IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CROWDSTRIKE, INC.,   )
)
        Plaintiff,   )
)
    v.   )
)   C.A. No. 17-146-GMS
)
NSS LABS. INC.,   )
)
        Defendant.   )
)

MEMORANDUM

I.   INTRODUCTION

On February 10, 2017, CrowdStrike, Inc. filed suit against NSS Labs. Inc. (D.I. 3).
Presently before the court is CrowdStrike's motion for a temporary restraining order and
preliminary injunction (D.I. 2), filed contemporaneously with its Complaint. (D.I. 3).
CrowdStrike's motion requests that the court order NSS: (1) "to refrain from using any
CrowdStrike software in any public test"; (2) "to refrain from publishing any document or writing
discussing or related to CrowdStrike," its software, its technology, or its information; (3) "to
comply with all contractual terms including destruction or return of the Falcon software and any
other CrowdStrike technology"; and (4) "to identify to CrowdStrike all circumstances in which
third parties have been provided by NSS Labs with CrowdStrike technology or information already
and ensure return or destruction of all such technology and information." (D.I. 2 at 12–13). For
the reasons that follow, this court will deny CrowdStrike's motion.

II.   BACKGROUND

CrowdStrike is a cybersecurity company that provides "cloud-based endpoint threat detection to clients." (D.I. 3 at 2). CrowdStrike developed the Falcon software to provide advanced endpoint protection "by combining next-generation antivirus, endpoint detection and response, and proactive features." *Id.* NSS is a company that, among other things, tests cybersecurity software and tools available in the marketplace to determine how well they stand up to attacks. (D.I. 7 at 3); (D.I. 3 at 3). In addition to conducting public tests, NSS also conducts private tests of cybersecurity platforms under contracts with vendors. (D.I. 3 at 3).

On April 11, 2016, CrowdStrike and NSS executed the Private Engagement Agreement #3246 ("Private Agreement"), whereby NSS was to conduct a private test of CrowdStrike's Falcon cybersecurity platform and provide CrowdStrike with a report detailing the results of the test. (D.I. 3, Ex. 2). According to the Complaint, NSS failed to perform the tests in a way that CrowdStrike deemed accurate and acceptable. (D.I. 3 at 11–12). NSS conducted additional testing to attempt to remedy the failures CrowdStrike identified. *Id.* at 8. Around January 18, 2016, during discussions regarding a third round of private testing, NSS notified CrowdStrike that it was planning to perform a public test of the Falcon software. *Id.* It is the results of NSS's public test that CrowdStrike seeks to enjoin NSS from disclosing during a major technology gathering which begins on February 14, 2017, known as the RSA Conference. (D.I. 2 at 12–13).

III.   STANDARD OF REVIEW

Federal Rule of Civil Procedure 65 permits a party to seek a preliminary injunction or a temporary restraining order prior to trial proceedings. Fed. R. Civ. P. 65(a), (b). A preliminary injunction is "an extraordinary remedy, which should be granted only in limited circumstances." *Frank's GMC Truck Ctr., Inc. v. Gen. Motors Corp.*, 847 F.2d 100, 102 (3d Cir. 1988) (citation

2

omitted). In certain situations where a party faces the possibility of irreparable harm before the court can hold a hearing on the motion for a preliminary injunction, a temporary restraining order may be appropriate to preserve the status quo and prevent such irreparable harm. *See Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck Drivers Local No. 70 of Alameda Cty.*, 415 U.S. 423, 439 (1974). Specifically, a temporary restraining order or a preliminary injunction should only be granted if: (1) the plaintiff is likely to succeed on the merits; (2) denial will result in irreparable harm to the plaintiff; (3) granting the preliminary relief will not result in even greater harm to the nonmoving party; and (4) granting the injunction is in the public interest. *See Tanimura & Antle, Inc. v. Packed Fresh Produce, Inc.*, 222 F.3d 132 (3d Cir. 2000) (citing *Council for Alternative Political Parties v. Hooks*, 121 F.3d 876, 879 (3d Cir. 1997)). A court should balance these factors in determining whether to grant either form of relief, and should deny such relief where the plaintiff has failed to establish each element. *See NutraSweet Co. v. Vit-Mar Enterprises, Inc.*, 176 F.3d 151, 153 (3d Cir. 1999); *In re Arthur Treacher's Franchisee Litig.*, 689 F.2d 1137, 1143 (3d Cir. 1982).

