UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Negative, Inc.,

Plaintiff,

v.

Melissa McNamara,

Defendant.

23-cv-08503 (NRM) (JAM)

MEMORANDUM AND ORDER

NINA R. MORRISON, United States District Judge:

In this action, Plaintiff Negative, Inc., alleges that one of its former contract workers, Defendant Melissa McNamara, misappropriated confidential information from Negative, including, *inter alia*, customer lists and product designs, in order to start her own competing business. The Complaint alleges violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*, violations of the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1832, *et seq.*, misappropriation of trade secrets, conversion, unfair competition, and unjust enrichment. McNamara has moved to dismiss the Complaint pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. For the reasons stated below, McNamara's motion to dismiss is GRANTED.

BACKGROUND

The following facts are taken from Plaintiff's Complaint, ECF No. 1,[1] and are accepted as true and construed in the light most favorable to Plaintiff for purposes of this motion.

Plaintiff, Negative, Inc., is a fashion business that "sells women's underwear, loungewear, and sleepwear." Compl. at 3. In January of 2019, Negative "engaged McNamara as a freelance contract worker to provide demand planning services." *Id.* at 5. To facilitate the work McNamara was retained to perform, Negative granted McNamara access to information[2] maintained on its Google Drive and Shopify user account (a sales platform). *Id.* Negative asserts that there is some data to which McNamara was granted access, but "would have no reason at all ever to access," like the "customer database." *Id.*

On May 10, 2023, McNamara resigned and "terminated her relationship with Negative." *Id.* Negative alleges that, "[u]pon information and belief," McNamara left to create a competing company. *Id.* Negative learned, months after McNamara resigned, that she spent the week before she left the company accessing and downloading information from Negative's Google Drive and Shopify user account to

[1] Pincites refer to page numbers generated by CM/ECF, and not the document's internal pagination.

[2] Throughout its Complaint, Negative refers to certain information as a "trade secret." *See* Compl. at 5. Because whether the information McNamara accessed was (or was not) a "trade secret" is central to the parties' legal dispute, the Court will not adopt this language in outlining the Complaint. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("[T]he tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions.").

her personal devices. *Id.* at 5, 6, 8. McNamara also logged into Negative's Shopify account and "exported and downloaded Negative's entire customer database." *Id.* at 8. The customer database, Negative explains, took "considerable resources" to develop and "represents the culmination of business relationships, market knowledge, and strategic insights." *Id.* All in all, Negative alleges that McNamara took many documents which included:

> (1) [C]ustomer contact and sales information, (2) information regarding supplier relationships, (3) financial information concerning Negative's costs of goods and pricing for various lines and styles of apparel, (4) marketing strategies, (5) pricing strategies, (6) information for managing inventory, logistics, and distribution, (7) business plans, (8) tech packs for the manufacture of Negative's products . . . , and (9) non-public product designs and drawings for Negative's future products.

Id. at 1–2.

Negative also contends that McNamara "knew what she was doing was wrong." *Id.* at 6. According to Negative, this conclusion flows from the fact that she did not simply download the files from Google Drive. Rather, she "creat[ed] a duplicate of each file" and "chang[ed] the access permissions and visibility settings of the duplicate files to ensure that no one else at Negative could access or even detect their existence, . . . [then] grant[ed] authorization to her personal email account to perform the download." *Id.*

Negative refers to all this information as "confidential, proprietary, and trade secret." *Id.* at 5. But nowhere in the Complaint is there any allegation or indication that these designations had ever been communicated to McNamara (or anyone else) before her resignation. Negative does plead that none of the downloaded information

is publicly accessible, and that to access it, a person requires "an intentional sign-in with multiple authentication factors." *Id.* at 9. Additionally, some of the files to which McNamara was given access were not accessible to all Negative employees, and certain files, "when they are to be shared internally, they are shared in a for-eyes-only format without the ability to download or print." *Id.* When Negative discovered that McNamara had downloaded the files, it demanded she destroy the information and provide a "full accounting" of what she took. *Id.*

On November 15, 2023, Negative filed this action in the Eastern District of New York. Negative alleges that McNamara violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*, Compl. at 9–10, as well as the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1832, *et seq.*, Compl. at 10–12. Negative also makes several claims under New York law, including misappropriation of trade secrets, conversion, unfair competition, and unjust enrichment. *Id.* at 12–16. Negative seeks both injunctive and monetary relief. *Id.* at 17.

