NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

STRIKEFORCE TECHNOLOGIES, INC., Plaintiff, v. WHITESKY, INC., Defendant.	**Civil Action No. 13-1895 (SRC)** **OPINION**

CHESLER, District Judge

This matter comes before the Court upon the motion filed by Plaintiff StrikeForce Technologies, Inc. ("Plaintiff" or "StrikeForce") for a preliminary injunction against Defendant WhiteSky, Inc. ("Defendant" or "WhiteSky") pursuant to Federal Rule of Civil Procedure 65. WhiteSky has opposed the motion. The Court has considered the papers filed by the parties, including a sur-reply brief submitted by WhiteSky in further opposition to the motion. It proceeds to rule on the motion based on the papers submitted and without oral argument, pursuant to Federal Rule of Civil Procedure 78. For the reasons expressed below, the Court denies StrikeForce's motion for a preliminary injunction.

I. BACKGROUND

StrikeForce, based in New Jersey, is a leading provider of anti-keylogging software intended to protect personal computer users from fraud perpetrated through surveillance spyware

that records the user's keystrokes, which may contain sensitive information such as the user's passwords and credit card numbers. The StrikeForce software, known as GuardedID, uses encryption and out-of-band authentication technology to prevent third parties from tracking a user's keystrokes. StrikeForce has developed a proprietary security feature known as CryptoColor® , which provides the user visual colored feedback indicating that the keystrokes the user entered are encrypted and secure. WhiteSky, a California software company, sells internet security products designed to provide computer users with enhanced security in their online transactions and web browsing. One of WhiteSky's products is known as IDVault, which it sells directly to computer users in the marketplace. WhiteSky also offers the ConstantGuard Protection Suite product, which is available for download for users of Comcast internet service as a benefit of their Comcast subscription.[1]

This case arises out of the business relationship between the parties. StrikeForce licensed to WhiteSky its GuardedID software, as customized for integration into WhiteSky's products, in exchange for royalties on the sale of products that include the licensed software. The initial licensing agreement between StrikeForce and WhiteSky was entered into in May 2010 and then subsequently amended at least twice, mainly for the purpose of modifying royalty terms. The currently operative contract is the "Second Amended Software License & Development Agreement" (the "Agreement") executed in May 2011.

It appears that royalty issues and disputes persisted, but the parties were unable to agree to terms modifying the Agreement. In January 2012, WhiteSky contracted with another vendor

[1] The Court notes that there is a pending motion to dismiss, grounded, in part, on WhiteSky's contention that this Court lacks in personam jurisdiction over it. While the Court will, in a separate Opinion, address WhiteSky's arguments that it lacks minimum contacts with New Jersey to establish specific jurisdiction, it wishes to make clear here that it is aware of WhiteSky's motion and has considered the parties' arguments and evidence concerning personal jurisdiction.

of anti-keylogging software, a company known as Zemana, to license Zemana's software for bundling with WhiteSky's internet security products. According to Plaintiff, WhiteSky's use of Zemana's anti-keylogging software has resulted in a decrease in the royalties payable to StrikeForce. WhiteSky began bundling the Zemana software into its ConstantGuard product for Comcast in November 2012. The IDVault product continues to use StrikeForce software. Of relevance to the motion before the Court, StrikeForce believes that WhiteSky is sharing confidential information about StrikeForce's intellectual property, that is, its customized GuardedID software and CryptoColor technology with third parties, specifically with anti-keylogging software provider Zemana.

StrikeForce filed this lawsuit against WhiteSky asserting, among others, claims for breach of contract and a claim for violation of the New Jersey Trade Secrets Act, N.J.S.A. 56:15-1 et seq. It moves for a preliminary injunction requiring WhiteSky to cease using or disclosing StrikeForce's trade secrets to third parties.

