

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge Christine M. Arguello**

Civil Action No. 10-cv-00109-CMA-MEH

ASSOCIATIONVOICE, INC.,

Plaintiff,

v.

ATHOMENET, INC.,
JEFFREY T. SANDERS,
SUSAN D. SANDERS, and
IMARI ADAMS,

Defendants.

**ORDER GRANTING IN PART AND DENYING IN PART PLAINTIFF'S MOTION FOR
A PRELIMINARY INJUNCTION AND DENYING PLAINTIFF'S MOTION TO STRIKE**

This matter is before the Court on Plaintiff AssociationVoice, Inc.'s ("Plaintiff") Second Renewed Motion for Preliminary Injunction (Doc. # 124) and Plaintiff's Motion to Strike Non-Record Evidence From Defendants' Proposed Findings of Fact and Conclusions of Law. (Doc. # 179.) For the following reasons, Plaintiff's motion for a preliminary injunction is granted in part and denied in part, and Plaintiff's motion to strike is denied.

I. BACKGROUND

A. FACTUAL BACKGROUND

Plaintiff and Defendant AtHomeNet, Inc. ("AHN") offer competing web-based HOA software applications. Plaintiff offers various features as part of its application.

Much of the features' functionality is found in the password-protected "site admin" areas of Plaintiff's application. Plaintiff alleges that access to the "site admin" areas can significantly reduce the time it takes a competitor to develop similar features. Accordingly, Plaintiff only permits authorized users who are bound by confidentiality agreements to access the "site admin" areas of Plaintiff's application.

Beginning in November 2007, Defendants AHN, Jeffrey Sanders, Susan Sanders, and Imari Adams (collectively, "Defendants") falsely claimed to be and acted as a legitimate HOA customer of Plaintiff in order to purchase Plaintiff's application and obtain access to the password-protected "site admin" areas. Acting as the fictitious HOA "Landings East," Defendants entered into a Services Agreement ("Services Agreement" or "Agreement") with Plaintiff.¹ (Doc. # 124-10, Services Agreement.) The Agreement prohibits Defendants from, among other things, reverse engineering and copying Plaintiff's source code or the processes and algorithms underlying the source code (*id.* at 3, § 8) or using Plaintiff's proprietary and confidential information. (*Id.* at 2, § 7).

Plaintiff contends Defendants engaged in the above conduct to obtain information about the features available in the "site admin" areas of Plaintiff's application. Defendants, on the other hand, contend they did so for three reasons, the

¹ The Services Agreement was signed by Defendant Adams under a pseudonym and on behalf of a non-existent HOA. The Defendants, however, do not dispute that the actions of Defendant Adams are attributable to AHN and that all Defendants are bound by the Services Agreement. (Doc. # 131, Defs.' Resp. at 2; Doc. # 124 at 15 n.2.)

first being to learn about Plaintiff's integration of its application with software provided by TOPS, a third party who is a software database provider for a large portion of the parties' potential customers. AHN and TOPS have an exclusive arrangement, through which AHN alone integrates its application with TOPS's databases. Because TOPS is a popular provider of database services to the parties' potential customers, Defendants consider this exclusive relationship valuable in distinguishing themselves from the competition. Thus, when Plaintiff began advertising that its application had the ability to integrate with TOPS's databases, Defendants wanted to investigate Plaintiff's claims. Plaintiff alleges Defendants obtained information about the TOPS integration by February 2008, yet continued to access the protected "site admin" areas of Plaintiff's application for almost two additional years. In addition to investigating Plaintiff's integration with TOPS, Defendants contend they accessed the "site admin" portions to respond to prospective customers' inquiries about the features offered by the respective parties and to prepare comparative marketing materials.

During the time defendants were accessing Plaintiff's application, AHN allegedly added at least 44 new features to its application, which Plaintiff alleges are substantially similar to those features found in the password-protected "site admin" areas of its own application. (Doc. # 1, Compl., ¶ 42; Doc. # 173-1, Pl.'s Suppl. Brief at 8, ¶¶ 27-31.) Plaintiff alleges Defendants copied these features. (Doc. # 124.)

B. PROCEDURAL BACKGROUND

At the time Plaintiff filed its Complaint, Plaintiff also filed a motion for preliminary injunction. (Doc. ## 1, 2.) In the Complaint, Plaintiff asserts multiple causes of action, including, *inter alia*, violation of the Computer Fraud and Abuse Act (“CFAA”), copyright infringement, fraud, misappropriation of business value, trade secret misappropriation, and breach of the parties’ Services Agreement. (Doc. # 1.) On June 7, 2010, as requested by the Court, Plaintiff filed additional briefing entitled Renewed Motion for Entry of Preliminary Injunction. (Doc. ## 85, 88.) The Court denied the renewed motion for Plaintiff’s failure to adhere to Court’s 15-page limitation. (Doc. # 98.) The Court did, however, allow Plaintiff to file a renewed motion of up to twenty (20) pages. (Doc. # 100.) On July 1, 2010, Plaintiff filed its corrected renewed motion. (Doc. # 109.) Although the brief itself was only 20 pages long, Plaintiff filed a separate 36-page “Evidentiary Appendix” which Plaintiff admitted amounted to the facts section of its brief. (Doc. # 105.) As such, the Court struck the corrected renewed motion for violating the Court’s page limitation. (Doc. # 122.) On August 9, 2010, Plaintiff filed its Second Renewed Motion and associated exhibits. (Doc. # 124.) It is this motion that currently is before the Court.

