] First, the Edible Arrangement's expert explained that because "the content of a webpage rendered in a browser can be accessed and inspected using the developer tools built into most modern web browsers," including via "right click" on the web browser, the "E-Commerce Integration Blueprint" was available to any discerning computer user, and therefore was readily ascertainable.[42] The district court found that Card Isle failed to meet its burden of showing that the E-Commerce Integration Blueprint was not "readily ascertainable."[43]

Card Isle's second alleged trade secret fared no better. The district court found that the code "cannot qualify as trade secret[]" because the "underlying functionality referred to by the Javascript libraries" was accessible to users of Edible Arrangements' website by using the browser's developer tools.[44]

Finally, the district court found that Card Isle's third alleged trade secret, "the combination of its technical know-how, approach to solving problems, and organization of individual pieces of technology," lacked a specific enough description for the court to discern what the claimed trade secret was.[45] It thus concluded the third alleged trade secret was "too vague and too inclusive to be considered a trade secret."[46]

Because all three of Card Isle's alleged trade secrets failed to pass muster, the court granted the motion for summary judgment in its entirety as to the trade secrets claim.[47]

FOURTH CIRCUIT FINDS A CONDITIONAL COVENANT-NOT-TO-SUE INSUFFICIENT TO MOOT A DECLARATORY JUDGMENT ACTION

***Synopsys, Inc. v. Risk Based Security, Inc.*, 70 F.4th 759 (4th Cir. 2023)**

Risk Based Security ("RBS") is a security company that curates and licenses VulnDB, a database of open-source software vulnerabilities.[48] One VulnDB licensee, Black Duck Software, was acquired by a RBS competitor, Synopsys.[49] Believing Black Duck and Synopsys to have misappropriated portions of VulnDB, RBS sued in Massachusetts state court.[50] In 2021, Synopsys became authorized to designate and publicly report software vulnerabilities through the federally sponsored Common Vulnerabilities and Exposures (CVE) program.[51]

RBS sent Synopsys a cease-and-desist letter, demanding that Synopsys refrain from designating software vulnerabilities to the CVE until their pending VulnDB litigation was resolved.[52] Synopsys responded with a declaratory judgment action in the Eastern District of Virginia, seeking a declaration that Synopsys did not misappropriate RBS's trade secrets.[53] Perhaps preferring to resolve the misappropriation issue in a forum of its choosing, RBS withdrew its cease-and-desist letter and sent Synopsys a covenant not to sue. However, the covenant and withdrawal were conditioned upon Synopsys's future work being "the product of its independent research and not based on any vulnerability database."[54] RBS then moved to dismiss the declaratory judgment action as moot. The district court denied the motion, explaining that "RBS has not demonstrated that the covenant remedies or prevents the injuries Synopsys alleges."[55]

After resolving dueling *Daubert* motions and excluding one RBS expert's testimony on the economic value of RBS's asserted trade secrets, the district court granted summary judgment to Synopsys. On appeal, the Fourth Circuit reexamined the district court's holdings that the case was not moot, excluding RBS's expert and granting summary judgment.

On the mootness issue, the Fourth Circuit applied the standard from *Already, LLC v. Nike*[56] by inquiring whether it was "absolutely clear" that the injury Synopsys sought to prevent by its declaratory judgment action "could not reasonably be expected to recur."[57] The court agreed that the case was not moot, giving three reasons. First, "the covenant not to sue and withdrawal letter only partially addressed the entire dispute."[58] Second, the covenant and withdrawal were "conditioned on Synopsys's future performance," leaving it less than "absolutely clear" that "RBS's allegedly wrongful behavior could not reasonably be expected to recur."[59] Finally, the covenant and withdrawal "were revocable at [RBS's] discretion and thus fell further short of the high benchmark established in *Already*."[60]

Turning to the *Daubert* issue, which courts of appeal review on an abuse of discretion standard, the Fourth Circuit upheld the exclusion of the expert's testimony on the economic value of the contested trade secrets.[61] The court agreed that the expert "had not demonstrated that he'd reviewed the alleged trade secrets individually" and made only "conclusory assertions about the trade secrets contained in the database."[62] The court rejected RBS's argument that an expert does not need to opine on the value of individual trade secrets if he establishes the value of the group of trade secrets, finding that "[e]ven if grouping is appropriate in some cases, it must be done in a way that permits the trier of fact to undertake this review."[63]

Left with no admissible evidence on the independent economic value of the claimed trade secrets, the Fourth Circuit affirmed summary judgment for Synopsys.