IV. DISCUSSION

In deciding whether to issue a temporary restraining order, the Third Circuit has required courts to consider the four elements defined in the Standard of Review. Each of these elements will be considered in turn below. Before the court addresses each element, it wishes to discuss the issue of subject matter jurisdiction in this case.

Subject-matter jurisdiction is non-waivable, and, as such, "courts have an independent obligation to satisfy themselves of jurisdiction if it is in doubt." *Nesbit v. Gears Unlimited, Inc.*, 347 F.3d 72, 76 (3d Cir. 2003). Accordingly, it is proper for the court to raise *sua sponte* subject-matter jurisdiction concerns. *Id.* Here, the parties are in federal court because the complaint

3

includes a count arising under of the laws of the United States. *See Merrell Dow Pharm. Inc. v. Thompson*, 478 U.S. 804, 808 (1986). The parties, both being citizens of Delaware, do not satisfy the requirements for diversity jurisdiction. 28 U.S.C. § 1332 (2012).

NSS contends that federal jurisdiction is not proper here because the Complaint "fails to plausibly state a claim under the Defend Trade Secrets Act." (D.I. 7 at 6). While the court does not have before it a Rule 12(b)(1) motion, it still finds the customary 12(b)(1) analysis instructive. *See* Fed. R. Civ. P. 12(b)(1). "A Rule 12(b)(1) motion may be treated as either a facial or a factual challenge to the court's subject matter jurisdiction." *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). When the court analyzes a facial attack on subject-matter jurisdiction, it must only consider the allegations in the complaint in the light most favorable to the plaintiff. *See id.* The court finds the current arguments that NSS makes with regard to subject-matter jurisdiction analogous to a facial attack usually made in a 12(b)(1) motion. As such, though the court finds CrowdStrikes' claim that NSS misappropriated trade secrets tenuous at best, the court will exercise jurisdiction over CrowdStrike's motion for a temporary restraining order because it considers the facts alleged in the complaint in the light most favorable to CrowdStrike.

A. Likelihood of Success on the Merits

1. Breach of Contract

To prove likelihood of success on the merits for a breach of contact claim, CrowdStrike's first count in its Complaint, the party must provide evidence of: "(1) a contractual obligation; (2) a breach of that obligation by the defendant; and (3) resulting damage to the plaintiffs." *Greenstar, LLC v. Heller*, 814 F. Supp. 2d 444, 450 (D. Del. 2011).

CrowdStrike and NSS entered into the Private Agreement, which neither party disputes was a valid contract. (D.I 2 at 6); (D.I. 7 at 7). At this stage in the proceedings, the court is not

4

persuaded that CrowdStrike is likely to succeed on the merits of its breach of contract claim. CrowdStrike alleges that NSS plans to publish information that it developed through use of the Falcon software during the private tests. (D.I. 2 at 6–7). NSS maintains that any information it plans to disclose in its report on the effectiveness of the Falcon tool it acquired through its public, not private test. (D.I. 7 at 7–8). CrowdStrike argues, in turn, that the contract prevented NSS from conducting a public test altogether. (D.I. 2 at 6). Additionally, CrowdStrike states that NSS labs refused to return the Falcon software or confirm in writing that it was destroyed, breaching another contractual term. (D.I. 3, Ex. 2, Ex. A).

The Private Agreement between the parties states in relevant part that NSS shall not retain "[c]ustomer's [c]onfidential [i]nformation . . . to perform a public test or otherwise release information about [c]ustomer's [p]roduct to third parties without [c]ustomer's separate express written approval." (D.I. 3, Ex. 2 at Ex. A). NSS maintains that it would not use anything or disclose anything it learned during its private testing of the Falcon software. The Test Report on Falcon states that the test was conducted "free of charge and NSS did not receive any compensation in return for CrowdStrike's inclusion." (D.I. 8, Ex.1, at 2). NSS's website also states that "results from a private engagement are just that, private, and they will never be shared publicly." (D.I. 8, Ex. 3). Thus, if NSS did not use the confidential information it obtained during the private test of the Falcon software to perform the public test, then NSS did not breach that term of the contract.

