

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

NETAPP INC.,

Plaintiff,

v.

Case No: 6:25-cv-2130-JSS-DCI

JON THORGRIMUR STEFANSSON,

Defendant.

ORDER

Plaintiff, NetApp Inc. (NetApp), sues Defendant, Jon Thorgrimur Stefansson, under the Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1836, and the Florida Uniform Trade Secrets Act (FUTSA), Fla. Stat. §§ 688.001–009, alleging that Stefansson misappropriated NetApp’s confidential and proprietary information, including core trade secrets. (Dkt. 1.) To prevent Stefansson’s alleged misuse of its information, NetApp moves for entry of an ex parte temporary restraining order (TRO). (Dkt. 3.) Upon consideration, for the reasons outlined below, the court grants the motion.

BACKGROUND

NetApp filed its complaint on November 6, 2025. (Dkt. 1.) NetApp alleges that Stefansson, a former senior executive, breached his Proprietary Information, Inventions, and Non-Solicitation Agreement (contract) and is currently

misappropriating NetApp's trade secrets in violation of the DTSA and FUTSA. (*Id.* ¶¶ 1, 4, 44–113.)

NetApp is “a leading provider of high-performance data management and cloud services.” (Dkt. 1 ¶ 4; *see* Dkt. 3-2 ¶¶ 3–8.) It has “invested years of engineering effort and substantial resources to . . . address[] one of the most complex challenges in modern IT: managing the ever-growing volume[] of data dispersed across multiple locations, both on-premises and in the cloud.” (*Id.* ¶ 23; *see* Dkt. 3-2 ¶ 9.) NetApp's investments ultimately paid off, resulting in the creation of its service delivery engine, which allows users “to manage and operate all elements of the[ir] data estate, including storage capacity, movement, protection, and analysis of [their] ever-expanding and increasingly dispersed data, from the hyperscaler's native interface.” (*Id.* ¶ 23; *see* Dkt. 3-2 ¶¶ 9–10.)

According to the complaint, Stefansson spent eight years working for NetApp. (Dkt. 1 ¶ 4; *see* Dkt. 3-3 ¶ 3.) In that time, Stefansson “played a central part” in developing NetApp's “advanced service delivery engines for cloud data management technologies, including its cloud control plane” and “was directly involved in the development and integration of NetApp's first-party, cloud-native storage products with the major hyperscalers.” (*Id.* ¶ 24; *see* Dkt. 3-3 ¶ 5.) As a result, Stefansson had “wide[-]ranging access to NetApp's most confidential information, proprietary innovations, intellectual property, and business relationships, including exclusive insight into [it]'s relationships and agreements with its hyperscaler business partners.” (*Id.* ¶ 4; *see* Dkt. 3-3 ¶¶ 6–9.)

As a condition of his employment, Stefansson signed a contract, in which he agreed to act in NetApp's best interest, not to engage in conflicting business ventures without NetApp's consent, and not to solicit its business partners or employees for at least a year following his employment. (Dkt. 1-2 at 8–9.) Stefansson also agreed not to disclose or improperly use NetApp's confidential and proprietary information, to assign NetApp any inventions conceived during his employment, and to notify NetApp of any inventions that he conceived in the six months that followed. (Dkt. 1 at ¶ 5; *see* Dkt. 1-2 at 3, 5–6.)

Stefansson “formally separated from NetApp on June 27, 2025.” (*Id.* ¶ 36.) Within a week, he incorporated Red Stapler. (*Id.*) Two months later, NetApp's direct competitor acquired Red Stapler. (*Id.*) According to the competitor's press release, it acquired Red Stapler because the company had developed “a cloud control plane and delivery platform.” (*Id.* ¶ 38.) The competitor also named Stefansson as its new General Manager of Cloud Solutions, in the hopes that he could accelerate its Hyperscale Cloud expansion. (*Id.*) NetApp does not believe that Red Stapler developed its own cloud control plane and delivery platform in under ten weeks. (*See id.* ¶ 9.) Instead, NetApp contends that Red Stapler's products are those which it “spent years and tens of millions of dollars developing.” (*Id.*)