DISTRICT COURT SETS ASIDE $64 MILLION JURY VERDICT BECAUSE TRADE SECRETS WERE INDEFINITE OR NOT "SECRET"

***Coda Dev. s.r.o. v. Goodyear Tire & Rubber Co.*, No. 15-cv-1572 (N.D. Ohio Mar. 31, 2023)**

A Czech inventor and his company, Coda Development, demonstrated self-inflating tire prototypes and disclosed testing results to Goodyear at preliminary meetings in 2009 subject to a non-disclosure agreement.[64] After discovering that Goodyear had applied for a self-inflating tire patent shortly after their meeting, Coda sued Goodyear for misappropriation of trade secrets and correction of inventorship of Goodyear's patent in 2015.[65] The district court dismissed the trade secret claim as time-barred, but the Federal Circuit overturned the dismissal in 2019 and remanded to permit Coda to file an amended complaint.[66] A series of pre-trial disputes followed, centering on the indefiniteness of trade secrets that Coda allegedly orally communicated to Goodyear and the risk that Coda would "'mold[]' their claims by way of subsequent supplementation of their original recollection of those two 2009 conversations."[67] The court, accordingly, ordered Coda to provide "closed-ended" interrogatory responses of the meetings (i.e., without the possibility of later supplementation).[68] The case proceeded to jury trial on 17 trade secrets in September 2022.[69]

At the close of testimony, Judge Lioi granted judgment as a matter of law ("JMOL") that five of the trade secrets were indefinite and would not be considered by the jury.[70] The jury returned a verdict for Coda, finding that seven of the twelve alleged trade secrets qualified as trade secrets and that Goodyear had misappropriated five of those seven trade secrets, and awarded Coda $2.8 million in compensatory damages and $61.2 million in punitive damages.[71] The court then granted Goodyear's renewed JMOL motion invalidating the five "misappropriated" trade secrets and setting aside the jury verdict.[72] The court concluded that four of the trade secrets were too indefinite.[73] For example, inconsistent expert testimony resulted in ambiguous language: "[T]he testimony showed that the language of the trade secret was susceptible to *too many* interpretations . . . and shed no light on *which* interpretation might be the one Coda claimed as secret."[74] Another was described only in "vague, functional terms (*i.e.*, an interface 'that can' accomplish certain ends)."[75] Two more articulated "no more than an undifferentiated list of components, which . . . cannot meet the definiteness requirement."[76] The court explained that "'a trade-secrets plaintiff must "defin[e] the information for which protection is sought with sufficient definiteness to permit a court to apply the [statutory] criteria for protection . . . and to determine the fact of an appropriation."'"[77]

The court also set aside the verdict on the fifth trade secret because it was not "secret."[78] This claimed trade secret was knowledge that Coda's prototypes had produced certain air pressures in varying configurations; for example, that a Coda pump placed in a tire tread could generate 6.5 atmospheres of pressure.[79] But simply knowing that Coda had succeeded in solving a problem was not a secret. This claimed trade secret was "merely a bald declaration that Coda developed such a tire that is 'functional'" and "reveals no secret at all."[80]

