TURRET LABS USA, INC., Plaintiff-Appellant,

v.

CARGOSPRINT, LLC, JOSHUA WOLF Defendants-Appellees.

No. 21-952.

United States Court of Appeals, Second Circuit.

March 9, 2022.

Appeal from a judgment of the United States District Court for the Eastern District of New York (Komitee, *J.*).

Leslie R. Bennett (Leslie R. Bennett LLC), Melville, NY, for Plaintiff-Appellant.

R. Dale Grimes, Virginia M. Yetter, and Nicholas J. Goldin (Bass, Berry & Sims, PLC), Nashville, TN; Michael Dashefsky (Bass, Berry & Sims, PLC), Washington, D.C.; Joseph A. Matteo (Barnes & Thornburg LLP), New York, NY, for Defendants-Appellees.

Present: DEBRA ANN LIVINGSTON, Chief Judge, AMALYA L. KEARSE, EUNICE C. LEE, Circuit Judges.

SUMMARY ORDER

RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT. CITATION TO A SUMMARY ORDER FILED ON OR AFTER JANUARY 1, 2007, IS PERMITTED AND IS GOVERNED BY FEDERAL RULE OF APPELLATE PROCEDURE 32.1 AND THIS COURT'S LOCAL RULE 32.1.1. WHEN CITING A SUMMARY ORDER IN A DOCUMENT FILED WITH THIS COURT, A PARTY MUST CITE EITHER THE FEDERAL APPENDIX OR AN ELECTRONIC DATABASE (WITH THE NOTATION "SUMMARY ORDER"). A PARTY CITING A SUMMARY ORDER MUST SERVE A COPY OF IT ON ANY PARTY NOT REPRESENTED BY COUNSEL.

UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED that the judgment of the district court is AFFIRMED.

Plaintiff-Appellant Turret Labs USA, Inc. ("Turret Labs") appeals from the district court's March 22, 2021 judgment dismissing its second amended complaint ("SAC") for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). *Turret Labs USA, Inc. v. CargoSprint, LLC,* No. 19-CV-6793, 2021 WL 535217, at *1 (E.D.N.Y. Feb. 12, 2021). Turret Labs alleges that Defendants-Appellees CargoSprint, LLC and its chief executive officer, Joshua Wolf, improperly gained access to Turret Labs' software, Dock EnRoll, and reverse engineered it to create their own competing program.[1] Turret Labs claims misappropriation of a trade secret under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C § 1836(b), and common-law misappropriation of a trade secret.[2] The district court dismissed these trade secret claims, ruling that Turret Labs failed as a matter of law to plead that Dock EnRoll was a "trade secret" under the DTSA and common law because the Plaintiff-Appellant did not adequately allege that it took reasonable measures to keep its information secret from third parties. *Turret Labs,* 2021 WL 535217, at *4-6. We

assume the parties' familiarity with the underlying facts, the procedural history of the case, and the issues on appeal.

*** * ***

We review *de novo* the district court's dismissal of Turret Labs' SAC pursuant to Rule 12(b)(6). *See* *Pettaway v. Nat'l Recovery Sols., LLC*, 955 F.3d 299, 304 (2d Cir. 2020). To survive a motion to dismiss brought under Rule 12(b)(6), a complaint "must contain sufficient factual matter, accepted as true, to `state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). We are "required to accept all well-pleaded factual allegations in the complaint as true" and "construe all reasonable inferences that can be drawn from the complaint in the light most favorable to the plaintiff," but we need not credit conclusory allegations. *Lynch v. City of New York*, 952 F.3d 67, 74-75 (2d Cir. 2020) (internal quotation marks and citations omitted).

Under Section 1836 of the DTSA, the owner of a "trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." § 1836(b)(1). For "financial, business, scientific, technical, economic, or engineering information" to constitute a "trade secret," two factors must be satisfied: (A) the owner must have "taken reasonable measures to keep such information secret"; and (B) the information must "derive[] independent economic value, 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), (3)(A)-(B). Turret Labs argues that the district court erred in concluding that it failed adequately to allege that it took reasonable measures to protect Dock EnRoll's secrecy. For the following reasons, we disagree.