The court is not convinced that NSS used confidential information it obtained during the private test to conduct the public test. The court is also not convinced that NSS failed to maintain the confidentiality of CrowdStrike's data in contravention of the Private Agreement. At this stage, the only colorable aspect of CrowdStrike's breach of contract claim is that NSS failed to return or destroy the Falcon software after termination of the Private Agreement. Even if CrowdStrike were

likely to succeed on that aspect of their claim, however, such a breach would not warrant granting a temporary restraining order or preliminary injunction.

CrowdStrike alleges that "a negative report shouted from the stage at the RSA Conference would damage" CrowdStrike's reputation, resulting in irreparable harm. Assuming such damage to CrowdStrike's reputation constitutes irreparable harm, NSS's failure to return or destroy the Falcon software is not related to that harm. It is a simple breach of contract claim that, if later proven, can be remedied with traditional monetary damages. *See Bennington Foods LLC v. St. Croix Renaissance, Grp., LLP*, 528 F.3d 176, 180 (3d Cir. 2008) (explaining that when a court confronts a typical breach of contract claim with no causal inferences necessary to find irreparable harm to reputation, any harm a party may suffer can remedied with traditional breach of contract damages).

2. Tortious Interference with a Contract

CrowdStrike's second count alleges that NSS tortiously interfered with a contract between CrowdStrike and Constellation when it obtained a copy of Falcon in violation of CrowdStrike's standard terms and conditions. To succeed in such a claim, CrowdStrike must demonstrate: (1) there was a contract; (2) which defendant knew of; and (3) an intentional act that played a significant role in causing the breach; (4) without justification; (5) that causes injury to the plaintiff. *Nelson v. Fleet Nat. Bank*, 949 F. Supp. 254, 260 (D. Del. 1996).

CrowdStrike states in the Complaint that it entered into a contract with the company Constellation for use of the Falcon software. (D.I. 3 ¶ 27). According to CrowdStrike, its contract with Constellation, like all of its other contracts, incorporated the CrowdStrike Terms and Conditions. (D.I. 2 at 7). CrowdStrike alleges that NSS knew of the Terms and Conditions which did not permit "third parties to access or use the Products," and prohibited "any competitive

6

analysis on the Products." (D.I. 3, Ex. 5 at ¶ 3.2). CrowdStrike further alleges that NSS sought a third-party with access to the Falcon software and induced that third-party to provide it access to the software, violating the Terms and Conditions of which NSS was aware. (D.I. 3 at 12). The court is not persuaded that CrowdStrike would succeed on the merits of this claim.

NSS maintains that it was not required to "click through" the Terms and Conditions prior to accessing the Falcon software for public testing. (D.I. 7 at 10–11). It, therefore, could not have been on notice of the terms of the contract between Constellation and CrowdStrike. *Id.* Further, NSS argues that even though its own contract with CrowdStrike prohibited it from disclosing or using private test results, that fact could not put NSS on notice that CrowdStrike's other contracts had similar terms. *Id.* at 10. The court agrees. The court finds no facts in the record before us that NSS was aware of the contract between Constellation and CrowdStrike, and intentionally acted in a way that caused the breach. The court, of course, does not have the benefit of a full evidentiary record on this point. More important though, even if the court were to find CrowdStrike's arguments persuasive, there is no interference with the contract to restrain. To the extent that the allegations in the Complaint are true, it is Constellation that breached its contract, and regardless of whether NSS played a role in that breach, it occurred in the past; therefore, there is nothing to restrain NSS from doing.