II. DISCUSSION

A. Legal Standard

Federal Rule of Civil Procedure 65 authorizes the Court to issue a preliminary injunction. A party seeking a preliminary injunction bears the burden of establishing that "he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." Winter v. Natural Resources Defense Council, Inc., 555 U.S. 7, 20 (2008). While all four elements are essential, the Third Circuit has held that a court may not grant injunctive relief, "regardless of what the equities seem to require," unless the movant carries its burden of

establishing both a likelihood of success and irreparable harm. Adams v. Freedom Forge Corp., 204 F.3d 475, 484 (3d Cir.2000); see also Hoxworth v. Blinder, Robinson & Co., 903 F.2d 186, 197 (3d Cir.1990) (holding same); In re Arthur Treacher's Franchisee Litig., 689 F.2d 1137, 1143 (3d Cir. 1982) (holding that "a failure to show likelihood of success or a failure to demonstrate irreparable injury must necessarily result in the denial of a preliminary injunction."). "[T]he grant of injunctive relief is an 'extraordinary remedy, which should be granted only in limited circumstances.'" Instant Air Freight Co. v. C.F. Air Freight, Inc., 882 F.2d 797, 800 (3d Cir.1989) (quoting Frank's GMC Truck Ctr. Inc. v. Gen. Motors Corp., 847 F.2d 100, 102 (3d Cir.1988)).

For the reasons that follow, the Court concludes that Plaintiff has failed to carry its burden to establish either likelihood of success on the merits or irreparable harm. As both lacking elements are essential to obtain a preliminary injunction, the Court will not proceed to consider the balance of equities or the public's interest in the relief sought by StrikeForce.

B. Likelihood of Success on the Merits

Plaintiff bases its request for a preliminary injunction on its claim that Defendant has misappropriated trade secrets and disclosed confidential information about StrikeForce's customized GuardedID software and its CryptoColor feature, in violation of New Jersey's Trade Secrets Act and breach of the Agreement's provision barring such conduct.[2] Thus, the Court must determine whether Plaintiff has demonstrated a likelihood of success on the merits of the claims for these alleged violations.

[2] Though its moving brief argued that a preliminary injunction is warranted based on the alleged violations underlying all of StrikeForce's claims against WhiteSky, including its claims for breach of contract and unjust enrichment, StrikeForce subsequently clarified that its application seeks only to protect the improper use and disclosure of its trade secrets. In its reply brief, StrikeForce stated that while it does base this application in part on the alleged breach of the Agreement's provision prohibiting WhiteSky from sharing confidential information with third parties, it does not seek an injunction for any claim for which a monetary award is sought.

The New Jersey Trade Secrets Act prohibits the actual or threatened misappropriation of a trade secret. N.J.S.A. 56:15-3. Under the statute, the following acts constitute misappropriation:

> (1) 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
>
> (2) Disclosure or use of a trade secret of another without express or implied consent of the trade secret owner by a person who:
>
> (a) used improper means to acquire knowledge of the trade secret; or
>
> (b) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was derived or acquired through improper means; or
>
> (c) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired through improper means.

N.J.S.A. 56:15-2. The statute defines "trade secret" broadly as "information . . . without regard to form" that has economic value as a result of not being known to others who might derive economic value from its use and that is the subject of reasonable efforts to maintain its secrecy. Id. The Trade Secrets Act provides that an injunction is an appropriate remedy for violation of the statute. N.J.S.A. 56:15-3.

With regard to StrikeForce's claim that improper use and/or disclosure has been made by Defendant in violation of the Agreement, StrikeForce points to provisions acknowledging that it has property rights in the customized GuardedID software (referred to in the Agreement as the "Customized Software"). StrikeForce relies on a clause in the Agreement in which "Whitesky acknowledges that SFT [StrikeForce] owns and distributes in various forms the components of the Customized Software as part of SFT's published and patent pending GuardedID products,

and that the GuardedID software is not generally published and embodies SFT trade secrets." Agreement § 3.1(a). It also points to the Agreement's broad definition of "intellectual property" as "any and all Trademarks, know-how, methodologies, processes, technologies, analysis, models, techniques, proprietary information . . . software, software code (in any form including without limitation source code and object code or executable code), user interfaces, and other forms of technology." Id., § 1.12 The Agreement expressly prohibits use, distribution, modification and/or reverse engineering of the software, except as authorized in the Agreement. Id., § 3.1(b). Moreover, the Agreement contemplates injunctive relief, to be sought by either party, for protection of intellectual property and confidential information. Id., § 12.