Several recent discoveries have led NetApp to the conclusion that Stefansson used his access to its confidential and proprietary information to develop “a competing cloud control plane and service delivery platform” while still in NetApp's employment. (*Id.* ¶¶ 1, 6–10, 30–33.) First, NetApp has uncovered text messages from

a former employee—who now sits on the board of directors for its competitor—stating that Stefansson had agreed to join the company in January. (*See id.* ¶ 7; *see also* Dkt. 3-5.) Second, NetApp has also discovered messages in which Stefansson allegedly discussed poaching other employees several months before he departed from NetApp. (*Id.*; Dkt. 3-6.) Third, NetApp has uncovered a shared account on GitHub—a platform “that allows groups of users to collaborate on projects, manage memberships, and control access to coding repositories”—named “redstapler-is,” (*id.* ¶¶ 7, 13; *see* Dkt. 3-7), thus “indicat[ing] that design and software development was underway during the period in which Stefansson remained employed by NetApp,” (Dkt. 3 at 10).

Considered together, NetApp contends that the compressed timeline surrounding Stefansson’s departure and Red Stapler’s incorporation, product development, and sale shows that Stefansson “was developing technology and/or source code and innovating on behalf of another entity” while he was still employed by NetApp. (Dkt. 1 ¶ 13; *accord* Dkt. 3 at 9 (“Stefansson secretly set about building a copycat product and new company—Red Stapler—while still employed by NetApp.”). NetApp, therefore, contends that it owns Red Stapler’s inventions under Stefansson’s contract. (*Id.* ¶¶ 5, 13; *see* Dkt. 1-2 at 5–6.) Thus, Stefansson “did not have the title or right to sell that intellectual property.” (*Id.* ¶ 13.) Because Red Stapler’s intellectual property is now in the hands of one its competitors, NetApp contends that “there is a real and immediate threat” that Stefansson will leverage NetApp’s trade secrets to empower its competitor to “fast-track [the] development of a competing product” and thereby interfere with NetApp’s “ongoing relationships

with its hyperscaler Business Partners.” (*See* Dkt. 1 at ¶¶ 49, 82, 107; Dkt. 3-2 ¶ 12 (“Were a competitor to gain access to these trade secrets, the competitor would gain an unfair competitive advantage over NetApp because it could pursue the same business opportunities at a lower cost, given that the competitor did not have to invest in the development of the trade secrets.”).)

APPLICABLE STANDARDS

Federal Rule of Civil Procedure 65 governs TROs and preliminary injunctions. *See* Fed. R. Civ. P. 65. The key difference is that while TROs may issue without notice to the adverse party, *see* Fed. R. Civ. P. 65(b)(1), “[t]he court may issue a preliminary injunction only on notice to the adverse party,” Fed. R. Civ. P. 65(a)(1). “Every order granting an injunction and every [TRO] must . . . state the reasons why it issued[,] . . . state its terms specifically[,] and . . . describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required.” Fed. R. Civ. P. 65(d)(1). Rule 65 also states: “The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” Fed. R. Civ. P. 65(c); *accord* M.D. Fla. R. 6.01(a)(4) (requiring a TRO motion to “include . . . a precise and verified explanation of the amount and form of the required security”); M.D. Fla. R. 6.02(a)(1) (requiring the same of a preliminary injunction motion).

“A TRO or preliminary injunction is appropriate where the movant” satisfies four requirements: (1) “there is a substantial likelihood of success on the merits,” (2) “the TRO or preliminary injunction is necessary to prevent irreparable injury,” (3) “the threatened injury outweighs the harm that the TRO or preliminary injunction would cause to the non-movant,” and (4) “the TRO or preliminary injunction would not be averse to the public interest.” *Parker v. State Bd. of Pardons & Paroles*, 275 F.3d 1032, 1034 (11th Cir. 2001); *accord* M.D. Fla. R. 6.01(b), 6.02(a)(1). Preliminary injunctive relief “is an extraordinary and drastic remedy not to be granted unless the movant clearly establishes the burden of persuasion as to each of the four prerequisites.” *Wall v. Ctrs. for Disease Control & Prevention*, 543 F. Supp. 3d 1290, 1292 (M.D. Fla. 2021) (alteration adopted and quotations omitted).