Defendants AHN, Jeffrey Sanders, and Susan Sanders opposed this motion on August 24, 2010. (Doc. # 131.) Defendant Imari Adams (“Adams”) filed a separate opposition the same day. (Doc. # 134.) Plaintiff filed its reply on September 10, 2010.

(Doc. # 136.) Expedited discovery related to the preliminary injunction issues closed two weeks later on September 24, 2010. (Doc. # 37.)

In its motion, Plaintiff seeks two preliminary injunctions. The first is sought under Plaintiff's claims related to the CFAA and would enjoin Defendants from accessing the password-protected "site admin" areas of Plaintiff's application ("CFAA Injunction").

The second injunction is premised on Plaintiff's claims for breach of the parties' Services Agreement. Plaintiff asks that AHN be enjoined from providing its customers with 20 features that it allegedly reverse engineered, copied or misappropriated in breach of the parties' Services Agreement ("Breach of Contract Injunction"). (Doc. # 173-1, Pl.'s Suppl. Brief at 19, ¶¶ 59-60.)

The Court held an evidentiary hearing on November 2, 2010, and November 18, 2010. The Court allowed the parties to file supplemental briefing to address the evidence presented at the hearing and to submit proposed findings of fact and conclusions of law. The parties filed their respective submissions on December 3, 2010. (Doc. ## 173-74.)

Although Plaintiff initially moved to enjoin AHN's use of the 44 features identified in the Complaint, Plaintiff later withdrew 24 features from the requested injunction and conceded that the evidence presented was not sufficient to satisfy its burden with respect to five of the remaining 20 features. Thus, only 15 features are subject to the motion for preliminary injunction. (Doc. # 173-1, Pl.'s Suppl. Brief at 10, ¶ 31.)

Plaintiff has also moved to strike Defendants' references to certain evidence on the grounds that such evidence was not presented at the preliminary injunction hearing. (Doc. # 179.)

II. MOTION TO STRIKE

As a threshold matter, the Court must determine what evidence is properly before the Court on Plaintiff's motion for a preliminary injunction. Plaintiff first moves to strike Defendants' reliance on the affidavits of Defendants' expert Russell L. Parr (Doc. # 131-2, Parr Aff.) and Defendant Susan Sanders (Doc. # 131-4, Sanders Aff.) and the deposition testimony of Plaintiff's president, Drew Regitz. (Doc. # 131-5, Regitz Dep. Tr.) Plaintiff argues "the only evidence relevant to the determination of its preliminary injunction motion is the evidence adduced at the preliminary injunction hearing, in the form of the testimony provided by the witnesses and the exhibits admitted by the Court," with one exception. The one exception is that Defendants may cite to portions of Mr. Regitz's deposition testimony for purposes of impeachment. (Doc. # 179, Pl.'s Motion Strike, ¶ 1.) Thus, Plaintiff claims Defendants' reliance on such evidence is improper.

The Court is not persuaded. "A hearing for preliminary injunction is generally a restricted proceeding, often conducted under pressured time constraints, on limited evidence and expedited briefing schedules." *Heideman v. South Salt Lake City*, 348 F.3d 1182, 1188 (10th Cir. 2003). As such, the Federal Rules of Evidence do not apply to such hearings. *Id.* While the preliminary injunction hearing in this case was

conducted after the close of discovery, it was subject to the same time constraints as most preliminary injunction proceedings. The evidence to which Plaintiff objects was adduced prior to the hearing and was submitted by Defendants in connection with their response to the motion for preliminary injunction. Consequently, Plaintiff was on notice that Defendants considered the evidence relevant and had the opportunity to rebut that evidence either at the hearing or with the submission of exhibits to its own briefing. Accordingly, the affidavits of Mr. Parr and Mrs. Sanders and the deposition testimony of Mr. Regitz can be considered by the Court on Plaintiff's motion for a preliminary injunction.

Second, Plaintiff objects to Defendants' citation to the rough transcript of the preliminary injunction hearing because the transcript "constitutes merely the court reporter's own notes of the proceedings and is therefore not an official record of anything." (Doc. # 179 at 2, n.1.) However, the Court allowed supplemental briefing for the sole purpose of allowing the parties to address the evidence presented at the hearing. While the transcript was not a final draft, due to the time constraints surrounding the proceeding, Defendants' citation to it was appropriate and helpful to the Court.

For the foregoing reasons, the Court denies Plaintiff's motion to strike.

III. ENTRY OF A PRELIMINARY INJUNCTION

The primary issue before the Court is whether Plaintiff has met its burden to support the issuance of a preliminary injunction.

To obtain a preliminary injunction, the moving party must establish that:

- (1) it will suffer irreparable injury if the preliminary injunction is not granted;
- (2) its threatened injury outweighs any harm caused to the opposing party as a result of the injunction;
- (3) the injunction is not adverse to the public interest; and
- (4) it has a substantial likelihood of success on the merits.