On December 6, 2023, Negative moved for emergency injunctive relief, asking the Court to, among other things, order McNamara to return all copies of the stolen information, refrain from possessing it, and identify the location of any copies of the information. *See generally* Motion for Order to Show Cause, ECF No. 7. Instead of opposing the motion, McNamara consented to a preliminary injunction, which ordered McNamara and those working with her to refrain from possessing, disclosing, or using any information obtained from Negative, and to return any copies of Negative information in her possession. Proposed Consent Order at 1–2, ECF No.

15-1. However, in the consent order, McNamara did not admit to any wrongdoing; nor did she concede the truth of any of Negative's factual allegations that sought to categorize the information as "confidential" or "trade secrets." *Id.* at 2.

On April 29, 2024, McNamara filed the instant motion to dismiss for failure to state a claim, pursuant to Federal Rule of Civil Procedure 12(b)(6). *See* McNamara Mot., ECF No. 23-1.

LEGAL STANDARD

McNamara seeks dismissal of all claims pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. Rule 12(b)(6) allows a party to assert that the complaint fails to state a claim upon which relief can be granted. "In considering a motion to dismiss . . . the court is to accept as true all facts alleged in the complaint" and must "draw all reasonable inferences in favor of the plaintiff." *Kassner v. 2nd Ave. Delicatessen Inc.*, 496 F.3d 229, 237 (2d Cir. 2007). However, allegations in the complaint that "are no more than conclusions[] are not entitled to the assumption of truth." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). This means that "a formulaic recitation of the elements of a cause of action will not do," *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007), nor will a complaint which simply "tenders 'naked assertions' devoid of 'further factual enhancement.'" *Iqbal*, 556 U.S. at 678 (alterations adopted) (quoting *Twombly*, 550 U.S. at 557).

DISCUSSION

I. The Computer Fraud and Abuse Act

Negative asserts that McNamara violated two provisions of the CFAA: 18 U.S.C. §1030(a)(2)(C), imposing liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer"; and (2) 18 U.S.C. § 1030(a)(4), imposing liability on anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." Compl. at 9–10.

To plead a violation of either subsection of the CFAA, Negative must plausibly allege that McNamara either accessed a protected computer "without authorization" or that her access to the computer "exceed[ed] authorized access." Negative has done neither.

The Second Circuit has held that the "without authorization" factor is met when "a user lacks permission to access the computer at all." *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015). And the Complaint does not allege that McNamara did not have access to Negative's computer systems. In fact, it specifically admits that "Negative *granted McNamara access* to certain confidential, proprietary, and trade secret information maintained on Negative's computer systems, including Negative's Google Drive (a cloud storage repository) and within Negative's Shopify user account (an online sales platform that stores, *inter alia*, Negative's sales data and customer database)." Compl. at 5 (emphasis supplied). Negative contends,

however, that its Complaint plausibly alleges McNamara's actions exceeded her *authorized* access on these computer systems. *See* Negative Opp. at 21–23, ECF No. 25. It has not.

The Supreme Court's decision in *Van Buren v. United States* controls the outcome here. 593 U.S. 374 (2021). In *Van Buren*, the Court examined a case in which a former police sergeant, Van Buren, was paid by a third party to run the license plate of a woman and tell that third party the information he obtained from the FBI-created license-plate entry. *Id.* at 379–80. Van Buren had valid credentials to access this database. *Id.* He was then charged with a violation of the CFAA "on the ground that running the license plate for [the third-party] violated the 'exceeds authorized access' clause of 18 U.S.C. § 1030(a)(2)." *Id.* Van Buren argued that the "exceeds authorized access" clause is complementary to the "without authorization clause," targeting "those who access a computer with permission, but then "'exceed" the parameters of authorized access by entering an area of the computer to which that authorization does not extend.'" *Id.* at 389–90 (alterations adopted) (quoting *Valle*, 807 F.3d at 524). The Supreme Court agreed with Van Buren, holding that his conduct was not prohibited by the CFAA. This is because an individual "'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer . . . that are off limits to him." *Van Buren*, 593 U.S. at 396. Thus, even though Van Buren "obtained information from the database for an improper purpose," he did not "exceed authorized access."

Id. The Court also referred to this interpretation as a "gates-up-or-down inquiry . . . one either can or cannot access certain areas within the system." *Id.* at 390.

Nowhere in Negative's Complaint is there any allegation that McNamara was not permitted to access the information in the Shopify or Google Drive that she allegedly downloaded — *i.e.,* that these "areas" within Negative's systems were off limits to her. In its Complaint, Negative does allege that:

> Whatever authority McNamara may have had to access Negative's computer systems, this authority was limited to particular information, and by making duplicates, changing access permissions and file visibility, and then extending access and download privileges to her personal email account, McNamara bypassed technological barriers in order to access and steal additional information and exceeded her authority.

