IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

NORTH CENTRAL FLINT HILLS
AREA AGENCY ON AGING, INC.,

Plaintiff,

vs. **Case No. 09-4130-RDR**

STEPPING STONES UNLIMITED,
L.L.C., a Kansas Limited
Liability Company, and
DEBRA KELLEY, CAROLYN STEVER
and LYNDA BURT, Individuals,

Defendants.

MEMORANDUM AND ORDER

Plaintiff is the North Central Flint Hills Area Agency on Aging, Inc., a not-for-profit corporation devoted to providing services to eligible aging persons under the Medicaid Act. Defendants are: Stepping Stones Unlimited, LLC, a limited liability company doing the same kind of work as plaintiff; and three former employees of plaintiff who created and/or work for Stepping Stones. The individual defendants are: Debra Kelley, Carolyn Stever and Lynda Burt. Plaintiff alleges that defendants violated the federal Computer Fraud & Abuse Act (CFAA), 18 U.S.C. § 1030, and committed Kansas state law violations, including breach of contract, misappropriation of trade secrets, and fraud.

This case is before the court upon defendants' motion to dismiss under FED.R.CIV.P. 12(b)(6). Defendants' motion contends that plaintiff has failed to state a claim under the CFAA and that

the court should decline to exercise supplemental jurisdiction over the state law claims.

Also pending is a motion for leave to file a surreply to defendants' motion to dismiss. Doc. No. 13. This motion for leave shall be granted.

I. LEGAL STANDARDS

To survive a motion to dismiss for failure to state a claim, a complaint must present factual allegations, assumed to be true, that "raise a right to relief above the speculative level" and must contain "enough facts to state a claim to relief that is plausible on its face." Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 & 570 (2007). "Plausibility" does not mean "likely to be true." Robbins v. Oklahoma, 519 F.3d 1242, 1247 (10th Cir. 2008). "'[P]lausibility' in this context must refer to the scope of the allegations in a complaint: if they are so general that they encompass a wide swath of conduct, much of it innocent, then the plaintiffs 'have not nudged their claims across the line from conceivable to plausible.'" Id. (quoting Twombly, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 129 S.Ct. 1937, 1949 (2009). "The complaint 'does not need detailed factual allegations'" to surmount a motion to dismiss for failure to state a claim. Christy Sports, LLC v. Deer Valley

Resort Co., 555 F.3d 1188, 1191 (10th Cir. 2009) (quoting Twombly, 550 U.S. at 555). "[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable and that recovery is very remote and unlikely." Twombly, 550 U.S. at 556 (interior quotations omitted). However, "the complaint must give the court reason to believe that [the plaintiff] has a reasonable likelihood of mustering factual support of [the plaintiff's] claims." Ridge at Red Hawk, L.L.C. v. Schneider, 493 F.3d 1174, 1177 (10th Cir. 2007).

If the court on a Rule 12(b)(6) motion looks to matters outside the complaint, the court generally must convert the motion to a Rule 56 motion for summary judgment. Dean Witter Reynolds, Inc. v. Howsam, 261 F.3d 956, 961 (10th Cir. 2001) rev'd on other grds, 537 U.S. 79 (2002). However, the court may consider documents which are referred to in the complaint. See GFF Corp. v. Associated Wholesale Grocers, 130 F.3d 1381, 1384-85 (10th Cir. 1997).

II. THE CFAA

The CFAA, 18 U.S.C. § 1030, is a criminal statute which punishes persons who obtain unauthorized access to computers or whose access to computers has exceeded their authorization. The CFAA also provides for a civil cause of action in § 1030(g):

> 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. 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). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.

18 U.S.C. § 1030(g).

The CFAA lists seven categories of criminal violations in § 1030(a). Although the complaint in this case does not identify by section and subsection which kind of CFAA violation is being alleged, the following sections appear to be relevant to the complaint and the motion to dismiss:

> § 1030(a)(2)(C) - "Whoever - - intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains - - . . . information from any protected computer . . ."

> § 1030(a)(4) - "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, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period"

> § 1030(a)(5)(A) - "Whoever - - knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct intentionally causes damage without authorization to a protected computer"

> § 1030(a)(5)(B) - "Whoever - - intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage"

> § 1030(a)(5)(C) - "Whoever - - intentionally accesses a protected computer without authorization and as a result of such conduct, causes damage and loss"

In this case, the parties agree that the alleged "violation"

involves only subclause I in subsection 1030(c)(4)(A)(I), that is conduct causing a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."