Beltronics USA, Inc. v. Midwest Inventory Distribution, LLC, 562 F.3d 1067, 1070 (10th Cir. 2009). “As a preliminary injunction is an extraordinary remedy, the right to relief must be clear and unequivocal.” *Schrier v. University of Colo.*, 427 F.3d 1253, 1258 (10th Cir. 2005). The “limited purpose” of a preliminary injunction “is merely to preserve the relative positions of the parties until a trial on the merits can be held.” *Univ. of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981).

“When a party seeking a preliminary injunction satisfies the first three requirements, the standard for meeting the fourth ‘probability of success’ prerequisite becomes more lenient. The movant need only show questions going to the merits so serious, substantial, difficult and doubtful, as to make them a fair ground for litigation.” *Resolution Trust Corp. v. Cruce*, 972 F.2d 1195, 1199 (10th Cir. 1992). This has been termed the “modified likelihood-of-success-on-the-merits standard.”

A. DISFAVORED INJUNCTIONS

Given the “limited purpose” of preliminary injunctions, the Tenth Circuit has identified certain disfavored injunctions that are subject to more intense scrutiny:

- (1) preliminary injunctions altering the status quo,
- (2) mandatory preliminary injunctions,
- and (3) preliminary injunctions granting the moving party all the relief it could recover at

the conclusion of a full trial on the merits. *O Centro Espirita Beneficente Uniao Do Vegetal v. Ashcroft*, 389 F.3d 973, 975 (10th Cir. 2004) (*en banc*), *cert. granted sub nom on other grounds, Gonzales v. O Centro Espirita Beneficente Uniao Do Vegetal*, 544 U.S. 973 (2005). Disfavored injunctions “must be more closely scrutinized to assure that the exigencies of the case support the granting of a remedy that is extraordinary even in the normal course.” *Id.* When a movant seeks a disfavored injunction, it must make a “strong showing” that the four injunction factors weigh in its favor. *Id.* at 976.

The requested CFAA Injunction (enjoining access to the “site admin” areas) is a prohibitory injunction that maintains the status quo. Accordingly, it is subject to the traditional standard. On the other hand, the Breach of Contract Injunction (requiring removal from Defendants’ software of the features allegedly developed using misappropriated know how) is disfavored because it would require Defendants to take the affirmative step of removing application features. As a result, Plaintiff must make a strong showing on each of the preliminary injunction factors to be entitled to such injunctive relief.

B. THE PRELIMINARY INJUNCTION FACTORS

For the following reasons, the Court finds that Plaintiff has satisfied the four preliminary injunction factors with respect to the injunction requested under the CFAA, but not with respect the injunction premised on the alleged breach of the Services Agreement.

1. Likelihood of Success

With respect to this factor, a movant must establish a “substantial likelihood of success” on the merits. *Resolution Trust*, 972 F.2d at 1198. “As a preliminary injunction is an extraordinary remedy, the right to relief must be **clear and unequivocal**.” *Schrier*, 427 F.3d at 1258 (emphasis added). The movant must carry the burden of persuasion by a “clear showing,” *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) (*per curiam*); accord *SCFIC ILC, Inc. v. Visa USA, Inc.*, 936 F.2d 1096, 1098 (10th Cir. 1991), or in the case of a disfavored injunction, a “strong showing.” *O Centro*, 389 F.3d at 976.

The Court finds that Plaintiff has established a substantial likelihood of success of prevailing on its claims that Defendants violated the CFAA, 18 U.S.C. § 1030, but has not made the sufficiently “strong showing” that Defendants breached the Services Agreement through reverse engineering and use of Plaintiff’s confidential and proprietary know how.

a) *The Computer Fraud and Abuse Act*

Plaintiff’s first and second claims for relief are for violations of the CFAA. (Doc. # 1, Compl.) Plaintiff alleges that Defendants violated two sections of the CFAA, §§ 1030(a)(2)(C) and (a)(4). Section 1030(a)(2)(C) provides:

[Whoever] intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished.

18 U.S.C. § 1030(a)(2)(C). Section 1030(a)(4) provides:

[Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . shall be punished.

18 U.S.C. § 1030(a)(4).

Although the CFAA was initially enacted as a criminal statute, the CFAA provides for a private right of action if the alleged violation involves one of five specified elements. 18 U.S.C. §§ 1030(g) and (c)(4)(A)(i). The additional element at issue in this case is “loss” to the plaintiff during any 1-year period aggregating at least \$5,000. (Doc. # 124 at 4.) “Loss” is an element of both of Plaintiff’s CFAA claims. The Act defines “loss” as:

any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11).

The parties’ dispute surrounding Plaintiff’s CFAA claims centers on two elements: (1) whether Defendants’ access was unauthorized and (2) whether Plaintiff suffered a “loss” as defined by the statute.

(i) Unauthorized Access

The first element of Plaintiff’s CFAA claims concerns whether Defendants’ access to Plaintiff’s application was authorized. In their briefing and at the preliminary injunction hearing, Defendants concede their access to the Landings East website was

not authorized. Defendants contend, however, that their member-level access to Plaintiff's publicly available Castle Breckenridge site and Plaintiff's website for the Austin chapter of the Community Associations Institute ("CAI-Austin"), to which AHN is a member, was authorized. (Doc. # 174, Defs.' Suppl. Resp. at 11, ¶ 31-32.)

