SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK: IAS PART 3

----------x

BITSIGHT TECHNOLOGIES, INC. and
NSEC-SISTEMAS INFORMATICOS, S.A.,
d/b/a ANUBISNETWORKS,

Plaintiffs,

-against-

SECURITYSCORECARD, INC.,

Defendant.

----------x

Index No. 650042/2015
Motion Seq. No. 003
Motion Date: 9/28/2015

EILEEN BRANSTEN, J.:

In this breach of contract action, plaintiffs Bitsight Technologies, Inc. ("Bitsight") and NSEC-Sistemas Informaticos, S.A., d/b/a Anubisnetworks ("Anubis") allege that defendant SecurityScorecard, Inc. ("SecurityScorecard") misappropriated and misused information received from Anubis pursuant to an agreement. Through this motion, SecurityScorecard seeks to bar litigation of certain issues on "law of the case" grounds and also moves for dismissal of the complaint in its entirety, pursuant to CPLR 3211(a)(7). For the reasons that follow, the Court deems that the "law of the case" doctrine does not apply, while SecurityScorecard's motion to dismiss is granted in part and denied in part.

I. Background

Plaintiff Anubis offers "real-time threat intelligence products" that provides "customers with actionable security information by gathering data from a wide range of sources worldwide." (Compl. ¶ 11.) At issue in this litigation is a real-time threat intelligence product called "Cyberfeed." "At its most basic level, the cyberfeeds identify computers across the globe that are infected or otherwise compromised with certain malware or viruses and thus pose a security threat to the organizations that own or communicate with those computers." *Id.* ¶ 12. Defendant SecurityScorecard produces security rating products for marketing and sale to third-parties. *Id.* ¶ 25. Plaintiff Bitsight likewise markets and sells security rating products to third-parties and was a subscriber to Anubis' cyberfeeds. *Id.* ¶ 14. Bitsight acquired Anubis on October 10, 2014. *Id.*

A. *The Agreement*

This dispute stems from a March 18, 2014 agreement between Anubis and SecurityScorecard, under which Anubis agreed to provide SecurityScorecard "a Cyberfeed Service" for one year (the "Agreement"). *See* Affirmation of Kenneth W. Taber ("Taber Affirm.") Ex. C. As defined in the Agreement, "Cyberfeed Services" ("Cyberfeeds") are "[a] subscription based feed service that allows customers to obtain real time intelligence feeds about events related to security threats, as seen world wide,

with relevance to their organization." *Id.* Ex. C at § 1(b). Under the Agreement, SecurityScorecard "warrant[ed] and agree[d] that it shall: a) Use provided feeds for own internal use only [and] b) Not resell cyberfeeds to customers (customers using directly cyberfeeds in their systems)." *Id.* Ex. C at Annex 1, § 2.1.

B. *Termination of the Agreement*

In an October 7, 2014 email to SecurityScorecard, Francisco Fonseca, Anubis's chief executive officer, wrote, "[i]t is our understanding that [SecurityScorecard] has been making Anubis' Cyberfeed Service available and/or reselling it to third parties." *Id.* Ex. B at 3. Fonseca demanded that SecurityScorecard cease using the Cyberfeeds in violation of the Agreement and that it delete all Cyberfeed data from "any external websites, databases, subscriptions, product offerings, servers or other services or offerings." *Id.* Fonseca also gave notice that the Agreement would be terminated effective November 5, 2014, pursuant to section 6.7 of the Agreement, which provided for termination of the Agreement without cause by either party upon 30 days notice. *Id.*

The chief executive officer of SecurityScorecard responded by email the same day, stating:

> I can assure you we are not reselling the feed to any third parties or making the feed available as is to anyone. We are using the feed in our

> SecurityScorecard grading service as one of many data components to help with our security assessments.

(Taber Affirm. Ex. B at 2.)

Three days later, Bitsight, a long-time customer of Anubis and a competitor of SecurityScorecard, acquired Anubis. (Compl. ¶ 14.) The Agreement terminated at midnight on November 5, 2014. *Id.* ¶ 30.