This Court finds that Plaintiff has not established that it is likely to succeed on its claims. The critical deficiency lies in the lack of evidence that WhiteSky has disclosed to a third party or improperly used any of StrikeForce's trade secrets. Before turning to an evaluation of the element of misappropriation, the Court must begin with an understanding of the non-public, economically valuable "information . . . in any form" that would trigger the protection of the Trade Secrets Act, or put differently, the trade secrets StrikeForce claims are protected by the Agreement.

StrikeForce identifies the trade secrets at issue as the GuardedID software, its anti-keylogging techniques and methods (which include its keystroke encryption technology and out-of-band authentication), and the proprietary CryptoColor feature of its software. It asserts, through the Declaration of StrikeForce CEO Mark Kay, that the methodologies and processes underlying the software are not known to the public and that, while StrikeForce has sought a patent for GuardedID, it maintains the secrecy of information concerning how the software and CryptoColor perform their encryption functions. Kay further declares that in the course of

developing a customized version of its software to meet WhiteSky's particular needs for its products, StrikeForce showed WhiteSky how to build the GuardedID functions into WhiteSky software and taught it how to recreate the CryptoColor feature. This sharing of knowledge and secrets, Kay asserts, was the equivalent of giving WhiteSky the source code for GuardedID and CryptoColor.

Were the Court to accept the truth of these assertions, the Court could theoretically reach the conclusion that the information at issue falls within the purview of the Trade Secrets Act, at least insofar as necessary for StrikeForce to demonstrate a likelihood of success on the merits. WhiteSky, however, controverts StrikeForce's evidence, submitting its own declarations made by Juan Gamez, its Chief Architect who leads development efforts, and V. David Watkins, its CEO. They deny receipt of anything but software in its executable form, that is, without any of the underlying source code or information concerning how the software was created or how it operates. Moreover, Gamez asserts that WhiteSky has "never made any effort to disassemble, decompile, reverse engineer, or otherwise attempt to discover the contents of the source code." (Gamez Decl., ¶ 5.)

Putting this factual dispute aside, the Court may, for purposes of this motion only, assume that GuardedID and CryptoColor themselves amount to trade secrets under the TSA, for even if StrikeForce had sufficiently established this aspect of its claim, it has not proffered evidence to demonstrate misappropriation. With respect to any confidential information and/or anti-keylogging methodologies (other than the CryptoColor feature), even if StrikeForce did in fact share with WhiteSky the equivalent of source code for its software, StrikeForce makes no attempt to substantiate its belief that WhiteSky is making unauthorized use of the information or is disclosing it to third parties, such as StrikeForce competitor Zemana.

As to the misuse of CryptoColor, the Court is presented with, at best, a disputed factual issue. On the one hand, StrikeForce asserts that WhiteSky continues to use CryptoColor for anti-keylogging in its ConstantGuard product, in which the StrikeForce software was replaced with Zemana software. In his declaration, StrikeForce CEO Kay states that he observed the improper use of StrikeForce's proprietary feature in the WhiteSky-Zemana consolidated product when, on May 8, 2013, he downloaded the then-current version of ConstantGuard. He attaches a screenshot of a webpage taken on that date to demonstrate the utilization of CryptoColor in the WhiteSky-Zemana product, which was then enabled to provide internet security. He also attaches, by way of comparison, a screenshot that shows the CryptoColor feature when StrikeForce's GuardedID software is activated and a screenshot that shows the absence of color highlighting when Zemana's anti-keylogging software is operating. This comparison, Kay asserts, illustrates that the WhiteSky-Zemana ConstantGuard product, which applies field color highlighting, continues to utilize CryptoColor. On the other hand, WhiteSky maintains that its products do not implement CryptoColor. According to the Gamez and Watkins declarations, although CryptoColor is a feature of StrikeForce's GuardedID product, WhiteSky requested that this feature be removed from the customized software developed by StrikeForce for incorporation into WhiteSky's products. WhiteSky's chief architect Gamez explains in his declaration that "Whitesky requested that this feature be removed from the Customized Software delivered to us because it required the use of the StrikeForce toolbar which White Sky did not want to include in our products. The StrikeForce toolbar increased the size of the product and could impact browser performance." (Gamez Decl., ¶ 8.) Instead of using CryptoColor in the WhiteSky products, Gamez further states, WhiteSky implemented field highlighting. Field highlighting, Gamez explains, colors a particular field when the focus is on that field and leaves