Turret Labs alleges that after developing Dock EnRoll, it entered into a joint venture agreement and an exclusive licensing agreement with Lufthansa Cargo Americas ("Lufthansa"), which authorized Lufthansa to manage Dock EnRoll and grant access to other users. SAC ¶ 21(f) ("User Access for Dock EnRoll is managed by Lufthansa only[] and no other party has access without Lufthansa's authority"); SAC ¶ 21(j) (pleading that Turret Labs "assign[ed] to Lufthansa the right to vet users and grant access"). The SAC alleges that Defendants-Appellees gained unfettered access to Dock EnRoll by falsely presenting themselves as freight forwarders to Lufthansa.[3] It is not clear from the SAC, however, whether such unfettered access was granted by Lufthansa, or if Defendants-Appellees used other wrongful means to expand their access after initially receiving login information.[4] Turret Labs pleads, without explanation, that Defendants-Appellees were "given unfettered access to all corners of the Dock EnRoll platform that, based on Lufthansa's protocols, no freight forwarder or other user would have been granted access to, and it was only due to Defendants' wrongful actions that they were able to obtain such greater access to the platform."[5] SAC ¶ 31. Such "expansive unauthorized access to [Dock EnRoll] and confidential information contained therein allowed [Defendants-Appellees] to reverse engineer the software," SAC ¶ 34, and create a program that is "identical to Dock EnRoll, particularly the scheduling system," SAC ¶ 35.

The DTSA gives scant guidance on what constitutes "reasonable measures" to keep information secret. But given that trade secrets may appear in a wide variety of "forms and types," § 1839(3), "[w]hat measures are `reasonable' must depend in significant part on the nature of the trade secret at issue," *see* *Exec. Trim Constr., Inc. v. Gross*, 525 F. Supp. 3d 357, 380 (N.D.N.Y. 2021). We agree with the district court that where an alleged trade secret consists "primarily, if not entirely," of a computer software's functionality

—"functionality that is made apparent to all users of the program"—the reasonableness analysis will often focus on who is given access, and on the importance of confidentiality and nondisclosure agreements to maintaining secrecy. *Turret Labs,* 2021 WL 535217, at *4; *see also Mason v. Amtrust Fin. Servs., Inc.,* 848 F. App'x 447, 450 (2d Cir. 2021) (holding that plaintiff's failure to "execut[e] a nondisclosure or licensing agreement or . . . stipulate[e] in his employment contract that the [software] was his proprietary information" evidenced that he "had not taken reasonable measures to protect his information"); *Inv. Sci., LLC v. Oath Holdings Inc.,* No. 20 Civ. 8159, 2021 WL 3541152, at *3 (S.D.N.Y. Aug. 11, 2021) (concluding that the plaintiff did not employ reasonable measures to protect its claimed trade secrets because, among other reasons, the plaintiff "concede[d] that it did not require [the defendant] to sign a confidentiality agreement before sharing the contents of the [product]"); *Exec. Trim,* 525 F. Supp. 3d at 380; *Charles Ramsey Co., Inc. v. Fabtech-NY LLC,* No. 1:18-CV-0546, 2020 WL 352614, at *15 (N.D.N.Y. Jan. 21, 2020) (collecting cases); *Mintz v. Mktg. Cohorts, LLC,* No. 18-CV-4159, 2019 WL 3337896, at *6 (E.D.N.Y. July 25, 2019) (dismissing a DTSA claim because plaintiff "did not require defendants to sign a non-disclosure agreement nor any sort of covenant to protect the passwords").

This observation is consistent with those of our sister circuits. *See, e.g., Farmers Edge Inc. v. Farmobile, LLC,* 970 F.3d 1027, 1033 (8th Cir. 2020) (holding that under the DTSA, a company that, "without a confidentiality agreement and without other policies or practices for safeguarding secrets . . . shared the relevant information with a third-party who had no obligation to keep it confidential . . . did not take reasonable steps to safeguard its trade secrets"); *InteliClear, LLC v. ETC Glob. Holdings, Inc.,* 978 F.3d 653, 660 (9th Cir. 2020) (holding, under the DTSA, that the plaintiff took "reasonable measures" by "encrypt[ing] and compil[ing] its source code and requir[ing] licensees to agree to confidentiality," as "[c]onfidentiality provisions constitute reasonable steps to maintain secrecy"); *VBS Distribution, Inc. v. Nutrivita Lab'ys, Inc.,* 811 F. App'x 1005, 1009 (9th Cir.), *cert. denied,* 141 S. Ct. 454 (2020) ("Providing alleged trade secrets to third parties does not undermine a trade-secret claim, so long as the information was provided on an understanding of confidentiality." (internal quotation marks and citation omitted)).

