

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

LASCO FOODS, INC.,)	
)	
Plaintiff,)	
)	
vs.)	Case No. 4:08CV01683 JCH
)	
HALL AND SHAW SALES, MARKETING,)	
& CONSULTING, LLC, et al.)	
)	
Defendants.)	

MEMORANDUM AND ORDER

This matter is before the Court on the Motion to Dismiss Counts II and III of Plaintiff's Amended Complaint (Doc. No. 15) of Defendants Hall and Shaw Sales, Marketing & Consulting, LLC, Charles R. Shaw, and Ronald N. Hall (collectively, "Defendants"). The matter is fully briefed and ready for disposition.

BACKGROUND

Plaintiff Lasco Foods, Inc. ("Lasco" or "Plaintiff") is a Missouri limited liability corporation with its principal place of business in the State of Missouri. (Amended Verified Complaint for Temporary Preliminary and Permanent Injunction ("Complaint" or "Compl."), Doc. No. 13, ¶ 1). Defendant Ronald N. Hall, a resident of Weatherford, Texas, was formerly employed by Lasco as a Regional Sales Manager. (Compl., ¶¶ 2, 31). Defendant Charles R. Shaw, a resident of St. Charles County, Missouri, was formerly employed by Lasco as a National and Regional Sales Manager. (Compl., ¶¶ 3, 18). Defendant Hall and Shaw Sales, Marketing & Consulting LLC ("HSSMC") is a Missouri limited liability company. (Compl., ¶ 4). Defendants Shaw and Hall formed and currently work for HSSMC. (Compl., ¶¶ 42 - 44).

Plaintiff filed its Amended Complaint on November 7, 2008. (Doc. No. 13). Plaintiff asserts the following claims for relief: Misappropriation of Trade Secrets in Violation of the Missouri Uniform Trade Secrets Act, Mo. Rev. Stat. § 417.450, et seq. (Count I), Violations of Stored Wire and Electronic Communications Act (“SECA”), 18 U.S.C. § 2701, et seq. (Count II), Violations of Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, et seq. (Count III), Unfair Competition (Count IV), Violation of the Missouri Statute Against Tampering with Computer Data and Equipment, R.S. Mo. §537.525, and the Missouri Statute Against Tampering with Computer Equipment, R.S. Mo. § 569.097 (Count V), Conversion (Count VI), Tortious Interference with Plaintiff’s Contracts and/or Business Expectancies (Count VII), Civil Conspiracy (Count VIII), and Breach of Duty of Loyalty to Lasco (Count IX).

As stated above, Defendants filed the instant Motion to Dismiss Counts II and III of the Amended Complaint on November 12, 2008. (Doc. No. 15). Defendants allege that Plaintiff has not properly pled its claims under SECA and CFAA, and those claims must be dismissed. Defendants assert that the remaining claims likewise must be dismissed because this Court lacks supplemental jurisdiction over them.

STANDARD FOR MOTION TO DISMISS

In ruling on a motion to dismiss, the Court must view the allegations in the complaint liberally in the light most favorable to Plaintiff. Eckert v. Titan Tire Corp., 514 F.3d 801, 806 (8th Cir. 2008) (citing Luney v. SGS Auto. Servs., Inc., 432 F.3d 866, 867 (8th Cir. 2005)). Additionally, the court, “must accept the allegations contained in the complaint as true and draw all reasonable inferences in favor of the nonmoving party.” Coons v. Mineta, 410 F.3d 1036, 1039 (8th Cir. 2005) (citation omitted). To survive a motion to dismiss, a complaint must contain “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 127 S. Ct. 1955,

1974 (2007) (abrogating the “no set of facts” standard for Fed. R. Civ. P. 12(b)(6) found in Conley v. Gibson, 78 S. Ct. 99 (1957)). While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff’s obligation to provide the grounds of his entitlement to relief “requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Bell Atl. Corp., 127 S. Ct. at 1965; Huang v. Gateway Hotel Holdings, 520 F. Supp. 2d 1137, 1140 (E.D. Mo. 2007).