it white when the focus is not on it. According to Gamez, field highlighting differs in numerous ways from CryptoColor and is a simple, common web function, for example, often used to alert a user that information entered in a field is incorrect. Both Gamez and WhiteSky CEO Watkins declare that WhiteSky informed StrikeForce that "it would create its own, independent implementation of field highlighting in White Sky software instead of using Crypto Color in the Customized Software." (Watkins Decl., ¶ 23; Gamez Decl., ¶ 9.) They further assert that while field highlighting is still used in the IDVault product (which incorporates StrikeForce's customized software), it has not been used in ConstantGuard since April 2013. WhiteSky argues that the screenshot provided by StrikeForce purporting to display the implementation of CryptoColor in a WhiteSky security product with a third party is not even the current version of the ConstantGuard, providing its own evidence that the ConstantGuard version available for download on May 8, 2013 did not contain field highlighting at all.

Based on the evidence provided to this Court, Plaintiff cannot demonstrate an imminent threat of disclosure or misappropriation of trade secrets, without which an injunction may not issue. See Continental Group, Inc. v. Amoco Chem. Corp., 614 F.2d 351, 358-59 (3d Cir. 1980); E.R. Squibb & Sons, Inc. v. Hollister, Inc., No. 91-203 (JCL), 1991 WL 15296, at *10-11 (D.N.J. Feb. 5, 1991). The Third Circuit has held that to satisfy the standard for obtaining a preliminary injunction, the moving party must demonstrate that there is an "imminent threat of the allegedly harmful disclosure." Continental Group, 614 F.2d at 358-59. Here, Plaintiff has not demonstrated that Defendant misappropriated its trade secrets or that the allegedly confidential information concerning StrikeForce anti-keylogging applications and methodologies has been divulged by Whitesky to a competitor of Plaintiff or other third party. Nor has it provided evidence that there is an imminent threat of misappropriation. Without a clear

demonstration by Plaintiff of actual misappropriation of trade secrets or, at the very least, an imminent threat of such unlawful use or disclosure, the Court cannot conclude that Plaintiff has satisfied the requirement that it is likely to succeed on the merits of its trade secrets claims.

C. Irreparable Harm

Related to the lack of proof concerning misappropriation, the motion for relief under Rule 65 also fails for insufficient evidence that StrikeForce faces irreparable harm if WhiteSky is not enjoined from disclosing and/or improperly using StrikeForce's trade secrets. A mere risk of harm is not enough. In a case involving the alleged disclosure of trade secrets and confidential information, the Third Circuit described the high standard required to enjoin a threatened misappropriation:

> [M]ore than a risk of irreparable harm must be demonstrated. The requisite for injunctive relief has been characterized as a clear showing of immediate irreparable injury, or a presently existing actual threat; [an injunction] may not be used simply to eliminate a possibility of a remote future injury, or a future invasion of rights . . .[i]njunctions will not be issued merely to allay the fears and apprehensions or to soothe the anxieties of the parties. Nor will an injunction be issued to restrain one from doing what he is not attempting and does not intend to do.

Continental Group, Inc., 614 F.2d at 359 (internal citations and quotations omitted).

As set forth above, Plaintiff has not demonstrated that WhiteSky has used or intends to use proprietary, confidential information belonging to StrikeForce. There is no proof that WhiteSky has incorporated or will incorporate aspects of the StrikeForce software or anti-keylogging and encryption trade secrets into its products which use the anti-keylogging software of a third party, such as its ConstantGuard product containing Zemana software. StrikeForce has not established that the field highlighting displayed when the non-StrikeForce version of ConstantGuard was in use implemented the CryptoColor feature or had been created using

StrikeForce's confidential anti-keylogging knowledge. Nor has it established that there is an imminent and actual danger that WhiteSky will misuse or disclose any such protected trade secrets. In short, a preliminary injunction is not warranted for the additional reason that Plaintiff has not demonstrated that a violation of its rights will occur and/or continue absent the injunction.

III. CONCLUSION

For the foregoing reasons, Plaintiff's motion for a preliminary injunction pursuant to Rule 65 will be denied. An appropriate Order will be filed.

s/Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

Dated: June 11, 2013