The evidence presented at the hearing indicates Defendants accessed only the member-level portions of these sites. Defendants' access to the member-level portions is not relevant to the instant motion. Plaintiff seeks a preliminary injunction enjoining Defendants' access to the "site admin" portions of Plaintiff's application, and the injunction is directed to features that can only be reviewed in their entirety through the "site admin" areas. (Doc. # 173-1, Pl.'s Suppl. Brief at 8-9, ¶ 28.) However, even if such member-level access is relevant, Plaintiff has not proffered any evidence demonstrating that Plaintiff did not authorize Defendants to access these sites in this way.

Defendants also claim their access to the "site admin" portions of the websites Plaintiff hosts for various customers was at the invitation of those customers for the purpose of moving the customers' content from Plaintiff's application to AHN's application. (Doc. # 174, Defs.' Suppl. Resp. at 11, ¶ 33.) However, Plaintiff has proffered evidence suggesting the customers did not have the right to authorize Defendants' access for this limited purpose. (Doc. # 136-1, Regitz Suppl. Dec., ¶¶ 1-6.) Therefore, the Court finds that Plaintiff has demonstrated a likelihood of success at trial that Defendants accessed, without authorization, the "site admin" portions of the

Landings East website and those websites belonging to various customers. However, Plaintiff has not demonstrated a likelihood of success with respect to the Castle Breckenridge or CAI-Austin sites.

(ii) *The Meaning of “Loss”*

The parties dispute two issues concerning the second element of “loss.” They first dispute the interpretation of the statute’s definition of the term. Plaintiff’s position is that the term includes costs associated with an investigation and assessment of the offender’s identity and access, irrespective of whether they relate to an interruption of Plaintiff’s service. (Doc. # 124.) Defendants take the contrary position. Defendants also argue that, even if Plaintiff’s interpretation is correct and an interruption of service is not a prerequisite, many of Plaintiff’s costs should not be considered a “loss” because they were not related to damage to Plaintiff’s application. (Doc. # 131, Defs.’ Resp. at 16-18.)

The Court agrees with the interpretation proffered by Plaintiff and adopted by a majority of courts. Costs do not need to relate to an “interruption of service” in order to fall within the ambit of “loss.” See, e.g., *A.V. v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009) (“This broadly worded provision plainly contemplates consequential damages of . . . costs incurred as part of the response to a CFAA violation, including the investigation of an offense.”); *Res. Ctr. for Indep. Living v. Ability Res., Inc.*, 534 F. Supp. 2d 1204, 1211 (D. Kan. 2008) (finding allegations of “loss of confidential and proprietary information for the benefit of defendants’ competing enterprise” sufficient to

withstand a motion to dismiss); *NCMIC Fin. Corp. v. Artino*, 638 F. Supp. 2d 1042, 1064 (S.D. Iowa 2009) (finding that “losses” include responding to a security breach, even if there is no change to the computers or the information contained thereon); *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008) (rejecting the defendant’s argument that the “[c]ost of investigating and trying to locate the perpetrator is not included as a qualifying type of loss”); *Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F. Supp. 2d 1026, 1036 (N.D. Ill. 2008) (noting that courts have held that “costs incurred to assess and repair damage” are recoverable “regardless of whether there is an interruption of service”); *see also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001) (finding that the meaning of the term “loss” prior to the inclusion of the statutory definition included diagnostic measures).

Additionally, the Court agrees with Plaintiff that actionable losses include costs associated with an investigation undertaken to determine the identity of and methods used by an offender and the extent of the offender’s access. The Court reaches this conclusion for multiple reasons. First, the plain language of the Act itself distinguishes between those losses that are a result of an interruption of service and those that are not. Specifically, the Act defines “loss” as the “cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense **and** any revenue lost, cost incurred, or other consequential damages incurred **because of interruption of service.**” 18 U.S.C.

§ 1030(e)(11) (emphasis added). Only those costs in the second half of the definition need to relate to an interruption of service. Costs that need not relate to an interruption include “the cost of responding to an offense” and “conducting a damage assessment.”
Id.

Second, while the statutory language is unambiguous, the legislative history also shows that the Act proscribes actions that do not result in *any* damage or interruption of service, including actions similar to those at issue in this case. In discussing the need for legislation directed to computer fraud, the House Report identified situations for which the then-current law was ineffective, and as such, for which the CFAA was designed to address. These situations included unauthorized access used to misappropriate a computer program even if no damage was done to the computer or the program. Specifically, the House Report states:

When a program of substantial commercial value is misappropriated, the person from whom it is stolen almost always remains in possession of the original. Indeed, the original program may not have been moved so much as a single inch while being illicitly copied. It is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes.

H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3695 (July 24, 1984). Because the legislative history contemplated such a situation as falling within the purview of the Act, Congress could not have intended for a plaintiff to have to prove an interruption of service, “damages,” or an assessment of “damages” to invoke the Act.