Damages

SEVENTH CIRCUIT AFFIRMS $140M PUNITIVE DAMAGES AWARD

***Epic Systems Corp. v. Tata Consultancy Services Ltd.*, No. 22-2420, 2023 WL 4542011 (7th Cir. July 14, 2023)**

Epic Systems Corp. ("Epic") and Tata Consultancy Services Ltd. ("Tata") are competitors that provide electronic, health-related software.[81] A jury awarded Epic $240 million in compensatory damages and $700 million in punitive damages after finding that Tata unlawfully downloaded thousands of documents from Epic's confidential customer portal that contained Epic's trade secrets.[82] Armed with Epic's trade secrets, Tata convinced one of Epic's largest customers to switch to Tata.[83] The district court struck $100 million in compensatory damages from the verdict, reducing it to $140 million, and also reduced the punitive damages award to $280 million to comply with Wisconsin's damages cap.[84]

The Seventh Circuit reversed the punitive damages award.[85] Applying the Supreme Court's test from *BMW of N. Am., Inc., v. Gore*—which requires courts to consider three factors, (1) degree of the defendant's reprehensibility, (2) ratio between the harm suffered and punitive damages award and (3) how the award authorized by the jury compared to the penalties imposed in comparable cases—the Seventh Circuit determined that $140 million was the "maximum constitutionally permissible" punitive damages award, and remanded the case to allow the District Court to reassess.[86] On remand, the district court reduced the punitive damages award to $140 million.[87] Tata appealed.

The Seventh Circuit affirmed the revised $140 million award, finding no fault with the district court's analysis on remand.[88] The Seventh Circuit explained that the district court appropriately analyzed reprehensibility, noting that Tata's employees "deliberately and repeatedly accessed and downloaded confidential information that Epic had spent years developing and then used that information to attempt to compete with Epic."[89] The Seventh Circuit then agreed with the district court's analysis of the ratio of the harm to the punitive damages award, citing the "massive gain" Tata would have experienced but for being caught.[90] Finally, the Seventh Circuit rejected Tata's comparators under the third *Gore* factor, explaining that Tata is one of the largest companies in the world, and "only a significant punishment would have a deterrent effect."[91]

SECOND CIRCUIT OVERTURNS $284 MILLION UNJUST ENRICHMENT JURY VERDICT

***Syntel Sterling Best Shores Mauritius Limited v. TriZetto Group*, 68 F.4th 792 (2d Cir. 2023).**

The TriZetto Group ("TriZetto") develops healthcare administration software, including Facets, a widely used platform.[92] In 2010, TriZetto subcontracted with Syntel Sterling Best Shores Mauritius Limited ("Syntel") to provide Facets support services to clients on behalf of, rather than in competition with, TriZetto.[93] In 2014, after a TriZetto competitor acquired Syntel, Syntel terminated its service agreement with TriZetto while requesting payment of rebates owed under the contract.[94] TriZetto refused to pay.[95] Syntel then sued TriZetto for breach of contract and other claims.[96] TriZetto counterclaimed for misappropriation of trade secrets related to the Facets software under the DTSA and New York law.[97]

At trial, Syntel did not contest that it downloaded and used the information claimed as trade secrets, arguing instead that their use was within the scope of the service agreement.[98] The jury was instructed to consider three damages theories if it found that Syntel misappropriated TriZetto's trade secrets: (1) TriZetto's lost profits of $8.5 million; (2) Syntel's avoided costs as unjust enrichment, the amount Syntel would have needed to spend to legitimately produce the software it misappropriated; and (3) the amount of a reasonable royalty.[99] The jury found for TriZetto on all counts and awarded both avoided costs and a reasonable royalty under state law.[100] The total compensatory damages award was $284 million with $567 million added in punitive damages.[101] The district court also issued a permanent injunction enjoining Syntel from using any of the asserted trade secrets.[102]

Seizure Orders and Injunctions

THIRD CIRCUIT DECIDES EX PARTE SEIZURE ORDERS UNDER THE DFTA ARE NOT IMMEDIATELY APPEALABLE

Janssen Prod., L.P. v. eVenus Pharms. Lab's Inc., 85 F.4th 147 (3d Cir. 2023)