C. *The Federal Action*

On November 10, 2014, Anubis filed a complaint against SecurityScorecard in the United States District Court for the Southern District of New York (the "Federal Action"). (Taber Affirm. Ex. F.) The complaint in the Federal Action asserted four claims: (1) breach of contract; (2) "misappropriation of confidential information/unfair competition"; (3) injunctive relief; and, (4) declaratory relief.

Contemporaneous with its filing of a complaint in the Federal Action, Anubis filed a motion for preliminary injunction. This motion for preliminary injunction was denied by the federal court on December 11, 2014. *See* Taber Affirm. Ex. A at 2:24-3:6 (Transcript of Dec. 11, 2014 Oral Argument). After denying Anubis' motion, the federal court directed the parties to report to the court on January 13, 2015 on the status of the litigation. *Id.* at 3:10-11.

D. *The Instant Action*

On January 7, 2015, Anubis filed a voluntary discontinuance in the Federal Action, and on the same day, commenced the instant action before this Court with Bitsight added as an additional plaintiff.

In the instant complaint, Plaintiffs contend that SecurityScorecard wrongfully continues to use the Cyberfeeds it obtained prior to termination of the Agreement. In support, plaintiffs allege that SecurityScorecard gave a presentation to potential clients about products that used the Cyberfeeds and continues to use the Cyberfeeds "as a critical component in the security rating products it sells to third parties." (Compl. ¶¶ 28-31.)

As in the Federal Action, Plaintiffs again assert causes of action for breach of contract, "misappropriation of confidential information/unfair competition," injunctive relief, and declaratory relief. In addition, Plaintiffs add misrepresentation, false advertising, and constructive trust claims, as well as a demand for punitive damages.

II. Discussion

Defendant now seeks to bar plaintiffs from re-litigating certain issues addressed by the federal court in its consideration of Anubis' preliminary injunction motion and likewise requests dismissal of the complaint in its entirety under CPLR 3211(a)(7) for failure to state a cause of action. These arguments are addressed in turn.

A. *Law of the Case*

SecurityScorecard first seeks to preclude litigation of issues, such as breach of the Agreement, contending that they were decided by the federal court and are therefore law of the case.

"[L]aw of the case addresses the potentially preclusive effect of judicial determinations made in the course of a single litigation *before* final judgment." *People v. Evans*, 94 N.Y.2d 499, 502 (2000). It is "a judicially crafted policy that expresses the practice of courts generally to refuse to reopen what has been decided, [and is] not a limit to their power. As such, law of the case is necessarily amorphous in that it directs a court's discretion, but does not restrict its authority." *Id.* at 503. "The granting or refusal of a temporary injunction does not constitute the law of the case or an adjudication on the merits." *J.A. Preston Corp. v. Fabrication Enter., Inc.*, 68 N.Y.2d 397, 402 (1986).

Anubis commenced the Federal Action as the sole plaintiff, asserting the same factual allegations that plaintiffs make in the instant action. The four claims asserted in the Federal Action – breach of contract, misappropriation of confidential information, injunctive relief and declaratory relief – are also asserted in the instant action. In the Federal Action, Anubis sought a temporary restraining order ("TRO"). The parties briefed the issue and presented oral arguments before the federal court on November 14, 2014 and December 2, 2014. In the course of those arguments, the judge questioned

whether the Cyberfeeds were confidential information pursuant to the Agreement and whether the Agreement barred SecurityScorecard's use of past Cyberfeeds, without explicitly ruling on any issue. (Taber Affirm. Ex. D at 10-11, 12; *id.* Ex. E at 8.) The federal judge denied the application for a TRO from the bench on December 11, 2014, stating:

> I am going to deny the plaintiff's request for a preliminary injunction. The plaintiffs have failed to demonstrate irreparable harm, and the plaintiffs have failed to show either a likelihood of success on the merits or sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly toward the party requesting the preliminary relief.

Id. Ex. A at 2-3.