3. Misappropriation of Trade Secrets

CrowdStrike avers that NSS misappropriated its trade secrets in violation of the Defend Trade Secrets Act of 2016 when it "acquir[ed] CrowdStrike software from a third-party in violation of CrowdStrike's standard Terms and Conditions of the Private Agreement." (D.I. 3 ¶ 80). CrowdStrike contends that the trade secrets contained in the Falcon software include its methods of threat detection and certain "[i]nformation provided to NSS pursuant to the Private Agreement

for use in testing the Falcon software." (D.I. 3 at ¶¶ 77–78). There is no doubt that Falcon's methods of threat detection qualify as trade secrets. *See* 18 U.S.C. § 1839(3) (2016) ("[T]he term 'trade secret' means all forms and types of . . . methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible . . . ."). The court does, however, doubt whether or not information provided to NSS for use in testing and operating the Falcon software could qualify as a trade secret. Without the benefit of a full evidentiary record, the court will defer to CrowdStrike's allegations in the Complaint. Even taking those allegations to be true, however, it is not clear to the court that a misappropriation of any trade secrets occurred or will occur.

Under the statute, misappropriation is defined as either:

> [T]he acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who--(i)used improper means to acquire knowledge of the trade secret . . . .

18 U.S.C. § 1839(5)(A), (B)(i). It does not appear to the court that NSS used any information provided to it during the private test in the subsequent public test. It does not even appear to the court that NSS ever acquired any trade secrets derived from its private tests or the software supplied by Constellation. *See* (D.I. 8 ¶¶ 6, 24). Further, the court cannot identify any trade secrets that NSS plans to disclose to the public.

The court reviewed NSS's Advanced Endpoint Protection Test report on the Falcon software that it plans to present at the RSA Conference on Tuesday, February 14, 2017. The court did not identify any trade secrets disclosed in that report. The court also finds that NSS's

statements with regard to the scope of the testing it did on Falcon undermine CrowdStrike's arguments.

NSS conducted "black box" testing on the Falcon software. (D.I. 8 at 2). Such testing seeks to satisfy the goal of determining the effectiveness of the software. NSS's report states that its aim was to "verify that the [Falcon software] is capable of detecting, preventing, and continuously logging threats accurately, whilst remaining resistant to false positive." (D.I. 8, Ex. 1 at 5). NSS's report does not disclose the method by which the Falcon software detects threats or any information CrowdStrike provided to NSS for use in testing the software. *See* (D.I. 8, Ex. 1). Instead, it analyzed how the software stood up to different threat categories. *Id.* Accordingly, the purported irreparable harm to CrowdStrike's reputation that it alleges will occur as a result of this misappropriation is unfounded. NSS does not plan to disclose any of CrowdStrike's trade secrets; the court, therefore, cannot restrain NSS from doing something it is not currently doing and does not plan to do.

B. Irreparable Harm

In order for the court to grant a temporary restraining order, the plaintiff must show that it will be irreparably harmed by the denial of such relief. *See Tanimura*, 222 F.3d at 140. Harm to reputation and goodwill can constitute irreparable harm "so long as the plaintiff makes a clear showing." *Groupe SEB USA, Inc. v. Euro-Pro Operating LLC*, 774 F.3d 192, 205 (3d Cir. 2014).

Here, CrowdStrike has not demonstrated that it is likely to suffer irreparable harm if the temporary restraining order is not granted. CrowdStrike contends that NSS's report will "cast the Falcon tool in a poor light, and a cursory analysis of the two private reports shows that the public report will be inaccurate." (D.I. 2 at 11). An inaccurate ranking of Falcon among its competitors

will, according to CrowdStrike, decrease sales and revenues. *Id.* The court finds that the harm CrowdStrike alleges it will suffer does not flow from CrowdStrike's claims.

The report NSS plans to present at the conference was the result of a public test. (D.I. 8 ¶ 6). NSS is not disclosing results of the private test it performed for CrowdStrike. *Id.* ¶ 20. Accordingly, even if NSS breached the Private Agreement with CrowdStrike, any harm resulting from that breach is not related to the harm CrowdStrike purports it will suffer here upon disclosure of the public report. As previously mentioned, even if the court found that NSS misappropriated CrowdStrike's trade secrets, the report does not disclose any trade secrets. Restraining NSS from presenting the report at the conference would not remedy the harm CrowdStrike claims it suffered as a result of the misappropriation. With regard to the tortious interference claim and any harm caused as a result, assuming the allegations in the Complaint are true, the interference with the Constellation contract already occurred and there is nothing to restrain NSS from doing with regard to that contract.

