

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION**

PIXSYS TECHNOLOGIES, INC.,)
)
Plaintiff,)
)
vs.)
)
AGEMNI, L.L.C.,)
)
Defendant.)

Case No. 2:13-CV-1929-SLB

MEMORANDUM OPINION

This case is presently before the court on plaintiff’s Motion for Temporary Restraining Order. (Doc. 3.)¹ Plaintiff seeks a TRO against defendant to temporarily enjoin it “from accessing, logging on to, otherwise viewing or obtaining data or information from any computer or computer system owned, operated, or leased by [plaintiff]” and “from using any knowledge, information, or data obtained by accessing or logging on to, or otherwise resulting from unauthorized access to, any such restricted Pixsys computer system.” (Doc. 3 at 1-2.) A hearing was held on October 21, 2013, before the unsigned, which counsel for both parties attended.

On October 18, 2013, plaintiff filed a Verified Complaint, which asserts the following facts:

- 2. Pixsys is a corporation organized under the laws of the State of Alabama, with its principal place of business in Vestavia Hills, Alabama.

¹Reference to a document number, [“Doc. ____”], refers to the number assigned to each document as it is filed in the court’s record.

3. Agemni is a limited liability company organized under the laws of the State of Utah. . . .

. . .

8. Pixsys is a cloud-based software designer and provider headquartered in Vestavia Hills, Alabama, focused on the installation and repair industry [footnote] for DISH satellite television. Pixsys has developed a software package, called Dish Operations, that enables service providers throughout the United States for DISH to manage their businesses, in particular back-office functions of such businesses, more efficiently and profitably. Dish Operations is “enterprise” software, in that it provides functionalities affecting all aspects of a customer’s business, including work order management, inventory, payables and receivables, employee recruitment and retention, basic human resources, and business and employee performance and productivity.

[Footnote:] There are two broad categories of independently-owned installation and repair service providers for DISH Network: Regional Service Providers with an exclusive service territory and (2) subcontractors who do not have an exclusive service territory and are typically smaller than Regional Service Providers. Both categories are collectively referred to herein as “service providers.”

9. Dish Operations is the product of extensive, long-term development effort by Pixsys, brought about by its long-term affiliation with a DISH Regional Service Provider, and by painstaking trial-and-error in determining the optimal features and their configuration for DISH service provider needs. Many aspects of Dish Operations are proprietary to Pixsys, including some or all of its inventory tracking, return authorization, and personnel hiring functions. Even such features as might not be proprietary standing alone are proprietary in their configurations and combinations.

10. The configuration and combination of features embodied in the Dish Operations software are not publicly known (outside of Pixsys’[s] Dish Operations customers, who receive and use the software pursuant to agreements strictly requiring user confidentiality and granting a limited license to use the software), and cannot readily be ascertained in the DISH support software business. The Dish Operations software, and its configuration and

combination of features, have significant economic value, and have been the subject of significant efforts to guard their secrecy.

11. Pixsys'[s] customers receive a license from Pixsys to use the software and are provided access to it via the Internet. Customers must have valid credentialing and passwords in order to have access to their Pixsys accounts and thus to Dish Operations. Apart from a login screen and public-facing job application screens, Dish Operations is not accessible without proper password credentialing.

12. Pixsys'[s] customers are granted a license to use Dish Operations pursuant to Subscription Agreements. Such Agreements prohibit the customers from licensing, reselling, distributing or otherwise making the software available to third parties. The Agreements also require customers to maintain the confidentiality of all passwords assigned to them, prohibit the sharing of passwords with third parties, and prohibit the use of passwords by more than one individual. In addition to limiting access by password, access to Dish Operations is further limited based on the individual user's role within the company. For example, technicians may access only that small subset of the Dish Operations functionality relevant to their job. Higher level managerial or executive employees, referred to internally as "power users," are given broader access to Dish Operations.

13. Agemni is a competitor of Pixsys in the provision of software to the DISH installation, service and repair industry. Historically, its software has lacked much of the functionality of Dish Operations. Historically, Agemni has had a lesser share of the software market for DISH Regional Service Providers than Pixsys. Over the last year, several Agemni customers have switched to Pixsys software, while no Pixsys customers have switched to Agemni software.

14. Among Pixsys'[s] customers is Southern Star, Inc. ("SSI"), a DISH Network Regional Service Provider with a territory including parts of Texas, Oklahoma and Arkansas. SSI is licensed to access and use Dish Operations through its affiliate, JF Leasing, LLC ("JFL"), under a Subscription Agreement with Pixsys. Under that Agreement, JFL (and SSI, which has operated under that Agreement) agreed that it would not transfer, distribute, or make available the Dish Operations software to any third party, would keep confidential all confidential information made available to it pursuant to the Agreement, and would not use the software for any non-authorized purpose.

JFL (and through it, SSI) also agreed that it would maintain as confidential, and not share, any password made available to it pursuant to the Agreement.

15. The Vice President of Administration of SSI is, and has at all relevant times been, an individual named Randy Reed. Reed has at all relevant times had a password and authorization to access and use the Dish Operations software in SSI's business. As an executive level employee of SSI, Reed had been granted "power user" access rights to Dish Operations.