The federal judge's preliminary injunction ruling is not a final determination for law of the case purposes, and neither his questions during oral argument nor his ultimate ruling on the TRO constitute a judicial determination or an adjudication on the merits. *J.A. Preston Corp.*, 68 N.Y.2d at 402. Accordingly, defendant's motion to preclude issues as barred by law of the case is denied.

B. *Defendants' CPLR 3211(a)(7) Motion*

On a motion to dismiss a complaint for failure to state a cause of action, all factual allegations must be accepted as truthful, the complaint must be construed in a light most favorable to the plaintiffs and the plaintiffs must be given the benefit of all reasonable

inferences. *Allianz Underwriters Ins. Co. v. Landmark Ins. Co.*, 13 A.D.3d 172, 174 (1st Dep't 2004). "We . . . determine only whether the facts as alleged fit within any cognizable legal theory." *Leon v. Martinez*, 84 N.Y.2d 83, 87-88 (1994). This Court must deny a motion to dismiss "if from the pleadings' four corners factual allegations are discerned which taken together manifest any cause of action cognizable at law." *511 W. 232nd Owners Corp. v. Jennifer Realty Co.*, 98 N.Y.2d 144, 152 (2002) (internal quotation marks and citations omitted).

1. Breach of Contract (fourth cause of action)

Plaintiffs next assert a breach of contract claim, grounded in the allegation that SecurityScorecard breached the Agreement's provisions governing "Confidential Information" (Section 10.2(c)), authorization to resell Cyberfeed (Sections 2 and 2.1 of Annex 1), and ownership of Cyberfeeds (Section 5.1). (Compl. ¶ 59.)

For a breach of contract claim, a plaintiff must allege: (1) the existence of a contract, (2) plaintiff's performance of the contract, (3) defendant's breach of the contract, and (4) resulting damages. *See Harris v. Seward Park Housing Corp.*, 79 A.D.3d 425, 426 (1st Dep't 2010).

a. **Section 10.2(c)**

The threshold question for plaintiff's breach of Section 10.2(c) is whether the Cyberfeeds were "Confidential Information" under the Agreement. "[W]ords and phrases" used in a contract must "be given their plain meaning." *Ellington v. EMI Music, Inc.*, 24 N.Y.3d 239, 244 (2014). "A contract is not rendered ambiguous simply because one of the parties attaches a different, subjective meaning to one of its terms." *Sasson v. TLG Acquisition LLC*, 127 A.D.3d 480, 481 (1st Dep't 2015). Here, the Agreement provides that "'Confidential Information' includes all information relating to the trade secrets, operations, processes, plans, intentions, product information, know-how, designs, market opportunities, transactions, affairs and/or business *of the other party* [i.e. Anubis] and/or to its Customers or suppliers." (Agreement § 10.1) (emphasis added).

A plain reading of the Agreement's definition of "Confidential Information" does not include the Cyberfeeds. As alleged in the complaint, the Cyberfeeds are data collected by Anubis regarding the security of other companies' computer networks. Data pulled from other companies' computer systems is not a "trade secret" belonging to Anubis nor does it fall under the remaining enumerated categories of "Confidential Information" in Section 10.1 of the Agreement. Further, such data is not the"know-how" or "product information" regarding plaintiffs' own subscription service. Defendant makes a sound analogy to Westlaw, a subscription legal research service that provides

access to, *inter alia*, court decisions. Westlaw does not produce the court opinions on its site; instead, Westlaw collects court decisions that are available on public dockets throughout state and federal courts and makes them more conveniently available in one location. While computer algorithms used by Westlaw to search for, collect, process and collate such decisions would be protected information under the Agreement's definition of "Confidential Information," the decisions themselves remain publicly available documents. The same is true here. The methods by which Anubis collected the Cyberfeed data fall under the definition of "Confidential Information"; however, the Cyberfeed information for which defendant purchased subscription access was not transformed into "Confidential Information" when Anubis decided to sell subscription access to it.