ANALYSIS

There are four prerequisites for obtaining a temporary restraining order. *See Parker*, 275 F.3d at 1034. The court will address each in turn.

A. Likelihood of Success on the Merits

The complaint asserts six causes of action. (Dkt. 1 at ¶¶ 44–113.) Although NetApp contends that there is a substantial likelihood that it will succeed on each claim, (*see* Dkt. 3 at 14–22), NetApp “need only establish a substantial likelihood of success on one claim” for now, *Sapphire Consulting Servs. LLC v. Anderson*, No. 6:20-CV-1724-CEM-LRH, 2021 WL 1053276, at *3 (M.D. Fla. Feb. 12, 2021) (“When a plaintiff asserts multiple claims as a basis for a preliminary injunction, the plaintiff

‘need only establish a substantial likelihood of success on one claim.’” (quoting *Freedom Med., Inc. v. Sewpersaud*, 469 F. Supp. 3d 1269, 1275 (M.D. Fla. 2020)). Still, the DTSA and FUTSA “authorize a court to grant an injunction to prevent ‘actual’ or ‘threatened’ misappropriation of a ‘trade secret,’” *Primo Broodstock, Inc. v. Am. Mariculture, Inc.*, No. 2:17-CV-9-FTM-29CM, 2017 WL 1502714, at *10 (M.D. Fla. Apr. 27, 2017), and may be considered together, *Freedom Med., Inc. v. Sewpersaud*, 469 F. Supp. 3d 1269, 1275 n.6 (M.D. Fla. 2020). Because NetApp has established a likelihood of success on the merits as to its DTSA and FUTSA claims, the court declines to address its contract claims at this time.

“To succeed on its DTSA and FUTSA claims, [NetApp] must prove that [Stefansson] disclosed or used a trade secret” without it’s express or implied consent and that “at the time of disclosure or use, [Stefansson] knew or had reason to know that the knowledge of the trade secret was...acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret.” *Castellano Cosm. Surgery Ctr., P.A. v. Rashae Doyle, P.A.*, No. 8:21-CV-1088-KKM-CPT, 2021 WL 3188432, at *4 (M.D. Fla. July 28, 2021); accord *Naples Cheer Acad. Inc. v. Naples Element All Stars, LLC*, No. 2:25-CV-296-JLB-KCD, 2025 WL 2852250, at *3 (M.D. Fla. Apr. 24, 2025). “Both the DTSA and the FUTSA define a trade secret as information that derives economic value from not being generally known to others, the owner of which has taken reasonable measures to keep secret.” *Id.*

The complaint contains a detailed description of facts, supported by affidavits, establishing that Stefansson has likely used NetApp’s confidential information and is

directly competing with NetApp by using its own proprietary information without NetApp's consent. According to NetApp's Vice President of Engineering, Sanjay Kumar, and its Chief Information Security Officer, Lyndall Gavin Guttersen, NetApp possesses trade secrets related to its first-party cloud storage services, hyperscaler-agnostic cloud solutions, and cloud control plane product. (*See* Dkt. 3-2 ¶ 11; Dkt. 3-4 ¶ 4.) According to Kumar and Guttersen, the value of NetApp's trade secrets and confidential information is derived from the fact that they are not generally known. (Dkt. 3-2 ¶ 12; Dkt. 3-4 ¶ 4.) Further, NetApp's Vice President of Legal, Adam Trister, explained in his declaration that Stefansson's position at the company provided him with a deep understanding of NetApp's trade secrets and confidential information. According to Trister, Stefansson was a "driving force in NetApp's first-party cloud storage business," had "broad access to NetApp's most sensitive confidential and proprietary information, including . . . the operational details of NetApp's hyperscaler relationships," and "was deeply entrenched in the development of NetApp's first native public-cloud offering and directly involved in product engineering with access to restricted technical and commercial information." (Dkt. 3-3 ¶ 7.)