Janssen Products, L.O. and Pharma Mar, S.A. (together, "Janssen") are pharmaceutical companies that developed an injectable version of the cancer drug trabectedin.[103] They documented how to produce the drug for treatment on a commercial scale and patented some of the processes.[104] They also kept their data, specifications and methods for manufacturing the drug confidential, and they consider that information trade secrets.[105] The final product they developed is sold as Yondelis®.[106] Two years after the U.S. Food and Drug Administration ("FDA") approved it for use in certain cancer patients, two competitors sought FDA approval to sell a generic version of Yondelis®.[107] Janssen sued those competitors for patent infringement.[108]

During discovery in the patent case, Janssen obtained documents that led them to believe the competitors misappropriated their trade secrets.[109] Accordingly, Janssen filed a separate lawsuit under the Defend Trade Secrets Act ("DTSA") and state law.[110] Through discovery, Janssen became convinced that the competitors had spoliated evidence and filed an ex parte seizure application under the DTSA, which provides that "the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[111] The district court denied the ex parte seizure application, and Janssen timely appealed.[112]

On appeal, the Third Circuit questioned whether it had jurisdiction to hear the appeal.[113] Generally, federal courts of appeals only have jurisdiction to review final decisions of the district courts.[114] However, Congress has created limited exceptions to this rule.[115] First, the Third Circuit analyzed whether DTSA ex parte seizure denials were "effectively injunctive" under a statute providing appellate jurisdiction to review certain non-final orders related to injunctions.[116] Then, the Third Circuit analyzed whether Congress intended DTSA ex parte seizure rulings to be immediately appealable, comparing the DTSA's language concerning ex parte seizure orders to that of the Lanham Act.

Federal courts of appeals have jurisdiction to review non-final orders "granting, continuing, modifying, refusing, or dissolving injunctions, or refusing to dissolve or modify injunctions."[117] Even orders that do not explicitly grant or deny injunctions are immediately appealable if they are “effectively injunctive.”[118] In analyzing whether an ex parte seizure order is “effectively injunctive,” the court applied a three-prong test that asks whether the order (1) is directed to a party, (2) may be enforced by contempt and (3) is designed to accord or protect some or all of the substantive relief sought by a complaint in more than a temporary fashion.[119] Ultimately, the court determined that “no DTSA seizure order can satisfy the first or the second prong”.[120] First, the DTSA requires law enforcement officials to execute any ex parte seizure order and, thus, an ex parte seizure order is not directed to a party.[121] Second, a party cannot be held in contempt for failing to comply with an order that does not direct it to do, or refrain from doing, anything.[122] Therefore, the district court’s order did not effectively deny an injunction.[123]

In comparing the DTSA and the Lanham Act, the court explained that, in analyzing the language and legislative history of the Lanham Act in a prior decision, it concluded Congress viewed the seizure orders described in that act as injunctive relief.[124] Additionally, the court stated that denial of an ex parte seizure application under the Lanham Act functions like an order denying a preliminary injunction because the order is a final resolution of the application.[125] Finally, the court explained that the denial of a Lanham Act seizure application worked a serious, perhaps irreparable consequence, and could be effectually challenged only by immediate appeal.[126] In contrast, the court determined that Congress had not provided a link between the DTSA’s civil seizure provisions and its injunction provisions and, in fact, had distinguished between an ex parte seizure order and injunctions in the DTSA.[127] Lacking a clear indication that Congress intended DTSA ex parte seizure rulings to be immediately appealable, the Third Circuit held it lacked jurisdiction and dismissed Janssen’s appeal.