Other than the Cyberfeeds, neither the complaint nor plaintiffs' opposition papers specify any confidential information allegedly misappropriated by SecurityScorecard. The same holds true for plaintiffs' claims that SecurityScorecard misappropriated intellectual property, which the Agreement defines as "patent, copyright, confidential information, database rights, rights in designs, know-how, mask works, trademarks, service marks, trade and business names, domain names, trade secrets and any other similar rights." *Id.* § 1(f). Nor do plaintiffs explain how the purported intellectual

property was misappropriated, other than through conclusory allegations of misappropriation.

Accordingly, the complaint does not state a breach Section 10.2 of the Agreement because the Cyberfeeds were not "Confidential Information," as defined in the Agreement. Accordingly, SecurityScorecard's motion to dismiss this portion of the breach of contract claim is granted.

b. **Annex 1 – Sections 2 and 2.1**

Plaintiffs next allege that SecurityScorecard breached the Agreement's provisions restricting use of the Cyberfeeds. Under Annex 1, Section 2.1(a) of the Agreement, SecurityScorecard agreed to "[u]se provided [Cyberfeeds] for internal use only." SecurityScorecard admits use of the Cyberfeeds "in our SecurityScorecard grading service as one of many data components to help with our security assessments." (Taber Affirm. Ex. B at 2.) SecurityScorecard contends that its use of Cyberfeeds, among many other sources of information in SecurityScorecard's own end products, was acknowledged and accepted by Anubis. It is a question of fact, however, whether such use constitutes "internal use only" or is otherwise permissible under the Agreement. Accordingly, SecurityScorecard's motion to dismiss this portion of the breach of contract

claim is denied. *Fischbach & Moore v. Howell Co.*, 240 A.D.2d 157, 157-58 (1st Dep't 1997) (affirming denial of CPLR 3211 motion based upon the existence of factual issues).

Plaintiffs allege that SecurityScorecard breached Annex 1, Section 2.1(b) of the Agreement, which provides that SecurityScorecard shall "[n]ot resell Cyberfeeds to customers (customers using directly Cyberfeeds in their systems)." SecurityScorecard contends that this provision prohibits only the resale of intact Cyberfeeds directly to its customers, which it states it did not do. However, a question of fact exists as to whether its use of the Cyberfeeds as an element of its end products was in accordance with this provision of the Agreement. Accordingly, SecurityScorecard's motion to dismiss this portion of the breach of contract claim is denied. *Fischbach & Moore*, 240 A.D.2d at 157-58.

c. **Section 5.1**

Plaintiffs further allege that SecurityScorecard breached Section 5.1 of the Agreement, which provides that "AnubisNetworks shall retain all rights, title and interest in and to the Services," which, in turn, refers to the Cyberfeed Services. (Agreement §§ 1(b) & (f), and Annex 1.) Plaintiffs contend that SecurityScorecard "is continuing to use the Cyberfeed data . . . that it received from Plaintiffs under the Agreement in its presentations to prospective customers and in the products it is selling to customers, post-

termination of the Agreement." (Compl. ¶ 29.) SecurityScorecard argues that its use of increasingly stale information that it previously paid for and that it transformed into its own reports, commingling the information with other sources, does not violate the Agreement. Whether such use is permissible under the Agreement is a question of fact. Accordingly, SecurityScorecard's motion to dismiss this portion of the breach of contract claim is denied. *Fischbach & Moore*, 240 A.D.2d at 157-58.

For the foregoing reasons, SecurityScorecard's motion to dismiss plaintiffs' breach of contract claim is granted to the extent of dismissing the portion of the breach of contract claim that is based upon Section 10.2(c) of the Agreement and is otherwise denied.

2. Misappropriation of Confidential Information/Unfair Competition (first cause of action)

In support of their misappropriation and unfair competition claim, plaintiffs allege that SecurityScorecard made the Cyberfeed data, provided by Anubis under the Agreement, available to third parties in contravention of SecurityScorecard's agreement that it would use the Cyberfeeds "only for its only [sic] internal use and would not resell those feeds." (Compl. ¶ 24.) Plaintiffs deem the Cyberfeeds to be "Confidential Information" under the Agreement and further contend that SecurityScorecard continues

to use such data in connection with the security rating products it sells to third parties. *Id.* ¶¶ 41-42.