DISCUSSION

I. SECA

In Count II, Plaintiff alleges a SECA claim against the Defendants. Section 2701(a) of SECA provides that:

whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2707 provides a civil cause for any violation of SECA. See 18 U.S.C. § 2707(a) (“any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter [18 U.S.C. §§ 2701 et seq.] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, ... which engaged in that violation such relief as may be appropriate”).

Defendants’ Motion presents the question of whether Lasco sufficiently has alleged a colorable claim that Defendants Hall’s and Shaw’s access to Lasco information was “unauthorized,” as required under SECA. Defendants argue that there cannot be a cause of action under SECA if Hall’s and Shaw’s access to the computer systems at issue was authorized. Based upon the legislative

history of SECA, the language of the statute and Plaintiff's allegations, this Court finds that Plaintiff has failed to state a claim against Defendants under SECA.¹

The legislative history and language of SECA indicate that it was not intended to apply to cases such as this. Federal courts interpreting SECA and CFAA have noted that their "general purpose . . . was to create a cause of action against computer hackers (e.g., electronic trespassers)." Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005) (citations omitted). The statutes are generally aimed towards outside, third parties or other "high-tech" criminals, rather than the rogue employee. Indeed, § 2701(c) (1) provides that the statute "does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service."

The allegations in this case are similar to those in Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817 (E.D. Mich. 2000). In Sherman & Co., Sherman had a contract with Salton to sell products to Kmart on behalf of Salton. Salton terminated Sherman's contract but Sherman continued as a product representative to Kmart for companies other than Salton. Salton alleged that, after Sherman was no longer its employee, he used a computer access code provided to Kmart to access Salton sales data in the Kmart computer system and thereafter provided that information to one of Salton's competitors. Id. at 219. Salton alleged that, even though Kmart had provided Sherman this access, Sherman knew that Salton "certainly did not authorize him to view this information and he knew he was not so authorized." Id. Salton filed a

¹Defendants also argue that Plaintiff is not a provider of an "electronic communication service" and, therefore, Plaintiff cannot allege a claim under SECA. See Defendants' Suggestions in Support of Their Motion to Dismiss Counts II and III of Plaintiff's Amended Complaint ("Suggestions in Support"), Doc. No. 16, pp. 9-11. Because this Court is granting Defendants' Motion to Dismiss the SECA claim on other grounds, the Court need not address whether Lasco is a provider of an "electronic communication service" at this time.

counterclaim against Sherman alleging a cause of action under SECA because of Sherman's allegedly "unauthorized" access to Salton's information.

The Sherman & Co. court granted the plaintiff's motion to dismiss Salton's SECA claim because the complaint failed to allege that Sherman's access was "unauthorized" within the meaning of SECA. Id. at 821. The Sherman & Co. court further explained that for:

"intentional" access in excess of authorization to be a crime and actionable civilly, the offender must have obtained the access to private files without authorization (e.g., using a computer he was not to use, or obtaining and using someone else's password or code without authorization). At a minimum, there must be a clearer and more explicit restriction on the authorized access than presented by Salton's proposed counterclaim. Here Sherman's access to the Salton data in the Kmart network system was in no way restricted by technical means or by any express limitation. Because section 2701 of [SECA] prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access. Section 2701 outlaws illegal entry, not larceny.

Id. Thus, according to the Sherman & Co. court, a SECA claim must allege Defendants were not "unauthorized" to access the information at issue.

Here, Lasco has alleged that Defendants had virtually unrestricted access to its information. (Compl., ¶¶ 19, 32). Yet, Lasco broadly, and without any factual support, alleges "Defendants Hall and Shaw fraudulently or intentionally exceeded their authorization to access Lasco's protected computers." (Compl., ¶¶ 57, 60). Lasco has not identified any restricted information that Defendants supposedly accessed. Rather, the thrust of Plaintiff's claim is the generalization that Defendants obtained information for improper purposes. See, e.g., Compl., ¶ 41 ("while Defendant Hall was still employed by Lasco, he attempted, through deception, to obtain reports from one of Lasco's [b]rokers"). This "deception," as pled, however, is not a SECA violation. "Where a party consents to another[']s access to its computer network, it cannot claim that such access was unauthorized." Sherman & Co., 94 F. Supp. 2d at 821. Lasco afforded Defendants access to its computers,

networks and information, which they utilized throughout their employment. Plaintiff has not alleged anything to the contrary. Thus, while Defendants may have improperly used Plaintiff's information, this is not a SECA violation and Count II fails to state a claim, as pled.