III. THE COMPLAINT

The complaint alleges that the individual defendants worked as case managers for plaintiff prior to resigning and working for defendant Stepping Stones. Defendants Stever and Kelley allegedly filed Articles of Organization for Stepping Stones in July 2007 and submitted Stepping Stones' application to be a service provider for the Medicaid program in August 2007, while they still worked for plaintiff. Defendant Stever resigned from plaintiff effective April 30, 2008. Defendant Kelley resigned from plaintiff effective May 31, 2008. Defendant Burt resigned on January 8, 2009, effective immediately. The complaint alleges that, contrary to what defendant Stever said in an exit interview, Stepping Stones has been competing with plaintiff in the provision of FE (frail elderly) services and has submitted approximately 75 requests to transfer plaintiff's customers' cases to Stepping Stones. According to the complaint, the majority of these case transfer requests involved customers previously served by the individual defendants when they worked for plaintiff.

The complaint alleges that defendants have accessed electronic information contained in the Kansas Aging Management Information System (KAMIS) which is managed by the Kansas Department on Aging

(KDOA). Service providers submit data on customers to the system. KAMIS users are required to read and sign a Security Agreement which requires users to acknowledge that all client information on KAMIS is confidential and to be used only in the lawful administration of the KDOA program. The complaint indicates that the 75 transfer requests occurred between January 1, 2009 and March 30, 2009 as a result of defendants contacting plaintiff's customers after plaintiff performed assessments of the customers and entered assessment information onto KAMIS.

The complaint asserts that: the individual defendants were provided access to and use of plaintiff's laptop and desktop computers when they worked for plaintiff; that the individual defendants acknowledged and agreed in writing that the computers were strictly for use performing plaintiff's business and not for private purposes; and that when the individual defendants returned plaintiff's computers upon their resignation, it was found that the computers had been used to create and develop Stepping Stones and that "much of the content of the computers had been intentionally deleted." Doc. No. 1, ¶ 43.

According to the complaint, the individual defendants signed statements as part of their employment with plaintiff which stated:

> I . . . recognize and understand that the NC-FH AAA systems are to be used for conducting the Agency's business only. I understand that use of this equipment for private purposes is strictly prohibited. Further, I agree not to use a password that has not been disclosed to the NC-FH AAA system administrator. I agree not to

> access a file or retrieve any stored communication other than where authorized.
> I am aware that the NC-FH AAA reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the NC-FH AAA electronic systems at any time, with or without employee notice and that such access may occur during or after working hours. I am aware that use of an Agency provided password or code does not restrict the NC-FH AAA right to access electronic communications. I am aware that violations of this policy may subject me to disciplinary action, up to and including discharge from employment.
> I acknowledge that I have read and that I understand the NC-FH AAA's policy regarding electronic messaging including e-mail, Internet and voice mail systems.

Doc. No. 1, Exhibit F.

The complaint alleges that using the computers to create and develop Stepping Stones was not authorized by plaintiff. The complaint further alleges that accessing and deleting data from the computers caused damage to and impaired the integrity of the computers. Plaintiff also alleges that defendants accessed confidential information on the computers for the benefit of defendants' competing enterprise, contrary to any use authorized by plaintiff.

Plaintiff alleges that defendants' actions caused economic damage and loss, including lost profits and goodwill, in an amount more than $5,000 during any one-year period and that the computers were used to transmit information in interstate commerce.

IV. DEFENDANTS' ARGUMENTS

A. Damage or loss

Defendants' first argument is that plaintiff has failed to

state a claim under the CFAA because plaintiff has not alleged compensable damages or loss.

The complaint generally alleges: "Defendants' conduct caused economic damage and loss, including lost profits and loss of goodwill, to [plaintiff] aggregating more than $5,000 during any one-year period." Doc. No. 1, ¶ 50. Defendants contends that this allegation is insufficient because the CFAA does not cover lost profits and loss of goodwill and because the CFAA does not cover losses stemming from a disloyal employee's dissemination of confidential information obtained from a computer. Defendants also argue that plaintiff does not allege losses resulting because of an interruption of computer service, as allegedly required by the CFAA.

"Damage" is defined in the CFAA as:

> any impairment to the integrity or availability of data, a program, a system, or information.

18 U.S.C. § 1030(e)(8).

"Loss" is defined in the CFAA 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).

Plaintiff initially responds that economic damage and loss has been alleged and is not limited in the complaint to loss of profits

and goodwill. As already mentioned, the complaint alleges "economic damage and loss, including lost profits and loss of goodwill." Doc. No. 1, ¶ 50 (emphasis added). The court agrees with plaintiff's point. The complaint does not limit plaintiff's claim of damage and loss to lost profits and goodwill. Therefore, the issue becomes whether the complaint's other allegations are sufficient to state a plausible claim of damage and loss for the purposes of the CFAA.