Third, the Court finds convincing the reasoning in *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008). The court recognized that in cases concerning damage to the computer itself, identifying the offender may be helpful but not essential to remedying or discovering the extent of the damage. In contrast, when the offense is accessing protected information for purposes other than causing damage, “discovering who has that information and what information he or she has is essential to remedying the harm.” *Id.* at 981 (finding the plaintiff established a likelihood of success on the merits of its CFAA claim). This is precisely the case we have here. The instant matter involves the accessing and the alleged reverse engineering and copying of protected information. In order to remedy this harm, it was necessary for Plaintiff to determine who was obtaining unauthorized access to its information, how they were accomplishing that access, and what they were doing with the information they obtained. The costs incurred from doing so result from responding to Defendants’ offense and thus are actionable “losses.” *Id.*

(iii) *Sufficiency of Plaintiff’s Evidence of “Loss”*

The second issue in dispute concerning “loss” is whether Plaintiff proffered sufficient evidence that it incurred at least \$5,000 in expenses.

To support its allegations of loss, Plaintiff submitted (1) an invoice from Cyopsis, Inc., a third-party forensic investigator whom Plaintiff hired to assist with its investigation and (2) information describing the steps Plaintiff’s employees took and the costs associated with the employees’ work. (Doc. # 124-16, Cyopsis Invoice; Doc. # 124-4,

Regitz Dec., ¶¶ 42-53; Doc. # 136-6, Spreadsheet of Time and Costs.) Defendants fault Plaintiff's evidence for not including a detailed description of the work each employee did and on which day. Defendants also argue that many of Plaintiff's costs should not be considered a "loss" because they were incurred after Plaintiff allegedly had "clearly identified" Defendant Adams as the offender. Because these costs were allegedly not necessary, Defendants characterize them as litigation expenses, not "losses." (Doc. # 131, Defs.' Resp. at 17-18.)

To begin, the Court rejects Defendants' argument that some costs are solely litigation expenses because they were not needed to identify Defendants. First, the evidence does not show that Plaintiff clearly identified Adams as the offender in October 2009. Plaintiff believed Adams was the offender based on a non-expert comparison of voice recordings, but non-expert voice analysis is not a clear identification of an offender. (Doc. #131-5, Regitz Dep. Tr. at 13:1-8.) Plaintiff acted reasonably in pursuing additional evidence of the offender's identity. Second, Defendants went to great lengths to hide their identity from Plaintiff. It, therefore, is not surprising that Plaintiff also had to go to great lengths to uncover Defendants' identity, as well as to uncover the extent of their unauthorized access and the methods they used. Accordingly, Defendants should not be allowed to complain about the costs Plaintiff incurred in doing so. Lastly, the amount of Plaintiff's expenses appears to be reasonable as it is in line with those incurred by plaintiffs in similar cases. *EF Cultural Travel*, 274 F.3d at 584 n.17 (finding that the \$20,944.92 paid to assess whether the

plaintiff's website had been compromised was a sufficient "loss"); *Artino*, 638 F. Supp. 2d at 1064-65 (finding \$11,193 resulted from remedial action and investigation into the defendant's conduct and therefore constituted a "loss").

The Court also finds the evidence submitted by Plaintiff sufficient to substantiate its costs. Plaintiff submitted a spreadsheet outlining the employees of Plaintiff who investigated the Defendants' access, the employees' calculated billable rates per hour, and the amount of time each spent on the investigation. (Doc. # 136-6, Spreadsheet of Time and Costs.) Plaintiff also submitted a declaration of its President attesting to the nature and timing of the investigation. (Doc. # 124-4, Regitz Dec., ¶¶ 42-49.) Moreover, Plaintiff made these employees available for deposition if Defendants desired additional information about how and when the time was spent. Defendants have proffered neither evidence nor argument that leads the Court to question the reasonableness or accuracy of Plaintiff's evidence.

In accordance with the foregoing, the Court finds that Plaintiff has a substantial likelihood of succeeding on its CFAA claims based on Defendants' access to the "site admin" portions of Plaintiff's application.

b) Breach of Contract

Plaintiff's ninth claim for relief is for breach of the parties' Services Agreement (Doc. # 1, Compl.) As noted, because the injunction related to this claim is disfavored, Plaintiff must make a "strong showing" that it has a substantial likelihood of success on the merits.

In its opening brief, Plaintiff contends that Defendants breached the Services Agreement when they “improperly used its unlawful access to obtain confidential information about [features available only in the password-protected ‘site admin’ areas of Plaintiff’s application] through reverse engineering, analyzing the underlying processes embedded in AV’s application and thereby violating the restrictions against the use of AV’s proprietary information contained in the Services Agreement.” (Doc. # 124 at 15.) In its supplemental briefing, Plaintiff contends that Defendants breached Sections 7 and 8 of the Services Agreement when they allegedly misappropriated the “know how” reflected in various features of Plaintiff’s application or when they reverse engineered those features. (Doc. # 173-1 at 20, ¶ 63.) Consistent with its opening brief, and in the absence of an indication to the contrary, the Court interprets such “know how” as the features’ underlying processes.

Although Defendants admit they used their access to the “site admin” portions to prepare comparative marketing materials, they deny they copied Plaintiff’s features or even used such access for the purpose of developing AHN’s competing application. (See Doc. # 173-1 at 4, ¶ 15.)

Section 8 of the Agreement concerns the “reverse engineering” of, among other things, Plaintiff’s source code and the processes and algorithms underlying the code. In pertinent part, Section 8 provides:

SUBSCRIBER will not permit any person or entity to copy, revise, alter, modify, decompile, reverse engineer, assemble, or attempt to discover . . . any AssociationVoice Property, including, without limitation, any object code,

source code, underlying processes or algorithms contained therein, other than as is permitted by AV in writing.