II. CFAA

Defendants claim that Plaintiff has failed to state a civil claim under CFAA because it has not alleged both damage and loss under CFAA. (Defendants' Reply Brief in Support of Their Motion to Dismiss Counts II and III of Plaintiff's Amended Complaint ("Reply"), Doc. No. 20, p. 8). Defendants also argue that Plaintiff's CFAA claim fails because it has not alleged that any damage or loss arose from an "interruption in service." (Suggestions in Support, pp. 11-13). Finally, Defendants briefly argue that Shaw's and Hall's alleged access to the computers was not in excess of their authorization, as required under CFAA. (Suggestions in Support, p. 13).

A. Background of CFAA.

CFAA recognizes "private causes of action for individuals damaged by computer fraud: 'Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.'" In re AOL, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1368 (S.D. Fla. 2001) (quoting 18 U.S.C. § 1030(g)). Section 1030(g) further requires that "[a] civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." Section 1030(c)(4)(A)(i)(I)² affords a cause of action, in relevant part, against whomever causes "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only,

²As noted by Defendants, "Section 1030 was amended by Pub. L. 110-326 which became effective September 26, 2008. ... Pub. L. 110-326 renumbered what was formerly § (a)(5)(B)(i)-(iv) as § (c)(4)(A)(i)(I)-(IV)." (Reply, p. 7).

loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$ 5,000 in value.”³

Courts dispute whether a plaintiff must allege both “damage” and “loss” to state a civil claim under CFAA. According to the statute, “damage” is defined as “any impairment to the integrity or availability of data, a program, a system, or information,” 18 U.S.C. §1030(e)(8), and “loss” is defined 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).

According to Defendants, to state a civil action, a plaintiff must allege both “damage” and “loss” under CFAA. (Reply, p. 8). Subsection 1030(c)(4)(A)(i)(I) specifically requires “loss,” and the legislative history further indicates that both “damage” and “loss” are required. See Garelli Wong & Assocs. v. Nichols, 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008) (“it is necessary for a plaintiff to plead both damage and loss in order to properly allege a civil CFAA violation”). Plaintiff, however, cites contrary authority that holds that a plaintiff is only required to show damage or loss to state a civil cause of action. See 18 U.S.C. §1030(g); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (“Congress’s use of the disjunctive, ‘damage or loss,’ confirms that it anticipated recovery in cases involving other than purely physical damage.”).

B. Plaintiff Has Alleged “Damage” and “Loss” under CFAA.

This Court need not address the issue of whether a civil claim under CFAA requires both damage and loss or damage or loss. The Court finds that Plaintiff sufficiently alleges damage and loss.

³Subsections II-V of §1030(c)(4)(A)(i) do not appear to be applicable to Plaintiff’s allegations.

In the Amended Complaint, Plaintiff alleges that “Lasco demanded the Defendant Shaw return to Lasco all electronic and hard copy information in his possession belonging to Lasco,” but that Defendant Shaw “deleted confidential and trade secret information from Lasco’s computer.” (Compl., ¶ 28).⁴ Plaintiff also alleges that “Defendant Shaw unlawfully copied or otherwise downloaded Lasco’s Trade Secret Information for his own personal use and for the use of HSSMC prior to his departure from Lasco and prior to deleting the Trade Secret Information from his Lasco computer and returning the computer to Lasco.” (Compl., ¶ 29). With respect to Defendant Hall, “Lasco demanded the Defendant Hall return to Lasco all electronic and hard copy information in his possession belonging to Lasco,” but Hall did not return Lasco’s computer prior to the filing of the original complaint. (Compl., ¶ 39). Plaintiff also “anticipates the results of its forensic examination of Defendant Hall’s computer will confirm he deleted electronically stored property before he returned his Lasco-issued computer to Lasco.” (Plaintiff’s Memorandum in Opposition to Defendants’ Motion to Dismiss Counts II and III of Plaintiff’s Amended Complaint (“Memorandum in Opposition”), Doc. No. 19, p. 5, n. 2).