1. Damage

Defendants characterize the complaint as focusing upon the copying of trade secrets. Defendants contend that the misappropriation of trade secret information is not categorized as "damage" under the CFAA. However, plaintiff also alleges that defendants deleted "much of the content of the computers issued to the Individual Defendants." Doc. No. 1, ¶ 43. The court believes deleting content from a computer falls within the definition of "damage," i.e., according to § 1030(e)(8), "any impairment to the integrity or availability of data, a program, system or information." Therefore, plaintiff has made a plausible allegation of "damage" for the purposes of the CFAA. See Lasco Foods, Inc. v. HSSMC, 600 F.Supp.2d 1045, 1052 (E.D.Mo. 2009). Other conduct alleged in the complaint may also have caused "damage" for the purposes of the CFAA. For instance, a court has held that the transfer of confidential documents from a secure server to a non-

secure server constitutes "damage." Black & Decker, Inc. (US) v. Smith, 568 F.Supp.2d 929, 937 (W.D.Tenn. 2008). But, at this stage, the court does not have to reach the issue of whether other impacts constitute "damage" under the CFAA.

2. Loss

Defendants argue that any loss covered by the CFAA must derive from the interruption of computer service. The court disagrees. We read the definition of "loss" as including the reasonable costs of responding to the violation (including the assessment of the damage and restoring data), as well as the reasonable costs incurred (including loss of revenue and consequential damages), from the interruption of service. See SKF USA, Inc. v. Bjerkness, 636 F.Supp.2d 696, 721 (N.D.Ill. 2009). It is plausible to infer from the facts alleged in the complaint that there was an interruption of service from the computers which had information deleted, and that some "loss" was incurred. It is also plausible to infer from the facts alleged in the complaint that plaintiff can demonstrate "loss" in the form of reasonable costs: of responding to the alleged offense; of conducting a damage assessment; and restoring the data, program, system or information to its condition prior to the offense. Accordingly, the court finds that plaintiff has adequately alleged a "loss" for the purposes of the CFAA.[1]

[1] The cases cited by defendants to support their arguments regarding "damage" and "loss" are distinguishable because the allegations in the complaints of those cases were more narrow than

B. Unauthorized access or exceeding authorized access to a protected computer

The complaint's allegations mostly relate to CFAA violations which require proof of access to a protected computer without authorization or access which exceeds authorization. Section 1030(a)(5)(A) also defines "damage without authorization" as a violation. The CFAA does not define "authorization." The statute does define "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6).

The complaint alleges that defendants' access and use of computers exceeded "that authorized" by plaintiff in four ways: by obtaining information for use in the organization and development of Stepping Stones (Doc. No. 1, ¶ 46); by accessing and deleting data from computers (Doc. No. 1, ¶ 47); by accessing confidential customer information transmitted to the KAMIS system from

---

the allegations in the complaint in the case at bar. In Andritz, Inc. v. Southern Maintenance Contractor, L.L.C., 626 F.Supp.2d 1264 (M.D.Ga. 2009) and Cenveo Corp. v. Celumsolutions Software GMBH & Co., 504 F.Supp.2d 574 (D.Minn. 2007), there were no allegations of deleted or altered data. These cases also held that there were insufficient allegations of "loss" from responding to an offense and conducting damage assessments. 626 F.Supp.2d at 1267; 504 F.Supp.2d at 581. The complaint in the case at bar makes allegations regarding a response to and assessment of the computers used by defendants when they worked for plaintiff. Doc. No. 1, ¶ 43. From these allegations and others in the complaint, the court believes it is plausible that plaintiff can demonstrate "damage" and "loss" for the purposes of the CFAA.

plaintiff's protected computers for the benefit of Stepping Stones (Doc. No. 1, ¶ 48); and by accessing confidential information on plaintiff's protected computers with the intent to defraud (Doc. No. 1, ¶ 49).

Defendants argue that plaintiff has not adequately alleged unauthorized access or access which exceeds authorization and that plaintiff relies upon an overly broad interpretation of unauthorized access, instead of a more narrow interpretation favored by Judge Lungstrum, for example, in US Bioservices Corp. v. Lugo, 595 F.Supp.2d 1189 (D.Kan. 2009) ("Bioservices"). Defendants contend that they were authorized to use the computers in question and that they were authorized to access customer files on the computers. Defendants further assert that accessing information on the KAMIS system has nothing to do with plaintiff's computers because the KAMIS system is operated by the State of Kansas.