Any harm to reputation or goodwill here is also not irreparable, even if it were to flow from the claims CrowdStrike alleged in its Complaint. As NSS points out, CrowdStrike could publicly correct any wrong test results that it believes NSS generated. The court thus finds that CrowdStrike has not demonstrated that it suffered harm resulting from the claims it made in its Complaint, or that such harm would be the types courts classify as irreparable. *See Groupe*, 774 F.3d at 205 (holding that plaintiff demonstrated irreparable harm to the brand's reputation because the claims made by defendants were unsubstantiated comparative claims, and the harm would be impossible to subsequently remedy).

C. Balance of Hardships

If the court finds that issuance of a temporary restraining order would irreparably harm the moving party pending final disposition of the case, the court must balance the hardships to both parties to ensure that the order does not harm the non-moving party more than the moving party. *See Kos Pharm., Inc. v. Andrx Corp.*, 369 F.3d 700, 727 (3d Cir. 2004). Here, the court does not find irreparable harm to CrowdStrike. Nonetheless, the court still believes that NSS would, in fact, suffer more harm than CrowdStrike if the court were to grant CrowdStrike's request for a temporary restraining order and preliminary injunction. If the court were to issue the order, NSS would be enjoined from disclosing likely true and legitimately obtained data, undermining a critical aspect of NSS's presence in the marketplace. The Complaint states that NSS tests cybersecurity tools and software to inform consumers which are the best to buy. (D.I. 3 ¶ 13). The court agrees with NSS that its business would be in jeopardy if a company could restrain NSS from publishing the results of its test every time a company questions the methods by which the test was conducted and the final results. (D.I. 7 at 13).

While it is possible that CrowdStrike will suffer a decrease in sales and revenue as a result of NSS's report, CrowdStrike could mitigate that hardship by challenging the veracity of NSS's results and their testing methods. As NSS points out, mitigating any hardship it suffers as a result of a wrongfully issued temporary restraining order would be much harder because the technological innovation is so rapid. The public would not be interested in the effectiveness of old products when there are already new ones on the market. Accordingly, the public interest weighs slightly in favor of denying CrowdStrike's request for a temporary restraining order and preliminary injunction.
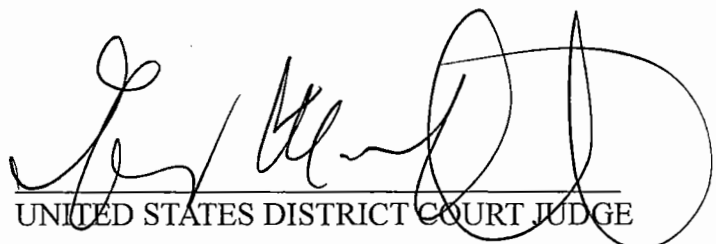
D. Public Interest

Finally, in determining whether to grant a preliminary injunction, the Third Circuit directs that courts should consider if doing so would be in the public interest. *See Tanimura*, 222 F.3d at 140. The recently enacted Consumer Review Fairness Act of 2016 underscores the public's interest in performance assessments. 15 U.S.C. § 45(b) (2016). The new law voids provisions of form contracts that restrict a party to that contract from conducting a "performance assessment of, or other similar analysis of, including by electronic means, the goods, services, or conduct of a person." *Id.* The court finds that the public has a very real interest in the dissemination of information regarding products in the marketplace. If it turns out, in this case, that NSS's data is inaccurate, CrowdStrike could publicly rebut that data with evidence of its faults. The public would, in fact, benefit from such an exchange between the parties because it would serve to inform them about the trust they should put in NSS's future reports. As such, the public interest weighs strongly in favor of denying CrowdStrike's motion.

VI.   CONCLUSION

Because the court concludes that Plaintiffs have failed to demonstrate a likelihood of success on the merits and irreparable harm, and because the remaining factors weigh against granting a temporary restraining order or preliminary injunction, the court will deny Plaintiffs' request.

Dated: February 13, 2017

UNITED STATES DISTRICT COURT JUDGE