These allegations in the Complaint that Defendants deleted information are sufficient to allege “damage,” as defined under CFAA. Int’l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (reversing the district court’s grant of summary judgment because plaintiff’s deletion of information on the company computer constituted “damage” under CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) and (ii)); see also Patrick Patterson Custom Homes, Inc. v. Bach, No. 07 C 7204, 2008 U.S. Dist. LEXIS 92761, *18-19 (N.D. Ill. Nov. 14, 2008) (“it is sufficient to show damage under the CFAA where a program intended to delete files is installed and files are subsequently

⁴As noted by Defendants, it is difficult to determine under which of the subsections of 1030(a) Plaintiff attempts to bring its claim, but Plaintiff’s pleadings most closely resemble a claim under section 1030(a)(5)(B) or (C). (Reply Memorandum, pp. 7-8).

deleted because such an erasure program impairs the integrity or availability of data, programs, or information on the computer”) (citing Citrin, 440 F.3d at 419-20); Alliance Int’l, Inc. v. Todd, No. 5:08-CV-214, 2008 U.S. Dist. LEXIS 56077, *20 (E.D.N.C. July 22, 2008) (“the relevant allegations of the complaint contend that defendants ‘deleted, removed and destroyed information, documents and/or data contained on . . . protected computers’ and ‘knowingly caused the transmission of a program, information, code or command, ... and as a result of such conduct, intentionally caused damage without authorization, to a protected computer’” sufficiently pled a cause of action in violation of the CFAA).

As discussed in detail in the following section, this Court also holds that the deletion of information, the cost of the forensic analysis and other remedial measures associated with retrieving and analyzing Defendants’ computers constitute “loss” under CFAA. See In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) (the legislative history makes “clear that Congress intended the term ‘loss’ to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.”).

Upon consideration, the Court finds that Plaintiff has alleged both “loss” and “damage”. Plaintiff sufficiently has plead impairment to the integrity or availability of data, a program, a system, or information as well as that Lasco reasonably incurred costs, including the cost of responding to the offense, conducting a damage assessment and restoring the integrity of its data.

C. Plaintiff Has Alleged Interruption in Service under CFAA.

“Courts have consistently interpreted ‘loss’... to mean a cost of investigating or remedying damage to a computer, or a cost incurred because the computer’s service was interrupted.” Frees, Inc. v. McMillian, No. 05-1979, 2007 U.S. Dist. LEXIS 57211, *7 (W.D. La. Aug. 6, 2007). The Court agrees that, under CFAA, any “loss” must result from an “interruption in service.” See Nexans

Wires S.A. v. Sark-USA, Inc., No. 05-3820, 2006 U.S. App. LEXIS 3619, at *6 (2d Cir. Feb. 23, 2006) (“Because it is undisputed that no interruption of service occurred in this case, L&K’s asserted loss of \$ 10 million is not a cognizable loss under the CFAA.”). Plaintiff, however, has sufficiently alleged loss as a result of an interruption of service.

Plaintiff alleged a loss as a result of an interruption in service when Defendants retained Plaintiff’s property and deleted some of Lasco’s information. Both Hall and Shaw refused to return their computers when Lasco demanded their return. (Compl., ¶¶ 28, 39). Defendants argue that the “minor gap in time” between when Lasco demanded Hall’s and Shaw’s computers and when Lasco received the computers cannot constitute a “loss.” (Reply, p. 11). According to Defendants, this “minor gap in time” totaled, at a minimum, 108 days (70 for Shaw and 38 for Hall). (Id., n. 3). Although this may be, as Defendants claim, a “minor” loss, the Court believe it constitutes a sufficient “interruption in service.”