Compl. at 7. However, besides the conclusory statements that McNamara's access was "limited to particular information" and that she "bypassed technological barriers," the complaint does not allege any facts from which a trier of fact could conclude that McNamara was actually prohibited from accessing any of the information in question, either as a technological matter or by company policy. That is, Negative nowhere contends that McNamara was not given the digital credentials to access this information while she worked at the company; nor does it contend that even if she had the login credentials to review those areas of Negative's system, she was advised that she was prohibited from doing so. Thus, even accepting as true Negative's allegation that McNamara ultimately downloaded and used that information for an improper purpose, her actions — like Van Buren's — are not covered by the CFAA.

Negative argues that this case is distinguishable from *Van Buren* because McNamara did not just *access* information and then use it improperly, as Van Buren did, but she made duplicate copies of the information and then downloaded those duplicates. Def. Opp. at 22–23. This is a distinction without difference. Negative can make the conclusory statement that McNamara "bypassed technological barriers," but nowhere in their pleadings do they indicate that McNamara *did not have access* to the information she allegedly downloaded and retained. The manner in which McNamara improperly used the information, and whether she attempted to hide the fact that she was taking it, is irrelevant as to whether her conduct is within the scope of the CFAA. The inquiry, as the *Van Buren* Court held, is whether McNamara "obtain[ed] information located in particular areas of the computer — such as files, folders, or databases — that [were] off limits to [her]." *Van Buren*, 593 U.S. at 396. Negative has not pled any facts that support even an inference that this was the case, and thus, it has failed to state a claim for relief under the CFAA.

II. The Defend Trade Secrets Act

Negative also asserts a claim of misappropriation under the Defend Trade Secrets Act, 18 U.S.C. 1832, *et seq*. *See* Compl. at 10–12. It alleges that the information McNamara obtained properly qualifies as a "trade secret," and her unauthorized use of that information to her benefit herself constitutes misappropriation and therefore violates the DTSA. *See id.*

The Defend Trade Secrets Act "provides a federal cause of action for trade-secret misappropriation involving a nexus to interstate commerce." *Turret Labs*

USA, Inc. v. CargoSprint, LLC, No. 19-cv-6793 (EK), 2021 WL 535217, at *4 (E.D.N.Y. Feb. 12, 2021) (citing 18 U.S.C. § 1836(b)), *aff'd*, 2022 WL 701161 (2d Cir. Mar. 9, 2022) (summary order). The elements required to prove a violation of the DTSA and trade secret misappropriation under New York common law are "fundamentally the same," and "[d]istrict courts often rely on cases discussing misappropriation under New York law to analyze DTSA claims." *Iacovacci v. Brevet Holdings, LLC*, 437 F. Supp. 3d 367, 380 (S.D.N.Y. 2020) (WHP) (internal quotation marks omitted). Thus, the Court looks to cases analyzing both the DTSA and New York trade secret misappropriation in determining if Negative has stated a claim for relief under the DTSA.

To succeed on a claim for the misappropriation of trade secrets under New York law, a plaintiff must allege "(1) that it possessed a trade secret, and (2) that the defendant[] used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means." *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 117 (2d Cir. 2009). The DTSA makes clear that a trade secret can involve many different types of information, so long as "the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic values, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3).

McNamara does not argue that the *type* of information she allegedly misappropriated does not "derive independent economic value . . . from not being generally known," *id.*, nor could she. It is well established that information such as customer lists, pricing strategies, and product designs satisfy this element of a "trade secret." *See, e.g., In re Dana Corp.*, 574 F.3d 129, 152 (2d Cir. 2009) ("Confidential proprietary data relating to pricing, costs, systems, and methods are protected by trade secret law."); *N. Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 44 (2d Cir. 1999) ("A customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret . . . ." (quoting *Defiance Button Mach. Co. v. C & C Metal Prods. Corp.*, 759 F.2d 1053, 1063 (2d Cir 1985))). Instead, McNamara argues that Negative has not pleaded that the company took reasonable measures to keep the information secret, and the information it claims she improperly downloaded is therefore not a "trade secret" under the DTSA. *See* McNamara Mot. at 9–13. This Court agrees.