COURT GRANTS PRELIMINARY INJUNCTION AGAINST FORMER COLLABORATOR FROM USING OR DISCLOSING ITS TECHNICAL “KNOW-HOW”

***SolarPark Korea Co., Ltd. v. Solaria Corp.*, No. 23-cv-01181-AMO, 2023 WL 4983159 (N.D. Cal. Aug. 2, 2023)**

SolarPark Korea Co., Ltd. (“SolarPark”) manufactures solar modules.[128] Defendant Solaria Corporation (“Solaria”) manufactures photovoltaic productions, some of which use a unique “shingling” technology whereby solar cells are cut and overlap with each other to form shingles.[129] Starting in 2016, the two companies worked together.[130] At first, Solaria supplied solar cells to SolarPark, but over time SolarPark sometimes manufactured Solaria products and therefore learned the “unique know-how to mass produce shingled solar modules.”[131] The parties entered into a cross license under which each party licensed the intellectual property of the other.[132] Later, SolarPark had financial troubles and shut down its manufacturing facilities.[133]

Solaria then merged with Complete Solar Holding Company to form a new entity, Complete Solaria.[134] In the S-4 Registration Statement filed with the U.S. Securities and Exchange Commission as part of the merger, Solaria disclosed that it had obtained new manufacturers to produce its products and represented that SolarPark had permanently ceased production and filed for bankruptcy.[135] SolarPark then sued Complete Solaria, including seeking a preliminary injunction restraining Solaria and Complete Solaria from using its trade secrets or producing Solaria's brand of shingled modules.[136]

The district court applied the factors from *Winter v. Natural Res. Def. Council, Inc.* to determine whether SolarPark was entitled to a preliminary injunction: (1) likelihood of success on the merits, (2) likelihood of irreparable harm absent preliminary relief, (3) the balance of equities and (4) the public's interest. [137]

In considering the likelihood of success on the merits, the court focused on whether SolarPark had sufficiently alleged the existence of a trade secret under California law.[138] SolarPark defined its trade secrets as the "know-how" related to "mass-producing low-cost, high-quality shingled solar modules."[139] The court agreed that the "know-how" was sufficiently specific to constitute a trade secret and cited the confidentiality agreements between the parties and the fact that the "know-how" was not generally known in the industry.[140] Finding that without an injunction SolarPark would likely suffer a loss of market position, loss of customers and increased risk that its trade secrets would be exposed to third parties, the court also found a likelihood of irreparable harm.[141]

The court concluded that SolarPark was entitled to preliminary relief, and preliminarily enjoined Solaria and Complete Solaria from: "Any and all use, disclosure, providing third parties access to, transferring, copying, duplication, reproduction, publication, distribution, broadcasting or marketing of any version of SolarPark's trade secrets as defined in SolarPark's Identification of Trade Secrets pursuant to California Code of Civil Procedure Section 2019.210."[142] However, the court found that SolarPark's other requests – viz, that the court enjoin Solaria from manufacturing or selling any other brand of shingled solar modules except for those produced by SolarPark and from any and all solicitation, negotiation or agreement with solar module manufacturers using shingling technology -- "reached beyond the protection of its trade secrets."[143]

COURT DENIED TRO AGAINST EX-EMPLOYEES FOR TAKING CUSTOMER LISTS

***Dental Health Services v. Miller*, No. 23-cv-00383 (W.D. Wash. Apr. 6, 2023)**

Longtime employees Miller and Nace left Dental Health Services (DHS), a health care service plan provider, and began working for DHS's competitors.[144] DHS sued both individuals and fifty unidentified "Doe" defendants under the DTSA and Washington trade secret law.[145] DHS sought a temporary restraining order (TRO) to enjoin Nace and the Doe defendants from using DHS's confidential and trade secret information.[146] Plaintiffs also sought expedited discovery from Nace and Miller.[147]

The court considered the likelihood of DHS's success on the merits.[148] The inquiry focused on whether the customer identities allegedly taken by the defendants qualify as trade secrets.[149] DHS defined its trade secrets as "customer lists, customer contact information, pricing, bid strategies, and insurance product plans."[150] However, those are only "vague and general categories of information" that did not identify specific trade secrets.[151] The court also considered two specific elements allegedly taken by the defendants: (1) knowledge that the City of Seattle and a California trade union were DHS clients and (2) knowledge of specific requirements imposed on DHS by regulators.[152] However, because these customer identities and regulatory orders were available in the public domain, they could not constitute trade secrets.[153] The court concluded that "DHS's failure to provide sufficient details regarding its alleged trade secrets and confidential information dooms its motion for a TRO."[154]