As alleged in the complaint, Stefansson used his access to NetApp's confidential and proprietary information to develop "a competing cloud control plane and service delivery platform" while still in NetApp's employment. (*Id.* ¶¶ 1, 6–10, 30–33.) The complaint supports this conclusion by describing the compressed timeline in which Red Stapler allegedly developed its cloud control plane and delivery platform. (Dkt. 1 at ¶¶ 9, 38.) What NetApp spent "years and tens of millions of dollars" developing,

Red Stapler purportedly achieved in less than ten weeks. (*See id.*) This timeline is especially concerning since Stefansson was contractually obligated to assign NetApp any inventions conceived during his employment, and to notify the company of any inventions conceived in the six months that followed, so that NetApp could determine whether it owned the invention. (Dkt. 1 at ¶ 5; see Dkt. 1-2 at 3, 5–6.)

NetApp has further presented evidence that it took reasonable measures to keep information concerning its first-party cloud storage services, hyperscaler-agnostic cloud solutions, and its cloud control plane product secret. As Guttersen explains in his declaration, NetApp “has implemented a comprehensive program of technical, administrative, and contractual safeguards designed to protect the secrecy, integrity, and controlled use of its confidential information and trade secrets,” that is “consistent with industry practices.” (Dkt. 3-4 ¶ 5.) Specifically, NetApp maintains a formal, company-wide policy “govern[ing] how information is labeled and handled based on sensitivity,” restricts access to information to personnel with a business need to know, and protects its information through encryption, passwords, multi-factor authentication, and other measures. (*See id.* ¶¶ 6–13.) Courts have found similar efforts to protect trade secrets and confidential information to be reasonable. *Castellano Cosm. Surgery Ctr., P.A.*, 2021 WL 3188432, at *6 (finding that the plaintiff employed “reasonable efforts” to protect its trade secrets where it maintained the information in a password-protected database, with restricted access, and required its employees to sign confidentiality agreements); *VAS Aero Servs., LLC v. Arroyo*, 860 F. Supp. 2d 1349, 1359 (S.D. Fla. 2012) (finding that security measures, which included multi-tiered

password protections and restricted access, were not only reasonable, but “substantial”). NetApp has therefore shown that Stefansson likely misappropriated its trade secrets by using them for his own pecuniary gain—when he sold them to its competitor—in violation of the parties’ contract. Thus, NetApp has shown a substantial likelihood of success on the merits of its DTSA and FUTSA claims.

B. Irreparable Injury

“To establish irreparable harm, the movant must show that the injury is immediate and is not compensable by monetary damages.” *Lead Creation Inc. v. Partnerships & Unincorporated Associations Identified on Schedule A*, No. 8:23-CV-49-CEH-CPT, 2023 WL 1993971, at *4 (M.D. Fla. Feb. 14, 2023) (quotation omitted). Here, NetApp submits that it “will suffer imminent and irreparable injury if the [c]ourt does not enjoin Stefansson from using [its] trade secrets and soliciting [its] customers in violation of [his] contractual obligations,” because it will “los[e] the value of its trade secrets and valuable business opportunities which [it] has expended extensive time, effort, and money to identify and create.” (Dkt. 3 at 22.) “The mere threat of disclosure, destruction or dilution of a plaintiff’s trade secrets constitutes irreparable injury justifying injunctive relief.” *Specialty Chemicals & Servs., Inc. v. Chandler*, No. CIV.A.1:87CV-2338MHS, 1988 WL 618583, at *5 (N.D. Ga. Sept. 29, 1988) (alterations adopted and quotation omitted). Further, because NetApp’s hyperscale-agnostic control plane and [service delivery engine] are tailor-made for each customer, (Dkt. 3-2 ¶ 9), it submits that there is a genuine concern that Stefansson will use NetApp’s trade secrets and confidential information to poach its clients, (*see* Dkt. 3 at

22–24). This too can constitute irreparable harm. *Ferrero v. Associated Materials Inc.*, 923 F.2d 1441, 1449 (11th Cir. 1991) (“[T]he loss of customers and goodwill is an ‘irreparable’ injury.” (citing *Spiegel v. City of Houston*, 636 F.2d 997 (5th Cir., Unit A, 1981))).