It is true that "[t]he DTSA gives scant guidance on what constitutes 'reasonable measures' to keep information secret." *Turret Labs USA, Inc.*, 2022 WL 701161 at *2. However, "[m]ost courts in this Circuit look to contractual confidentiality agreements or physical security measures" in asking whether reasonable measures were taken. *Rodney v. United Masters*, No. 21-cv-5872 (DG) (LB), 2023 WL 2184865, at *5 (E.D.N.Y. Feb. 10, 2023) (quoting *Charles Ramsey Co. v. Fabtech-NY LLC*, No. 18-cv-0546 (LEK) (CFH), 2020 WL 352614, at *15 (N.D.N.Y. Jan. 21, 2020)). Additionally, while a "confidentiality agreement alone does not

suggest existence of a trade secret," *Universal Processing LLC v. Zhuang*, No. 17-cv-10210 (LTS), 2018 WL 4684115, at *3 (S.D.N.Y. Sept. 28, 2018), the absence of such an agreement is certainly probative as to whether a plaintiff took reasonable measures to keep the information secret. Indeed, in *Pauwels v. Deloitte LLP*, the Second Circuit found that even an "oral agreement" to keep certain information secret was "at most an informal understanding" and not a formal or binding agreement; and where the plaintiff did not plead any other "steps required of [the defendant] to ensure compliance" with its alleged expectations of confidentiality, it had failed to plead this essential element of a DTSA claim. 83 F.4th 171, 182 (2d Cir. 2023). Here, Negative has not pled *any* facts which indicate that it even communicated to McNamara that the information she accessed was meant to be secret, let alone that it had her affirm that understanding by, for example, signing a non-disclosure agreement ("NDA") or its equivalent. Nor has it alleged that there was even a general company policy communicated to contractors like McNamara that they were expected to keep confidential any information they might access during their tenure at the company.

Negative contends that the following actions it took are sufficient reasonable measures to keep its information secret: that its Google Drive and Shopify account require "an intentional sign-in with multiple authentication factors;" that the files McNamara accessed were not accessible to all Negative employees or contractors, and the access to those files is controlled on a "need-to-know" basis; that some of the files McNamara retained would be shared in a "for-eyes-only format," meaning they could

not be downloaded or printed; that when someone stops working for Negative, Negative terminates their file access; and that when Negative became aware McNamara had downloaded information, they demanded its return. Negative Opp. at 14. Again, tellingly absent is any indication that Negative actually communicated to McNamara or its other employees that any of this information was to be kept secret. If this Court were to hold that these actions constituted "reasonable measures" to keep information secret under the DTSA, the implications would be sweeping indeed; essentially, it would mean that many of the basic procedures that line employees use to log into the computer systems at their place of work every day qualify as "reasonable measures" from which their employers could later deem that information to be "trade secrets." Regardless, the fact that Negative does not plead that it ever communicated to its freelancers what information they might encounter on Negative's electronic systems should (or should not) be kept confidential cuts strongly against its position that the information McNamara accessed can be considered "trade secrets."

The Court also notes that Negative refers to McNamara as a "freelance contract worker," not an employee. Compl. at 5. Thus, while it may be "implied in every contract of employment that the employee will hold sacred any trade secrets . . . which [s]he acquires in the course of [her] employment," *N. Atl. Instruments*, 188 F.3d at 48 (quoting *L.M. Rabinowitz & Co. v. Dasher*, 82 N.Y.S.2d 431, 435 (Sup. Ct. 1948)), that principle only applies if the information acquired by the contractor is a "trade secret" in the first place.

Negative argues that some courts have held that a trade secret exists even in the absence of an NDA. *See* Negative. Opp. at 15–16. This is true. However, this Court can find no other case where so little was pleaded in the form of "reasonable measures" as here and a court still found that the disputed information qualified as a trade secret. In *B.U.S.A. Corp. v. Ecogloves, Inc.* — the case Negative relies upon for this proposition — while no NDA was in place, the court found the misappropriation of a trade secret because, among other reasons, the defendant conceded at oral argument that it owed a fiduciary duty to the plaintiff. No. 5-cv-9988 (SCR), 2006 WL 3302841, at *6 (S.D.N.Y. Jan. 31, 2006). There is no fiduciary duty pled here. And as the Second Circuit in *Pauwels* explained, "'employment relationships,' without more, 'do not create fiduciary relationships.'" *Pauwels*, 83 F.4th at 184 (quoting *Rather v. CBS Corp.*, 188 N.Y.S.2d 121, 125 (N.Y. App. Div. 2009)).