16. For reasons unknown to Pixsys, and commencing at some time in 2013 but not known by Pixsys until very recently, Agemni has repeatedly accessed Dish Operations through SSI's customer account, using Randy Reed's credentials and password. This access by Agemni (emanating from one or more Agemni IP addresses) has amounted to hundreds of page views to private areas of Pixsys'[s] software, not viewable by the public or anyone lacking valid credentials. These logins have also been focused heavily on Dish Operations features which Agemni's software product does not offer. This access has been done without the knowledge or consent of Pixsys, in violation of the law, and in violation of the Subscription Agreement referenced in the preceding paragraph. Such access has made available to Agemni details, process flows, business know-how, configurations and combinations of features and functions of Dish Operations.

17. On information and belief, Randy Reed or some other individual or individuals within SSI provided the Randy Reed log-in credentialing and password to an individual or individuals within Agemni, allowing the above-described industrial espionage and theft to take place.

18. On October 11, 2013, Agemni's Chief Financial Officer, Erik Felsted, sent the following email to a Pixsys customer. (The "to" and "cc" lines in the email, and its salutation, have been redacted.)

From: Erik Felsted
Date: October 11, 2013 at 4:21:22 PM CDT
To:
Cc:
Subject: Thank you

I don't know if you had heard but the largest RSP Southern Star is switching from Pixsys to AgemniST at the end of this year.

We have been working with them for several months confidentially (so I couldn't tell you this earlier) on making tons of enhancements that I know our clients will love. I wouldn't be surprised if we don't see more of the larger RSPs and DNS companies switching or coming back as the case may be after all of these new features are rolled out so they don't have to share their information with a competitor.

We will be here for you if you need anything.

Best regards,

Erik

19. Prior to the sending of this email (which states that Agemni has been "working with" SSI "for several months . . . confidentially"), Agemni had accessed Pixsys'[s] Dish Operations software through unauthorized use of Randy Reed's credentialing and password on multiple occasions, from one or more Agemni IP addresses, amounting to hundreds of page views, including in areas as to which Agemni's software historically has had no or limited functionality.

20. Agemni would not have been able to make the "tons of enhancements" in its software, within the time frame in which it apparently has, had it not unlawfully and impermissibly taken and used proprietary, confidential and trade secret information belonging to Pixsys.

(Doc. 1 ¶¶ 2-3, 8-20.)

Rule 65(b) provides:

The court may issue a temporary restraining order without written or oral notice to the adverse party or its attorney only if:

(A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and

(B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.

Fed. R. Civ. P. 65(b)(1). The Eleventh Circuit has held:

The purpose of a temporary restraining order, like a preliminary injunction, is to protect against irreparable injury and preserve the status quo until the district court renders a meaningful decision on the merits. *Canal Auth. of State of Florida v. Callaway*, 489 F.2d 567, 572 (5th Cir. 1974). A district court may grant a preliminary injunction only if the moving party shows that:

- (1) it has a substantial likelihood of success on the merits;
- (2) irreparable injury will be suffered unless the injunction issues;
- (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and
- (4) if issued, the injunction would not be adverse to the public interest.

Klay v. United Healthgroup, Inc., 376 F.3d 1092, 1097 (11th Cir. 2004); *Suntrust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257, 1265 (11th Cir. 2001). A preliminary injunction is “an extraordinary and drastic remedy” and is “not to be granted unless the movant ‘clearly established the burden of persuasion’ as to the four prerequisites.” *United States v. Jefferson County*, 720 F.2d 1511, 1519 (11th Cir. 1983)(quoting *Canal Auth. of State of Florida*, 489 F.2d at 573).

Schiavo ex rel. Schindler v. Schiavo, 403 F.3d 1223, 1232 (11th Cir. 2005). For the reasons set forth below, the court finds that plaintiff has shown the Motion for Temporary Restraining Order is due to be granted.

A. Likelihood of Success on the Merits

Plaintiff’s Verified Complaint contains claims for (1) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (2) violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201, (3) violation of Alabama’s Trade Secrets Act, Ala. Code § 8-27-1, et seq., (4)

violation of Alabama’s Digital Crime Act, Ala. Code § 13A-8-112, (5) common-law tortious interference with business relations, (6) common-law conversion, and (7) common-law trespass. Given the facts set forth in the Verified Complaint, the court finds that plaintiff has established a likelihood of success on the merits of its claims. Specifically, as asserted by plaintiff, defendant used a password without authorization to access, copy, and use for its own unauthorized purposes plaintiff’s proprietary and copyright protected material – the Dish Operations systems, its configuration, and combination of features. If true this unauthorized access, taking, and use provides the basis for finding defendant liable for violations of the Computer Fraud and Abuse Act,² the Digital Millennium Copyright Act,³ and Alabama’s Trade Secrets Act.⁴

²The Computer Fraud and Abuse Act is violated whenever an individual (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer” 18 U.S.C. § 1030(a)(2)(C).

³The Digital Millennium Copyright Act provides, “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.” 17 U.S.C. § 1201(a)(1)(A).