NetApp has made a sufficient showing based on the facts alleged, as supported by the declarations, that disclosure of information related to its first-party cloud storage services, hyperscaler-agnostic cloud solutions, and its cloud control plane product would result in irreparable harm. As explained above, NetApp has shown that Stefansson likely misappropriated its trade secrets when he sold Red Stapler, as well as the company’s purported technology, to NetApp’s competitor. (Dkt. 1 at ¶¶ 9, 38.) As Sanjay Kumar explained in his declaration, NetApp “invested years of engineering effort and substantial resources” to develop its hyperscale-agnostic control plane and service delivery engine, and NetApp has trade secrets related to those technologies that derive value “from the fact that they are not generally known.” (Dkt. 3-2 ¶¶ 9, 11, 12.) Further, because NetApp “worked closely with its hyperscaler Business Partners to develop solutions that worked for their unique business needs,” its hyperscale-agnostic control plane and [service delivery engine] are tailor-made for its clients. (*Id.* ¶ 9.) “Were a competitor to gain access to NetApp’s trade secrets, the competitor would gain an unfair competitive advantage over NetApp, because it could pursue the same business opportunities at a lower cost, given that the competitor did not have to invest in the development of the trade secrets.” (*Id.* ¶ 12.) Accordingly, NetApp has

provided sufficient evidence to show that a temporary restraining order is necessary to prevent Stefansson from diluting the value of its trade secrets and taking its customers.

C. Balance of Harms

The balance of harms weighs in favor of granting a temporary restraining order. NetApp contends that it “faces irreparable harm to its business and customer relations, whereas Stefansson will only be enjoined from activities he has agreed not to perform.” (Dkt. 3 at 24.) Courts routinely find that the scales favor plaintiffs whose trade secrets and confidential information are at stake. *See Naples Cheer Acad. Inc.*, 2025 WL 2852250, at *5 (determining that the balance of the harms favored a plaintiff who “own[ed] the confidential and proprietary information at stake” because, absent a temporary restraining order, the defendant could continue benefitting from information that the plaintiff had developed for its business); *Grady Minor & Assocs., LLC v. Blueshore Eng’g, LLC*, No. 2:24-CV-634-JLB-KCD, 2024 WL 3361270, at *5 (M.D. Fla. July 10, 2024) (finding that the balance of harms favored a plaintiff who purportedly owned the trade secrets at issue, because, absent a restraining order, the defendant could “continue to use [the plaintiff’s] trade secrets and confidential information to take away [its] customers and benefit from information that [the plaintiff] spent hours obtaining”); *Truepenny People LLC v. Cota*, No. 3:16CV424/MCR/CJK, 2016 WL 9308534, at *2 (N.D. Fla. Oct. 18, 2016) (“[B]ecause [the plaintiff] owns the trade secrets and confidential and proprietary information is at stake, the harm to [the plaintiff] outweighs any threat of potential harm to the [the defendant] from the injunction.”). As discussed, NetApp has

sufficiently alleged that Stefansson is misappropriating NetApp's trade secrets and confidential information, which it invested substantial time and money to develop. (See Dkt. 3-2 ¶¶ 9, 11, 12.) Further, Stefansson's employment with NetApp was conditioned on his promise not to use or disclose NetApp's proprietary information, and anything relating thereto, except as necessary to perform his duties for NetApp. (Dkt. 1-2 at 3.) Accordingly, the harm to Stefansson "is minimal because the [c]ourt is simply requiring [him] to do that which he willingly promised"—i.e., not disclose NetApp's proprietary and confidential information. *Freedom Med., Inc. v. Sewpersaud*, 469 F. Supp. 3d 1269, 1279 (M.D. Fla. 2020).