(Doc. # 124-10, Services Agreement at 3, § 8.) “AssociationVoice Property” is defined to include processes, systems, and tools which are subject to protection by the traditional intellectual property laws (*i.e.*, patent, copyright, trademarks, and trade secrets), but also those which are not. (*Id.* at 2-3, § 8.)

Section 7 prohibits Defendants from “us[ing] . . . or disclos[ing] . . . any Confidential Information.” “Confidential Information” is defined to include, without limitation, “information relating to a party’s business and marketing plans and . . . software, hardware and technology.” (*Id.* at 2, § 7.) Confidential Information, however, does not include “information (a) already known or independently developed by the recipient, (b) in the public domain through no wrongful act of the recipient, or (c) received by the recipient from a third party who was authorized to disclose it.” *Id.*

(i) Plaintiff’s Allegations of Copying

Plaintiff attempts to show Defendants misappropriated AHN’s confidential “know how” and reverse engineered AHN’s features by showing Defendants copied the implementation of Plaintiff’s features. (Doc. # 173-1, Pl.’s Suppl. Brief at 20-21, ¶ 63; Doc. # 124, Pl.’s Motion at 15.) Plaintiff explains that discovery generated only “limited direct evidence” of copying because Defendants do not maintain memoranda regarding the development of its software and because they regularly replaced some computers during the time in question. (Doc. #124 at 16.)

Because direct evidence of copying is limited, Plaintiff seeks to implicate a rule of copyright law to show with indirect evidence that Defendants copied Plaintiff's features. This rule traditionally comes into play in the context of a claim of copyright infringement which requires a showing of (1) ownership of a valid copyright, and (2) copying by the defendant of protected components of the copyrighted material. *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 831 (10th Cir. 1993). The rule provides for a rebuttable inference of the second factor, copying, if the evidence shows "(1) that the defendant had access to the copyrighted program, and (2) that there are probative similarities between the copyrighted material and the allegedly copied material." *Id.* at 832. "[W]here there is strong proof of access, the necessary showing of factual similarity will be relatively lower;" however, there must be "some showing of similarity." *Id.* at 833 n.9. Importantly, the defendant can rebut the inference of copying with evidence of independent creation. *Id.* at 833 n.8.

The undisputed evidence Plaintiff proffered on the extent of Defendants' access is substantial. The instances of access are discussed in detail in Plaintiff's opening brief. (Doc. # 124 at 16-18.)

With respect to the alleged similarity between the parties' corresponding features, Plaintiff compares the features available on the Landings East website with those AHN offered after accessing the Landings East site. (Doc. # 173-1, Pl.'s Suppl. Brief at 19-20, ¶¶ 61-62; Hearing Exhibits 116-122, 126-136.) Plaintiff then concludes the parties' respective features are substantially similar "in terms of meeting

substantially similar business requirements in a substantially similar fashion,” in other words, substantially similar in their overall function and underlying processes. (Doc. # 173-1 at 10, ¶ 32.)

In response, Defendants contend two of the 15 disputed features (setting status/disposition of submitted forms, 42.6.2, and reporting all changes made to directory listings, 42.8.7) have not been incorporated into *any* version of AHN’s application. (Doc. # 174, Defs.’ Suppl. Resp. at 15-16, ¶¶ 44-45; Doc. #131-4, Sanders Aff. at 4, ¶ 14.) As such, Defendants could not have copied these features.

Defendants also point to Plaintiff’s server logs that suggest one feature (saving content templates, 42.1.7) lacked the requisite access. Specifically, Plaintiff’s server logs do not show Defendants accessed the specific webpage that displayed this feature.

Lastly, Defendants criticize the use of the copyright approach to infer copying because such approach depends on the copied material being original to Plaintiff. (Doc. # 131, Defs.’ Resp. at 14.) In this regard, Defendants contend 12 of the remaining 15 features were available in AHN’s application (either Classic or Elite version) in some form or another prior to their accessing the Landings East website. (Doc. # 174, Defs.’ Suppl. Resp. at 13, ¶¶ 38-40, 42.) At the preliminary injunction hearing, Mrs. Sanders demonstrated for the Court the existence of some of these features in the 2007 version of AHN’s application.

(ii) Analysis

The Court agrees with Defendants that Plaintiff has not submitted sufficient evidence demonstrating Defendants copied the underlying processes or algorithms of Plaintiff's features. For some of the corresponding features, Defendants have shown similarity only in the overall function, not in the features' implementation. Thus, for these features, the Plaintiff is essentially asking the Court to apply a double inference, *i.e.*, to infer probative similarity in the underlying processes based on evidence of access and similarity in the features' overall functions, and then infer that AHN copied those processes. This, the Court cannot do. Although Plaintiff's evidence of access is substantial, it must show some similarity between the parties' underlying processes in order to infer copying of them. *Gates Rubber*, 9 F.3d at 833 n.9.

Furthermore, for those features in which substantial similarity arguably exists, Defendants have demonstrated either the absence of access to that particular feature, or that Defendants are likely to succeed in rebutting the presumption of copying with evidence of their independent development of the feature.

Accordingly, Plaintiff's ability to succeed on the merits of its breach of contract claim is questionable.² Plaintiff's evidence is not sufficient to meet the heightened burden it faces for this disfavored injunction.