Moreover, a claim for misappropriation of confidential information must "allege that [the plaintiff] took sufficient precautionary measures to insure that the information remained secret." *Edelman v. Starwood Capital Grp., LLC*, 70 A.D.3d 246, 249 (1st Dep't 2009), *lv. denied* 14 N.Y.3d 706 (2010). Of course, the complaint makes no such allegation with respect to the third-party information that Anubis sold to SecurityScorecard as well as to others. To the contrary, plaintiffs concede that Anubis' business hinged on making this data available to Cyberfeed subscribers. (Compl. ¶¶ 11-12.) Accordingly, plaintiffs fail to state a claim for misappropriation of confidential information on this basis as well.

Plaintiffs likewise fail to state a claim for unfair competition, since the claim "lacks the requisite elements of either a confidential relation between the parties or a valid agreement to refrain from the alleged unfair competition." *V. Ponte & Sons v. Am. Fibers Int'l*, 222 A.D.2d 271, 272 (1st Dep't 1995). Defendant's motion to dismiss this cause of action is granted.

3. Misrepresentation (second cause of action)

In discussions preceding the termination of the Agreement, plaintiffs allege that SecurityScorecard acknowledged that plaintiffs were the owners of confidential information and intellectual property. Nevertheless, according to plaintiffs, defendant's representations that plaintiffs owned this confidential information and intellectual property were false, as demonstrated by the fact that defendant subsequently "represent[ed] to the market that it [SecurityScorecard] is the owner" of the information received under the Agreement. (Compl. ¶¶ 45-46.)

Plaintiffs first fail to state a claim for misrepresentation because, as addressed above, the complaint does not allege that the Cyberfeeds are confidential information or intellectual property. This claim is dismissed for the additional reason that it merely restates the breach of contract claim. *OP Solutions, Inc. v. Crowell & Moring, LLP*, 72 A.D.3d 622, 622 (1st Dep't 2010). Accordingly, SecurityScorecard's motion to dismiss this cause of action is granted.

4. False Advertising/Unfair Competition (third cause of action)

Plaintiffs next allege that SecurityScorecard engaged in false advertising by marketing products containing old Cyberfeeds that it obtained while the Agreement was in effect, representing the products as providing "real-time threat intel and actionable

intelligence to customers." (Compl. ¶ 50.) According to plaintiffs, the use of stale Cyberfeeds renders SecurityScorecard's claims for its products false and misleading and that such advertising has diverted sales from Bitsight.

"Claims under General Business Law §§ 349 and 350 are available to an individual consumer who falls victim to misrepresentations made by a seller of consumer goods through false or misleading advertising." *Solomon v. Bell Atl. Corp.*, 9 A.D.3d 49, 52 (1st Dep't 2004). To state a claim under these sections, "a plaintiff must allege that the defendant has engaged in an act or practice that is deceptive or misleading in a material way and that plaintiff has been injured by reason thereof." *Id.* (internal quotation marks and citations omitted).

Although plaintiffs argue that they are asserting claims on behalf of consumers, they fail to allege any specific misrepresentation in SecurityScorecard's promotions of its products. They likewise do not allege that SecurityScorecard is representing that it uses the Cyberfeeds in its products and make only the conclusory allegation that any use of dated Cyberfeeds in SecurityScorecard products is deceptive. Accordingly, plaintiffs' unfair competition claim in connection with this cause of action also fails to state a claim. *V. Ponte & Sons, Inc.*, 222 A.D.2d at 272. For these reasons, SecurityScorecard's motion to dismiss this cause of action is granted.

5. Declaratory Relief (sixth cause of action)

Plaintiffs seek a judgment declaring that:

(a) Plaintiffs retain all right, title, and interest in the Confidential Information and intellectual property (including cyberfeed data) provided to SecurityScorecard at any time under the Agreement;

(b) Plaintiffs have lawfully terminated the Agreement;

(c) Plaintiffs are entitled to a return of all Confidential Information and intellectual property (including cyberfeed data) provided to SecurityScorecard and a certification from SecurityScorecard that it is not using such Confidential Information and cyberfeed data for any purpose; and

(d) SecurityScorecard is prohibited under the Agreement from using the Confidential Information and intellectual property (including cyberfeed data) in connection with the provision of products or services that it licenses or sells to third-parties, including without limitation its security rating products.