Plaintiff contends that defendants' motion to dismiss makes overly narrow assumptions regarding the information defendants took or deleted from plaintiff's computers; that defendants' authorized access to the computers was limited by agreements signed as a condition of their employment; and that the broad view of unauthorized access or access exceeding authorization should be employed in this case.

In Bioservices, Judge Lungstrum described a split of authority in cases interpreting the terms "without authorization" and

"exceeds authorized access" in the CFAA. He noted that some cases hold that when an employee violates his duty of loyalty to his employer, under agency law analysis, that employee has lost his authorization to use the employer's computer for purposes that do not further the employer's interests. See, e.g., International Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); Dental Health Products, Inc. v. Ringo, 2009 WL 1076883 (E.D.Wis. 4/20/2009); ViChip Corp. v. Lee, 438 F.Supp.2d 1087, 1100 (N.D.Cal. 2006) Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1124-25 (W.D.Wash. 2000). This is the broad view which defendants disfavor in this case.

A narrower approach holds that accessing a computer "without authorization" means bypassing passwords or other codes intended to limit access to a computer, such as a "hacker" might do. Many district courts have followed this approach. See, e.g., Black & Decker (US), Inc., 568 F.Supp.2d at 933-36; Shamrock Foods Co. v. Gast, 535 F.Supp.2d 962, 963-68 (D.Ariz. 2008); B&B Microscopes v. Armogida, 532 F.Supp.2d 744, 758 (W.D.Pa. 2007).

In Biosciences, the court dismissed any claims involving violations under §§ 1030(a)(5)(B) & (C) because those claims required proof of access to a protected computer "without authorization" when the complaint made it clear that the defendants had at least some authority to use the plaintiffs' computer systems. Thus, the court followed the narrower interpretation of

the CFAA and rejected the view that a disloyal employee who accesses his employer's computer with the passwords or codes permitted by the employer is acting "without authorization." However, the court permitted the case to go forward upon CFAA claims which only required proof of access which "exceeds" authorization.

The court is not inclined to choose between the two schools of thought discussed in the Biosciences case because under either approach it is plausible that plaintiff could develop factual support to substantiate a claim under multiple sections of the CFAA. Even under the approach followed in Biosciences, it is plausible that plaintiff could support an action alleging a violation under §§ 1030(a)(2)(C), (a)(4), and (a)(5)(A). In other words, plaintiff can plausibly claim that defendants exceeded their authorized access to plaintiff's computers to obtain information or with intent to defraud. Plaintiff can also plausibly claim that defendants caused damage to plaintiff's computers without authorization. As the focus of defendants' motion to dismiss appears to be whether there is any federal claim present which would allow this case to go forward in this court, the court does not believe it is necessary at this stage to determine exactly which CFAA claims may or may not proceed.

C. Interstate commerce

The CFAA claims in this case involve the use of "protected"

computers which are defined in the statute as including: "a computer . . . which is used in or affecting interstate or foreign commerce or communication . . ." 18 U.S.C. § 1030(e)(2)(B). Plaintiff alleges that the computers in this case "are used to transmit information in interstate commerce." Doc. No. 1, ¶ 45. Defendant claims that this "blanket allegation" is insufficient. Doc. 10, p. 13.

We disagree. We believe it is plausible that plaintiff can find factual support for a claim that the computers in question were used in or affecting interstate or foreign commerce or communication. See Paradigm Alliance, Inc. v. Celeritas Technologies, L.L.C., 248 F.R.D. 598, 601 n.5 (D.Kan. 2008) (a computer that provides access to worldwide communications through the internet qualifies as protected computer); Patrick Patterson Custom Homes, Inc. v. Bach, 586 F.Supp.2d 1026, 1032 (N.D.Ill. 2008) (same); Modis, Inc. v. Bardelli, 531 F.Supp.2d 314, 318-19 (D.Conn. 2008) (computer used to engage in business in different states). As with the other arguments made in defendants' motion, the court is not concluding that plaintiff will prove the elements of a CFAA violation. The court is only holding that it is plausible that plaintiff can develop factual support for its claim.

V. CONCLUSION

For the above-stated reasons, defendants' motion to dismiss shall be denied. Plaintiff's motion for leave to file a surreply

to the motion to dismiss shall be granted.

IT IS SO ORDERED.

Dated this 2nd day of February, 2010 at Topeka, Kansas.

s/Richard D. Rogers
United States District Judge