Notably absent from Turret Labs' SAC is any specific allegation that Lufthansa or any other user of Dock EnRoll was required to keep Turret Labs' information confidential. Turret Labs does not plead that it had confidentiality or nondisclosure agreements in place with Lufthansa or other users of Dock EnRoll. Nor does it allege that Lufthansa was obligated to limit access to the software to freight forwarders that were themselves bound to respect the secrecy of Turret Labs' information. Although the SAC alleges generally that Lufthansa's internal guidelines dictated the terms of use, there is no allegation that these guidelines contractually obligated users to keep the software, its client-facing functionality, or its internal mechanics confidential. And without confidentiality or nondisclosure agreements in this context, it is not apparent from the SAC that *any* user could not simply replicate the software after using it.

Turret Labs argues that, regardless, its extensive list of security measures for Dock EnRoll, as pled in the SAC, plausibly constitutes "reasonable measures" to keep its information secret. *See* § 1839(3)(A). The SAC pleads, among other things, that Dock EnRoll's physical servers were kept in monitored cages within a data center with restricted access and that access to the software was limited to those with usernames and passwords approved by Lufthansa. SAC ¶ 21. But secured physical servers are largely irrelevant where users such as Defendants-Appellees could simply be given access by Lufthansa and view and replicate Dock EnRoll's functionality. And, again, the SAC is silent regarding any obligation on Lufthansa's part to protect proprietary information by granting access only to legitimate freight forwarders bound by confidentiality agreements. The SAC implies (but does not allege) that Defendants-Appellees hacked into the software to obtain unfettered access to Dock EnRoll's algorithms and other internal mechanics after

getting login information from Lufthansa. But Turret Labs has failed to plead how any of its security measures might have prevented such an unwanted intrusion.

In the absence of nonconclusory allegations that it took reasonable measures to keep its information secret, Turret Labs has not plausibly alleged that Defendants-Appellees misappropriated a "trade secret" under the DTSA. *See* § 1839(3)(A). Turret Labs' common-law misappropriation claim is inadequately pled for the same reason. *See* *Defiance Button Mach. Co. v. C & C Metal Prod. Corp.*, 759 F.2d 1053, 1063 (2d Cir. 1985) (noting that under New York common law, owner of a trade secret must take "reasonable measures to protect its secrecy" (internal quotation marks omitted)); *Mason,* 848 F. App'x at 450-51. Accordingly, the district court did not err in dismissing these claims.

*** * ***

We have considered Plaintiff-Appellant Turret Labs' remaining arguments and find them to be without merit. Accordingly, we AFFIRM the judgment of the district court.

[1] Dock EnRoll is an "air cargo ground handling control application that allows for payment of fees and scheduling of shipments based on synchronized real-time United States Customs release notifications, [and] was the first software of its kind at the time." SAC ¶ 17.

[2] The SAC also brings claims for common-law unfair competition, conversion, and defamation, as well as fraud in connection with computers under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The district court dismissed the unfair competition, conversion, and CFAA claims, *Turret Labs,* 2021 WL 535217, at *6-7, and the parties voluntarily agreed to dismiss the defamation claim with prejudice shortly thereafter. Turret Labs does not pursue these claims on appeal.

[3] "Freight forwarders" are "the entities that arrange for the storage and shipping of merchandise on behalf of shippers." SAC ¶ 16.

[4] Turret Labs alternatively alleges that Defendants-Appellees gained access by "[u]sing a pre-approved access through Damco or other authorized freight forwarders [to] log[] in to the system . . . ." SAC ¶ 24(b). Turret Labs alleges nothing further regarding "Damco," however, or how access to an approved freight forwarder's login information was used to obtain unfettered access "above and beyond what authorized [freight forwarders] would be entitled to access . . . ." *See* SAC ¶ 35.

[5] Turret Labs alleges that a freight forwarder's access to Dock EnRoll would generally "allow such forwarder to be able to see information for airway bills assigned to that [particular] forwarder," SAC ¶ 32, but that Defendants-Appellees were "able to gain access to the airway bill information of multiple freight forwarders," providing them information such as the name of the shipper, consignee name, nature of the goods, weight, volume and customs release information, "which is proprietary information for the specific freight forwarder," SAC ¶ 33.