The court also denied DHS's motion for expedited discovery, finding that DHS failed to show that disclosure of confidential information would lead to irreparable harm, giving little weight to a contractual provision that purported to stipulate that "disclosure of Confidential Information would cause irreparable harm."[155] The court also concluded that the threat of irreparable harm had been mitigated when the plaintiffs "addressed and improved" the problems that had prompted regulatory action, thus "diffusing the sting" of any disclosure of DHS's past troubles by Nace.[156]

BUILDING SUPPLY DISTRIBUTOR WINS PARTIAL PRELIMINARY INJUNCTION AGAINST RIVAL'S USE OF VENDOR DISCOUNT INFORMATION

Foundation Building Materials, LLC v. Conking & Calabrese, Co., 2023-NCBC-46, 2023 WL 4561583 (N.C. Super. Ct. 2023)

Conking & Calabrese Co. ("Conking"), a regional distributor of building materials, expanded into North Carolina in early 2023.[157] Foundation Building Materials ("FBM") is a national supplier and distributor of building materials with an existing branch in Charlotte, NC.[158] Conking first recruited the branch manager from FBM to run its new Charlotte office[159] and then seventeen other FBM employees.[160] On their way out of FBM, different employees emailed to Conking a list of 2,930 Outlook contacts, a price sheet from an FBM vendor, personnel files and other information related to a specific customer that was redacted from the public opinion.[161]

FBM sued Conking and several individual defendants in North Carolina court.[162] FBM won motions for a TRO and for expedited discovery.[163] FBM also moved for a preliminary injunction.[164]

North Carolina courts examine six factors to determine whether contested information qualifies as a trade secret:

> (1) the extent to which the information is known outside the business; (2) the extent to which it is known to employees and others involved in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of information to business and its competitors; (5) the amount of effort or money expended in developing the information; and (6) the ease or difficulty with which the information could properly be acquired or duplicated by others.[165]

A plaintiff must also show that a defendant (1) knew or should have known of the trade secret, and (2) acquired, disclosed or used it, or had a specific opportunity to do so, without consent.[166] To win a preliminary injunction, a plaintiff must show a likelihood of success on the merits and that it is likely to suffer irreparable loss without an injunction.[167]

FBM asserted seven categories of trade secrets, and the court granted preliminary injunctions on two. The court found that FBM's vendor pricing information was a trade secret, "[b]ecause the information has competitive value," "[n]either FBM nor its vendors share this information with others" and "[i]nternally, FBM takes steps to secure the information and permits only a few employees to access it."[168] There was also direct evidence that one ex-FBM employee emailed the price sheet to Conking. The court found that these facts support a likelihood of success as well as irreparable harm.[169] The court made similar findings for the specific customer information redacted from the public record.[170]

On the personnel file category, the court also found a likelihood of success on the merits, but not irreparable harm.[171] One employee mailed to Conking the personnel files containing compensation information for drivers from FBM, which were valuable for recruiting those drivers away from FBM.[172] But all of the drivers whose files were taken had already left FBM.[173] With the horse bolted, closing the barn doors would not undo any irreparable harm.

On the remaining categories, the court did not find likelihood of success on the merits. The contact information in the Outlook lists was available in the public domain, and "the record contains no evidence that compiling the contacts took great effort."[174] Several other categories of trade secrets—customer credit information and market product utilization rates—bore no evidence that any ex-employee transmitted that data to Conking.[175] The court reasoned that the ability to access a trade secret, without more, is not enough to show misappropriation, explaining that "North Carolina courts are reluctant to grant injunctive relief solely on the basis of *threatened* misappropriation without proof of *actual* misappropriation."[176]

CONCLUSIONS

This White Paper highlights recent noteworthy trade secret cases. In these cases, courts have provided insight into several key trade secret issues, including:

- The importance of defining trade secrets in clear and definite terms;
- When customer lists and knowledge of unfavorable regulatory action may constitute trade secrets;
- When compilations of data from publicly available sources can constitute trade secrets;
- When trade secrets are too vague and inconclusive to survive summary judgment;
- The circumstances in which a covenant not to sue might moot an action seeking a declaratory judgment that a trade secret was not misappropriated;
- Maximum punitive damages awards for trade secrets misappropriation;
- The requisite direct and circumstantial evidence of trade secret misappropriation to support a preliminary injunction;

- Whether unjust enrichment damages are permitted by the DTSA when actual damages alone would make a trade secret plaintiff whole; and
- When the knowledge element of misappropriation may be plausibly alleged on the basis of "information and belief" at the pleading stage.

Readers are encouraged to contact Kelsey I. Nix, Co-Chair of Smith Anderson's Intellectual Property Litigation practice, with questions or for more information regarding trade secrets or intellectual property litigation

---

DISCLAIMER: Because of the generality of this paper, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

END NOTES

1 *Ahern Rentals, Inc. v. EquipmentShare.com, Inc.*, 59 F.4th 948, 951 (8th Cir. 2023).
2 *Id.*
3 *Id.*
4 *Id.*
5 *Id.*
6 *Id.*
7 *Id.*
8 *Id.*
9 *Id.* at 952.
10 *Id.*
11 *Id.* at 953 (internal citations and quotations omitted). *Iqbal* and *Twombly* refer respectively to *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).
12 *Ahern Rentals, Inc*, 59 F.4th at 953.
13 *Id.* at 954 (emphasis added).
14 *Id.* at 955–56.
15 *Id.* at 956.
16 *Id.*
17 *Id.* at 958.
18 *Allstate Insurance Co. v. Fougere*, 79 F.4th 172, 177, 179 (1st Cir. 2023).
19 *Id.* at 179.
20 *Id.* at 180.
21 *Id.*
22 *Id.*
23 *Id.* at 180–81.
24 *Id.* at 181.
25 *Id.*
26 *Id.* at 189–93.
27 *Id.* at 189.
28 *Id.* (emphasis added)
29 *Id.* at 191.
30 *Id.* at 192–93.
31 *Id.* at 194.
32 *Id.* at 195–96.
33 *Id.* at 196.
34 *Card Isle Corp. v. Farid*, -- F. Supp.3d --, 2023 WL 5618246 at *1 (N.D. Ga. 2023).

[35] *Id.* at *2–3.
[36] *Id.* at *4.
[37] *Id.* at *4–5.
[38] *Id.* at *5.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.* at *6.
[43] *Id.*
[44] *Id.* at *7.
[45] *Id.*
[46] *Id.* at *8.
[47] *Id.*
[48] *Synopsys, Inc. v. Risk Based Sec., Inc.*, 70 F.4th 759, 762 (4th Cir. 2023).
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.* at 763.
[53] *Id.*
[54] *Id.* at 765.
[55] *Id.* (quoting *Synopsys, Inc. v. Risk Based Sec., Inc.*, 2022 WL 107184, at *1 (E.D. Va. Jan. 11, 2022)).
[56] 568 U.S. 85 (2013).
[57] *Synopsys*, 70 F.4th at 765 (quoting *Already*, 568 U.S. at 91) (emphasis omitted).
[58] *Id.* at 766.
[59] *Id.* (internal citations and quotations omitted).
[60] *Id.*
[61] *Id.* at 775.
[62] *Id.* at 774.
[63] *Id.*
[64] *Coda Dev., s.r.o. v. Goodyear Tire & Rubber Co.*, 916 F.3d 1350, 1353–54 (Fed. Cir. 2019).
[65] *Id.*
[66] *Id.* at 1361–62.
[67] *Coda Dev., s.r.o. v. Goodyear Tire & Rubber Co.*, No. 15-cv-1572, slip op. at 3 (N.D. Ohio Mar. 31, 2023), Dkt. No. 393 (order granting defendants' renewed Rule 50 motion).
[68] *Id.* at 3.
[69] *Id.* at 8.
[70] *Id.* at 8–9.
[71] *Id.* at 9.
[72] *Id.* at 29–30.
[73] *Id.* at 14–25.
[74] *Id.* at 17.
[75] *Id.* at 18.
[76] *Id.* at 20.
[77] *Id.* at 11–12 (internal citation omitted).
[78] *Id.* at 26–27.
[79] *Id.* at 25.
[80] *Id.* at 27.
[81] *Epic Systems Corp. v. Tata Consultancy Services Ltd.*, No. 22-2420, 2023 WL 4542011 at *1 (7th Cir. July 14, 2023).
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.* (citing *BMW of N. Am v. Gore*, 517 U.S. 559 (1996)).
[87] *Id.* at *2.
[88] *Id.* at *3.
[89] *Id.* at *2.
[90] *Id.* at *3.
[91] *Id.*
[92] *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Grp.*, 68 F.4th 792, 796 (2d Cir. 2023).