As previously stated, Lasco alleges that Shaw (and possibly Hall) deleted information from their computers. (Compl., ¶ 29; Memorandum in Opposition, pp. 5-6). Implicit in Plaintiff’s Complaint is that it had to hire an expert to investigate Hall’s and Shaw’s computers when they were returned. (See, e.g., Compl., ¶ 28). Plaintiff’s Memorandum further details that they had to perform a forensic investigation to determine what information was deleted from Hall’s and Shaw’s computers. (Memorandum in Opposition, pp. 5-6). The cost of these investigations also constitutes a loss from the interruption in service under CFAA. “The cost of hiring an expert to investigate the computer damage is clearly a ‘reasonable cost’ sufficient to constitute ‘loss’ under the CFAA.” Frees, Inc., 2007 U.S. Dist. LEXIS 57211, at *8 (citing 18 U.S.C. § 1030(e)(11)); Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro, No. 3:06-CV-2175, 2007 U.S. Dist. LEXIS 45953, at *5

(M.D. Pa. Jun. 25, 2007)).⁵ Thus, Plaintiff has sufficiently alleged loss from an interruption in service under CFAA.

D. Plaintiff Has Failed to Allege Defendants Accessed Information Without Authorization.

Defendants briefly argue in their Suggestions in Support that Plaintiff has failed to allege that Defendants accessed information “without authorization,” as required under CFAA (similar to the requirement in SECA).⁶ (Suggestions in Support, p. 13; see 18 U.S.C. § 1030 (§ 1030(a)(1), which states, “having knowingly accessed a computer without authorization or exceeding authorized access...”; § 1030(a)(2), which states, “intentionally accesses a computer without authorization or exceeds authorized access...”; § 1030(a)(4), which states, “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access...”; § 1030(a)(5), which states, “causes damage without authorization. . .”). As Plaintiff has failed properly to allege “without authorization,” this Court grants Defendants’ Motion to Dismiss the CFAA claim. See also Condux Int’l, Inc. v. Haugum, No. 08-4824, 2008 U.S. Dist. LEXIS 100949, at *19 (D. Minn. Dec. 15, 2008) (where the “heart of the dispute” was “not the access of the confidential business information but rather the alleged subsequent misuse or misappropriation of that information,” plaintiff failed to state a claim under CFAA); In re AOL, Inc. Version 5.0 Software Litig., 168 F.

⁵Forensic analysis and other similar activities also constitute “damage” under CFAA. Cf. Kalow & Springnut, LLP v. Commence Corp., No. 07-3442, 2009 U.S. Dist. LEXIS 320, at *7-8 (D. N.J. Jan. 5, 2009) (“To the extent Defendant argues that Plaintiff failed to plead adequate types of damages, the Court finds that Plaintiff has sufficiently pled damages recoverable under the CFAA, namely, the unavailability of certain customer data and information due to the intentional placement of a time bomb, the purchase of an upgrade, and lost productivity and wages or fees paid to computer consultants.”)

⁶In fact, Plaintiff does not respond to this argument in its Memorandum in Opposition and Defendants do not argue it in their Reply.

Supp. 2d at 1370 (the phrase “without authorization” in §§ 1030(a)(5)(B) and (C)⁷ “contemplate[s] a situation where an outsider, or someone without authorization, accesses a computer”).

III. SUPPLEMENTAL JURISDICTION

This Court dismisses Counts II and III of Plaintiff’s Complaint. As these counts are the only bases for federal court jurisdiction, this Court will likewise dismiss Counts I, IV-IX. The Court, however, affords Plaintiff the opportunity to amend its complaint to cure the deficiencies discussed herein, which may include allegations and counts similar to Counts I, IV-IX.

CONCLUSION

Accordingly,

IT IS HEREBY ORDERED that Defendants’ Motion to Dismiss to Dismiss Counts II and III of Plaintiff’s Amended Complaint (Doc. No. 15) is **GRANTED**, in accordance with the foregoing.

IT IS HEREBY FURTHER ORDERED that Counts I, IV-IX are **DISMISSED** for lack of jurisdiction, in accordance with the foregoing.

IT IS FURTHER ORDERED that Plaintiff is granted until **Friday, February 6, 2009**, within which to file an Amended Complaint, curing the above-described deficiencies.

Dated this 22nd day of January, 2009.

/s/ Jean C. Hamilton

UNITED STATES DISTRICT JUDGE

⁷As previously stated, Plaintiff’s allegations most closely resemble claims under these subsections of CFAA. See, supra, n. 4.