(Compl. at Prayer for Relief ¶ 4.)

A plaintiff "may not seek a declaratory judgment when other remedies are available, such as a breach of contract action." *Singer Asset Fin. Co., LLC v. Melvin*, 33 A.D.3d 355, 358 (1st Dep't 2006). The declaratory relief that plaintiffs seek is either duplicated in its other causes of action or is not contested (for example, that the Agreement was lawfully terminated), evidencing the lack of a justiciable controversy. *Matter of Gates v. Hernandez*, 26 A.D.3d 288, 289 (1st Dep't 2006). Accordingly, SecurityScorecard's motion to dismiss this cause of action is granted.

6. Constructive Trust (seventh cause of action)

Plaintiffs seek the imposition of a constructive trust "over all profits that SecurityScorecard has derived, and will in the future derive, from its misconduct." (Compl. ¶ 81.) "To impose a constructive trust, the following factors must be shown: (1) a confidential or fiduciary relationship, (2) a promise, (3) a transfer in reliance thereon, (4) a breach of the promise and (5) unjust enrichment." *Zuch v. Zuch*, 117 A.D.2d 397, 403-04 (1st Dep't 1986). A cause of action for constructive trust is subject to dismissal where the plaintiff can be adequately compensated by money damages. *Knopf v. Sanford*, 123 A.D.3d 521, 522 (1st Dep't 2014).

Plaintiffs pleaded a conventional arms length business relationship with defendant and therefore have failed to allege facts demonstrating either a confidential or fiduciary relationship. *See, e.g., EBC I, Inc. v. Goldman, Sachs & Co.*, 5 N.Y.3d 11, 20 (2005) (stating that a fiduciary relationship "is grounded in a higher level of trust than normally present in the marketplace between those involved in arm's length business transactions."). In addition, plaintiffs have not pleaded that money damages would be inadequate to compensate them for their remaining claim – breach of contract. Consequently, SecurityScorecard's motion to dismiss this cause of action is granted.

7. Injunctive Relief (fifth cause of action)

Plaintiffs next seek injunctive relief in connection with their claims, alleging that the actions of SecurityScorecard have caused them irreparable harm. (Compl. ¶¶ 64-65.)

To show entitlement to injunctive relief, a plaintiff must demonstrate "irreparable harm for which monetary damages could not adequately compensate." *Derfner Mgmt. Inc. v. Lenhill Realty Corp.*, 105 A.D.3d 683, 684 (1st Dep't 2013). Plaintiffs have failed to make such a showing. Plaintiffs have one viable claim remaining in this action – breach of contract. The damages available for this breach of contract are monetary in nature, as they hinge on the sale of plaintiffs' information to SecurityScorecard's customers and the profits derived therefrom. If plaintiffs prevail on their claim, they could be adequately compensated by an award of monetary damages.

Accordingly, SecurityScorecard's motion to dismiss plaintiffs' claim for injunctive relief is granted.

III. **Conclusion**

Accordingly, it is

ORDERED that defendant SecurityScorecard's motion to dismiss is granted to the extent of dismissing the complaint's first, second, third, fifth, sixth and seventh causes of action and that portion of the fourth cause of action that is based upon defendant's alleged

breach of section 10.2(c) of the parties' March 18, 2014 Cyberfeed Service Agreement, and is otherwise denied; and it is further

ORDERED that defendant is directed to serve an answer to the complaint within 20 days after service of a copy of this order with notice of entry; and it is further

ORDERED that counsel are directed to appear for a preliminary conference in Room 442, 60 Centre Street, on March 15, 2016, at 10 a.m.

Dated: New York, New York
January 25, 2016

ENTER

Hon. Eileen Bransten, J.S.C.