[93] *Id.* at 797.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.* at 798.
[99] *Id.*
[100] *Id.* at 799.
[101] *Id.*
[102] *Id.*
[103] *Janssen Prod., L.P. v. eVenus Pharms. Lab'ys Inc.*, 85 F.4th 147, 149 (3d Cir. 2023).
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.* at 150.
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.* at 150–51
[117] *Id.* at 150 (quoting 28 U.S.C. § 1292(a)(1)).
[118] *Id.*
[119] *Id.* at 150–51.
[120] *Id.* at 151.
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.* at 151–52.
[126] *Id.* at 151 n.2, 152.
[127] *Id.* at 152.
[128] *SolarPark Korea Co., Ltd. v. Solaria Corp.*, No. 23-cv-01181-AMO, 2023 WL 4983159 at *1 (N.D. Cal. August 2, 2023).
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.* at *2.
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.* at *3 (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008)).
[138] *Id.*
[139] *Id.* at *4.
[140] *Id.* at *4–5.
[141] *Id.* at *8.
[142] *Id.* at *10.
[143] *Id.*
[144] *Dental Health Servs. v. Miller*, No. 23-cv-00383, slip op. at 2–3 (W.D. Wash. Apr. 6, 2023), Dkt. No. 37 (order denying motion for a temporary restraining order and for expedited discovery).
[145] *Id.* at 4.
[146] *Id.* at 1.
[147] *Id.* at 2.
[148] *Id.* at 12.
[149] *Id.* at 10.
[150] *Id.*

[151] *Id.*
[152] *Id.* at 10–11.
[153] *Id.*
[154] *Id.* at 7.
[155] *Id.* at 13.
[156] *Id.* at 14.
[157] *Found. Bldg. Materials, LLC v. Conking & Calabrese, Co.*, 2023-NCBC-46, ¶¶ 15–16 (N.C. Super. Ct. 2023).
[158] *Id.* ¶¶ 10, 13.
[159] *Id.* ¶¶ 13, 18–19.
[160] *Id.* ¶ 20.
[161] *Id.* ¶¶ 31–32, 41, 45, 56.
[162] *Id.* ¶ 3.
[163] *Id.* ¶¶ 4–6.
[164] *Id.* ¶ 4.
[165] *Id.* ¶ 66.
[166] *Id.* ¶ 68.
[167] *Id.* ¶ 58.
[168] *Id.* ¶ 81.
[169] *Id.* ¶¶ 82, 94.
[170] *Id.* ¶¶ 83–84, 94.
[171] *Id.* ¶¶ 92, 94.
[172] *Id.* ¶ 92.
[173] *Id.* ¶ 94.
[174] *Id.* ¶ 72.
[175] *Id.* ¶¶ 76, 88.
[176] *Id.* ¶ 78 (emphasis added).