⁴The Alabama Trade Secrets Act states:

A person who discloses or uses the trade secret of another, without a privilege to do so, is liable to the other for misappropriation of the trade secret if:

(1) That person discovered the trade secret by improper means;

...

(3) That person learned the trade secret from a third person, and knew or should have known that (i) the information was a trade secret and (ii) that the

Therefore, the court finds plaintiff has show a substantial likelihood of success of the merits as to these claims.

B. Immediate and Irreparable Injury

In order to satisfy the requirements for a TRO, plaintiff must “show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition” – that is, plaintiff “will suffer irreparable injury and that the irreparable injury is of such imminence that there is a clear and present need for equitable relief to prevent harm.” *Taxsalelists.com, L.L.C. v. Rainer*, Civil Action No. 09-CV-02898 REB-KMT, 2009 WL 4884273, *3 (D. Colo. Dec. 11, 2009)(citing *Heiddeman v. S. Salt Lake City* 348 F.3d 1182, 1189 (10th Cir. 2003)). As set forth in the Verified Complaint, plaintiff asserts that defendant has taken its proprietary and copyright protected computer software package and is using or will use such property to compete with plaintiff. “Particularly when documents such as database information that is the foundation of [plaintiff’s] business . . . are being used improperly by one or more competing enterprises, and the evidence in this case indicates such information is being used improperly in such a

trade secret had been appropriated under circumstances which violate the provisions of (1) or (2), above

Ala. Code § 8-27-3. “A ‘trade secret’ is information that: a. Is used or intended for use in a trade or business; b. Is included or embodied in . . . computer software . . .; c. Is not publicly known and is not generally known in the trade or business of the person asserting that it is a trade secret; d. Cannot be readily ascertained or derived from publicly available information; e. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy; and f. Has significant economic value.” Ala. Code § 8-27-2.

fashion, [plaintiff] will suffer injuries that are irreparable because they are difficult or impossible to measure.” *Id.* Damage to plaintiff’s relationships with its clients and its position in the marketplace are virtually impossible to calculate and to remedy. *See Hal Wagner Studios, Inc. v. Elliott*, No. 09-CV-0031-MJR, 2009 WL 102435, *6 (S.D. Ill. Jan. 15, 2009).

Therefore, the court finds that plaintiff has shown that it will suffer immediate and irreparable injury if defendant’s unauthorized access and/or use of its software is not enjoined.

C. Balance of Harms

Plaintiff must show that its “threatened injury . . . outweighs whatever damage the proposed injunction may cause [defendant].” *Four Seasons Hotel and Resorts v. Consorcio Barr, S.A.*, 320 F.3d 1205, 1210 (11th Cir. 2003). The Verified Complaint shows that defendant had no authority to access and/or use the Dish Operations software. Therefore, defendant “will suffer no harm that is recognized in law if [it is] prohibited from unlawfully obtaining information from [plaintiff] and from using information to which [it has] no legal right or which [it has] no legal right to use to support competing enterprises or to conduct a competing enterprise.” *See Taxsalelist.com*, 2009 WL 4884273 at *3. Therefore, the harm to plaintiff outweighs any harm to defendant.

D. Public Interest

Nothing before the court indicates any public interest that would be harmed by enjoining defendant's unlawful access and use of plaintiff's software. Therefore, this factor weighs in favor of granting plaintiff's requested TRO.

E. Certificate of Counsel

Counsel for plaintiff served the Verified Complaint and Motion for Temporary Restraining Order on defendant on October 18, 2013. Over the weekend, defendant contacted attorneys in Alabama to represent them in this matter at the hearing. However, given the short period of time between service and this hearing, defendant's ability to meaningfully respond to plaintiff Motion was limited. Nevertheless, the court finds that plaintiff has established its injury is imminent and irreparable; therefore, temporary injunctive relief is appropriate.

F. Bond

“The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” Fed. R. Civ. P. 65(c). “The amount of security required is a matter for the discretion of the trial court; it may elect to require no security at all.” *Corrigan Dispatch Co. v. Casa Guzman, S.*

A., 569 F.2d 300, 303 (5th Cir. 1978).⁵ Plaintiff asks for a bond of no more than \$10,000. Defendant argues that a bond of \$ 50,000 to \$100,000 is appropriate in this case.

Given the limited life span of a TRO the court finds a relatively small bond is appropriate. Therefore, the court will require plaintiff to post a bond of \$5,000. The amount of the bond will be revisited at the time set for the preliminary injunction hearing.

Based on the foregoing, the court finds that plaintiff is entitled to a TRO prohibiting defendant from accessing, taking, and/or using plaintiff's Dish Operations software. An Order granting plaintiff's Motion for Temporary Restraining Order will be entered contemporaneously with this Memorandum Opinion.

DONE, this 22nd day of October, 2013.



SHARON LOVELACE BLACKBURN
CHIEF UNITED STATES DISTRICT JUDGE

⁵Decisions of the former Fifth Circuit Court of Appeals rendered prior to October 1, 1981, constitute binding precedent in the Eleventh Circuit. *Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir.1981) (en banc).