² Nothing in this order concerns Plaintiff's ability to show a breach of the Services Agreement premised on conduct other than the alleged reverse engineering and copying of Plaintiff's know how.

2. Irreparable Injury

The showing of irreparable harm “is the single most important prerequisite for the issuance of a preliminary injunction.” Thus, the moving party must “first demonstrate that such injury is likely before the other requirements for the issuance of an injunction will be considered.” *Dominion Video Satellite, Inc. v. Echostar Satellite Corp.*, 356 F.3d 1256, 1261 (10th Cir. 2004).

“To constitute irreparable harm, an injury must be certain, great, actual and not theoretical The party seeking injunctive relief must show that the injury complained of is of such *imminence* that there is a clear and present need for equitable relief to prevent irreparable harm . . . [S]imple economic loss usually does not, in and of itself, constitute irreparable harm; such losses are compensable by monetary damages.” *Heideman v. South Salt Lake City*, 348 F.3d 1182, 1189 (10th Cir. 2003) (internal citations and quotations omitted). The following factors support irreparable harm determinations: (1) inability to calculate damages, (2) harm to goodwill, (3) diminishment of competitive positions in marketplace, and (4) lost opportunities to distribute unique products. *Dominion*, 356 F.3d at 1261.

Plaintiff contends that it will suffer irreparable competitive injury if Defendants are permitted to use Plaintiff’s proprietary and confidential know how to “cut corners in the research and development process” and “attain a competitive product . . . much sooner” than if it developed the features independently. (Doc. # 173-1, Pl.’s Suppl. Brief at 22, ¶ 68.) Additionally, Plaintiff alleges irreparable injury exists because “there is no

practical way the plaintiff will ever be able to prove what sales the defendant's competition will make it lose, to say nothing of the indirect, though at times far-reaching, effects upon its good will." (*Id.* at 14, ¶ 44 (quotations and citation omitted).)

With respect to the CFAA Injunction, Defendants respond that an order enjoining them from accessing the "site admin" portions of the Landings East website would be moot because Plaintiff's have already severed their access to the site.³ (Doc. # 174, Defs.' Suppl. Resp. at 10-11, ¶ 30.) While such access may have been severed, the Court finds that Plaintiff could be irreparably harmed if Defendants are not enjoined from accessing the protected "site admin" portions of Plaintiff's application without Plaintiff's authorization. Defendants have exhibited the willingness to engage in improper conduct to obtain protected information from its direct competitor and, at the very least, they have used that information for marketing purposes. There is nothing to indicate to the Court that Defendants will not engage in similar conduct in the future, if left to their own devices.

³ Defendants also allege the requested injunction is directed to enjoining their access to other websites to which Defendants have a legitimate right to access, including (1) the publicly available Castle Breckenridge site, (2) the website for CAI-Austin, to which AHN is a member, and (3) the web-based sites of transitioning customers who are converting content from Plaintiff's application to AHN's application. However, the requested CFAA Injunction will not reach Defendants' access to the first two sites because Plaintiff has not demonstrated such access was unauthorized and because Defendants' access was at member-level, not "site admin" level. As to the sites of transitioning customers, there is evidence in the record that suggests access to the "site admin" portions is not necessary to effectuate a transfer of customer data. (See Doc. # 136-3, Pl.'s Jan. 14, 2009 Email to Customer ("your content could have been copied/transferred without having to give anyone login access"). However, to the extent such access is necessary, the Court has fashioned an appropriate injunction.

As to the Breach of Contract Injunction, Defendants contend that “[t]here is no presumption . . . that damages are too difficult to quantify, even in a case of misappropriated intellectual property.” (Doc. # 174, Defs.’ Suppl. Resp. at 8, ¶ 23.) In support, Defendants present the affidavit of their expert Russell L. Parr, a consultant, author, lecturer, and publisher specializing in intellectual property valuation. Mr. Parr states that various methodologies exist for calculating lost profits and other intangible injuries, such as competitive advantage, that result from the misappropriation of intellectual property. (Doc. # 131-2, Ex. 1 to Defs.’ Resp., ¶¶ 11-13.) Because monetary damages allegedly will be available to fully compensate Plaintiff, Defendants argue preliminary injunctive relief is not appropriate.

On this issue, the Court agrees with Defendants. Plaintiff has not made a “strong showing” that it will be irreparably harmed if Defendants are not enjoined from offering the 15 disputed features. Assuming *arguendo* that Defendants did copy the disputed 15 features, methodologies exist to approximate the monetary damages necessary to address any competitive advantage Defendants may have gained from enhancing the features that were available in AHN’s prior version of the application. Furthermore, although Plaintiff has demonstrated Defendants’ actions were wrongful, the evidence suggests that Defendants used the improperly obtained information to short cut market analysis of its competitor’s product, not to short cut the development of its own

application. Thus, any irreparable injury Plaintiff believes it has suffered or will suffer as a result of the competitive advantage Defendants may have obtained in AHN's marketing can be addressed by the requested CFAA Injunction.

3. Balance of Harms

The Court next weighs the harms Defendants face if the injunction is granted against the harms Plaintiff will face if the injunction is not granted.