D. Public Interest

"In exercising their sound discretion, courts of equity should pay particular regard for the public consequences" when providing injunctive relief. *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008). NetApp contends that the court should issue a restraining order because the public interest will be served by protecting its "investment in . . . trade secrets and [by] uphold[ing] and promot[ing] the integrity of binding contracts under Florida law." (Dkt. 3 at 25.) Courts regularly find that the public interest is served by protecting trade secrets. See *Naples Cheer Acad. Inc.*, 2025 WL 2852250, at *5 ("The Court agrees with other courts that have found that the public interest is served by protecting trade secrets" (quotation omitted)); *Q. Grady Minor & Assocs.*, 2024 WL 3361270, at *5 (finding that "the public interest is served by protecting trade secrets" (quotation omitted)); *Freedom Med., Inc.*, 469 F. Supp. 3d at

1279 (concluding that “the public interest is served by protecting trade secrets and enforcing confidentiality agreements”); *Truepenny People LLC*, 2016 WL 9308534, at *2 (granting injunctive relief because “the public interest [is served] by protecting trade secrets, consistent with federal and state law”). Accordingly, the public interest is served by restraining Stefansson.

E. Bond Requirement

Federal Rule of Civil Procedure 65(c) specifies that the court “may issue a ... temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” Fed. R. Civ. P. 65(c). Bonds are typically required, but “the amount of security . . . is a matter within the discretion of the trial court, and the court may elect to require no security at all.” *BellSouth Telecommunications, Inc. v. MCIMetro Access Transmission Servs., LLC*, 425 F.3d 964, 971 (11th Cir. 2005) (alterations adopted and quotation omitted).

NetApp asks the court not to impose a bond because “[i]t is only seeking that Stefansson be enjoined from activities he already agreed not to engage in.” (Dkt. 3 at 26.) Having considered the matter, the court will exercise its discretion not to require security at this time. That said, the issue of the bond may be revisited at any time, and one may be imposed should an application be made in the interest of justice.

Accordingly:

1. Plaintiff NetApp Inc.'s Emergency Motion for Temporary Restraining Order (Dkt. 3) is **GRANTED** and shall take effect immediately upon entry of this Order.
2. Defendant Jon Thorgrimur Stefansson is hereby **ENJOINED and RESTRAINED**, directly and indirectly, and whether alone or in concert with others, from:
 - a. Using NetApp's confidential and Proprietary Information—as those terms are defined in Stefansson's Proprietary Information, Inventions, and Non-Solicitation Agreement—including, but not limited to, any information related to NetApp's cloud control plane and service delivery engine;
 - b. Engaging in any work activities, including development or sales, that relate to any products, services, source code, software, or similar technologies that Stefansson created or developed while employed by NetApp or which Stefansson assisted in the creation or development of, in whole or in part, with any individual who was then employed by NetApp, including source code and software related to NetApp's service delivery engine and cloud control plane;
 - c. Soliciting, directly or indirectly, or in any way interfering with, any of NetApp's Business Partners, as that term is defined in Stefansson's Proprietary Information, Inventions, and Non-Solicitation Agreement;

- d. Destroying, concealing, or disposing of any documents, paper, electronic files, media (including social media), or other materials that in any way relate to, or are relevant to, the conduct, causes of action, or defenses in this lawsuit;
 - e. Altering, modifying, editing, deleting, removing, or writing over in any respect any documents, computer files (including, but not limited to, emails, hard drives, disc drives, zip drives), data, drafts, text messages, social media (including, but not limited to, posts, comments, reactions, and “likes”), other media, or other things relating in any way to NetApp.
3. This Temporary Restraining Order will expire on November 26, 2025, in accordance with Federal Rule of Civil Procedure 65(b)(2) unless, for good cause shown, this Order is extended or Stefansson consents that it should be extended for a longer period of time. However, the court may, upon demonstration of good cause by any party of interest, shorten or lift this Order.
4. NetApp need not post a bond with the Clerk of Court. However, upon a showing of good cause by any party of interest, the court may enter a further order amending the amount of NetApp’s bond requirement as a means of providing a source of funds to which Stefansson may be entitled for a wrongful injunction or restraint.
5. NetApp **SHALL** serve Stefansson with a copy of this Order. Thereafter, NetApp shall file a certificate of service advising the court that Stefansson has

been served. Once Stefansson has been served, NetApp **SHALL** file a motion to convert the temporary restraining order into a preliminary injunction.

ORDERED in Orlando, Florida, on November 12, 2025.



JULIE S. SNEED
UNITED STATES DISTRICT JUDGE

Copies furnished to:

Counsel of Record
Unrepresented Party