Instead, courts in this Circuit have consistently held that even simply informing an employee that information should be kept secret — which Negative has not pled here — is not a sufficient "reasonable measure" to keep information secret. *See, e.g.*, *Altman Stage Lighting, Inc. v. Smith*, No. 20-cv-2575 (NSR), 2022 WL 374590, at *5 (S.D.N.Y. Feb. 8, 2022) (dismissing DTSA suit where it was alleged that employees "working on the [prototype] were informed by Defendant to not discuss the project with anyone inside or outside the company" because "informing employees that certain information is a trade secret can be a reasonable measure, [but] this is generally not sufficient without more"); *MedQuest Ltd. v. Rosa*, No. 21-cv-5307 (PGG),

2023 WL 2575051, at *5 (S.D.N.Y. Mar. 20, 2023) (finding that simply "distribut[ing] a policy manual" saying that costumer lists were secret and limiting access to certain employees and making it "difficult for other employees not involved with [the project] to print, download, or e-mail the list" was not sufficient to plausibly allege "reasonable measures to protect the confidentiality" of the plaintiff's customer list (alterations adopted)).

Here, Negative has not shown that McNamara's actions were in violation of any agreement, formal or informal. In fact, by its own pleadings, Negative admits that it allowed a freelance contractor unfettered access to information that could not be accessed by some of its regular employees, *see* Compl. at 1, 9, without any indication that she was ever advised not to share said information, much less that she agreed not to do so. Even drawing all reasonable inferences in Negative's favor, this Court cannot conclude that the company took "reasonable measures to keep [its] information secret." 18 U.S.C. § 1839(3). Thus, Negative's DTSA claim must be dismissed as it has failed to plead that the information allegedly taken by McNamara was a trade secret.[3]

[3] Given that the DTSA claim must be dismissed on this ground, the Court declines to analyze whether the Complaint sufficiently pleads the second element of a DTSA claim — that the information was "misappropriated."

III. State Law Claims

The Complaint pleads state law claims for misappropriation of trade secrets, conversion,[4] unfair competition, and unjust enrichment. *See* Compl. at 12–16. It asserts that that the Court has supplemental jurisdiction over these claims pursuant to 28 U.S.C. § 1367 because they form part of the same case and controversy as the federal claims — the alleged violations of the CFAA and DTSA.

A district court "may decline to exercise supplemental jurisdiction over a claim . . . if the district court has dismissed all claims over which it has original jurisdiction." 28 U.S.C. § 1367(c)(3). The Supreme Court has indicated that "decisions of state law should be avoided both as a matter of comity and to promote justice between the parties," and that "if the federal claims are dismissed before trial, . . . the state claims should be dismissed as well." *United Mine Workers v. Gibbs*, 383 U.S. 715, 726 (1966); *see also Denney v. Deutsche Bank AG*, 443 F.3d 253, 266 (2d Cir. 2006) ("A district court usually should decline the exercise of supplemental jurisdiction when all federal claims have been dismissed at the pleading stage"). There is no reason to depart from this rule here. Thus, the Court will not exercise

[4] Earlier in this litigation, Negative agreed to "voluntarily dismiss its claim for common law conversion." Response to Motion for Pre-Motion Conference at 2 n.2, ECF No. 17. However, while Negative has not argued that this claim should survive, it has not taken steps to dismiss the claim. As the Court declines to exercise jurisdiction over the state law claims, it will not treat Negative's conversion claim differently than its other state law claims. It does so, however, without prejudice to McNamara's right to argue in state court that Negative should be bound by its earlier agreement to dismiss this claim.

supplemental jurisdiction over Negative's state law claims, and they are dismissed without prejudice to pursue those claims in state court.

CONCLUSION

For the reasons above, McNamara's motion to dismiss is GRANTED. Negative's CFAA and DTSA claims are dismissed with prejudice, while its state law claims are dismissed without prejudice. The Court dismisses the federal law claims with prejudice since at no time since the Court was presented with Plaintiff's motion did Negative ask this Court to consider granting it leave to amend to cure any potential pleading defects alleged by Plaintiff as an alternative to dismissing the Complaint. *See Gallop v. Cheney*, 642 F.3d 364, 369 (2d Cir. 2011) ("[N]o court can be said to have erred in failing to grant a request [to amend] that was not made."). The previously-entered preliminary injunction at ECF No. 15-1 — to which Plaintiff had earlier consented pending resolution of this motion — is hereby terminated. *See Madison Square Garden Boxing, Inc. v. Shavers*, 562 F.2d 141, 144 (2d Cir. 1977) ("With the entry of the final judgment, the life of the preliminary injunction came to an end"); *see also Venezia v. Robinson*, 16 F.3d 209, 211 (7th Cir. 1994) ("A preliminary injunction cannot survive dismissal of a complaint.").

SO ORDERED.

/s/ Nina R. Morrison
NINA R. MORRISON
United States District Judge

Dated: March 13, 2025
Brooklyn, New York