Defendants claim the CFAA Injunction would harm its ability to gain customers from AV in the normal course of its business. (Doc. # 174, Defs.' Suppl. Resp. at 17, ¶ 49.) Defendants also contend that the Breach of Contract Injunction would cause it to lose existing customers by requiring it to remove services which the customers have become accustomed to using and for which they contracted, thereby potentially jeopardizing the company's existence. (*Id.*, ¶¶ 50-51.) On the other hand, Defendants claim the requested injunctions do not threaten Plaintiff's existence because it has continued to gain customers during the time period Defendants have been using the disputed features. (*Id.*, ¶ 52.)

The Court finds that the balance weighs in Defendants' favor with respect to the Breach of Contract Injunction, but not, the CFAA Injunction. The evidence submitted by the parties, both with the briefs and at the hearing, indicate that Defendants unlawfully obtained valuable information regarding Plaintiff's software application and are using that information to market AHN's application in direct competition with Plaintiff's application. Defendants will not suffer any harm recognized in law if they are prohibited

from unlawfully using Plaintiff's information. However, the evidence does not suggest that Defendants used such information to design and develop a competing product. Consequently, they could suffer greatly if required to remove functionality that they developed independently.

4. Public Interest

Finally, the Court considers whether injunctive relief would be adverse to the public interest.

Plaintiff contends that "the public interest is served by enjoining unlawful competition." (Doc. # 124 at 3.) The Court agrees. However, Plaintiff has demonstrated only that Defendants violated the CFAA; it did not demonstrate that Defendants likely breached the Agreement through reverse engineering or misappropriation or use of confidential know how. Thus, prohibiting Defendants from further accessing the "site admin" portion of Plaintiff's application and from copying, disclosing, or otherwise using the valuable information they obtained unlawfully from Plaintiff would, if anything, tend to serve the public interest. But the public interest would not be served by requiring Defendants to remove features they may have independently developed.

For the reasons discussed above, the Court concludes that Plaintiff has met its burden for the entry of the requested CFAA Injunction, but has not demonstrated a "strong showing" on each of the four preliminary injunction factors necessary for the entry of the disfavored Breach of Contract Injunction.

C. UNCLEAN HANDS

The Court next considers Defendant Adams' contention that Plaintiff is not entitled to injunctive relief under the doctrine of unclean hands. Specifically, Adams asserts that Plaintiff acted improperly when it created tools that allowed its application to integrate with TOPS' software database, despite knowing of TOPS' exclusive relationship with Defendant AHN. (Doc. # 134, Adams' Resp. at 6.) The other defendants do not join and Plaintiff has not responded to this argument.

The Court rejects Adams' argument because he has not submitted sufficient evidence to show unclean hands. Adams argues that a party may be guilty of unclean hands "even if his or her behavior does not rise to the level of bad faith;" it is enough that the party acted improperly. (Doc. # 134 at 5.) Adams is correct. However, he has not shown that Plaintiff acted improperly. Specifically, he has not shown, or even alleged, that Plaintiff has breached any contract or has violated any duty, statute, or law. *Cf. Hocker v. New Hampshire Ins. Co.*, 922 F.2d 1476, 1476 (10th Cir. 1991) (finding unclean hands due to contractual breach); *Oklahoma Retail Grocers Assoc. v. Wal-Mart Stores, Inc.*, 605 F.2d 1155 (10th Cir. 1979) (affirming summary judgment that the plaintiff was barred by unclean hands because the members of the plaintiff engaged in the very activity that was the basis for the complaint against the defendant, namely competition through price cutting in violation of the Oklahoma Unfair Sales Act). Without some improper conduct on the part of Plaintiff, the doctrine of unclean hands cannot apply.

IV. POSTING OF BOND

Federal Rule of Civil Procedure 65(c) provides that a court may issue a preliminary injunction “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.” Under the circumstances of this case, the Court concludes that security is not necessary to serve the purposes established in Rule 65(c).

V. CONCLUSION

It is, therefore,

ORDERED that Plaintiff’s Motion to Strike Non-Record Evidence from Defendants’ Proposed Findings of Fact and Conclusions of Law (Doc. # 179) is DENIED. It is further

ORDERED that Plaintiff’s Second Renewed Motion for Preliminary Injunction (Doc. # 124) is GRANTED IN PART and DENIED IN PART as set forth herein. It is further

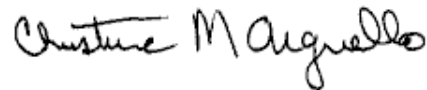
ORDERED that Defendants, their agents, employees, and those people in active concert or participation with them are preliminarily enjoined from accessing the password-protected “site admin” portions of Plaintiff’s web-based software application without Plaintiff’s authorization. To the extent access to such “site admin” portions may

be necessary to convert customers' content from Plaintiff's application to AHN's application, Defendants so inform Plaintiff and work with Plaintiff to effectuate such transfer in the least intrusive manner possible. It is further

ORDERED that Defendants, their agents, employees, and those people in active concert or participation with them are preliminarily enjoined from using the information it gained through its improper access to the "site admin" portions of the Landings East website for any purpose, including but not limited to, the preparation and distribution of marketing materials, responding to prospective and existing customer inquiries, and the design and development of AHN's application.

DATED: January 06, 2011

BY THE COURT:



CHRISTINE M. ARGUELLO
United States District Judge