IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

US BIOSERVICES CORPORATION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 08-2342-JWL
	)	
LETICIA LUGO, et al.,	)	
	)	
Defendants.	)	
	)	
_____	)	

MEMORANDUM AND ORDER

Plaintiffs are specialty pharmaceutical care providers, servicing the pharmaceutical needs of manufacturers, physicians, patients, and payors. In this action, by their second amended complaint, plaintiffs allege that defendants Leticia Lugo and Garth Groman, while still employed by plaintiffs, obtained plaintiffs' confidential information; that Ms. Lugo and Mr. Groman disclosed such information to their new employer, defendant Axelcare Health Solutions, LLC ("Axelcare"), a competitor of plaintiffs; and that defendants have used such information to interfere with plaintiffs' contractual and business relationships. Plaintiffs assert claims for violations of the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030; misappropriation of trade secrets in violation of K.S.A. § 60-3320; tortious interference with contract and prospective business relations; and breach of contract.

This matter presently comes before the court on defendants' motion to dismiss

the entire complaint for failure to state a claim, pursuant to Fed. R. Civ. P. 12(b)(6) (Doc. # 41). For the reasons set forth below, the court **grants the motion in part and denies it in part**. The court grants the motion with respect to plaintiffs' claims for violations of section 1030(a)(5) of the CFAA, and those claims are hereby dismissed. The court denies the motion as it relates to plaintiffs' other claims.

I. Applicable Standards

The court will dismiss a cause of action for failure to state a claim only when the factual allegations fail to "state a claim to relief that is plausible on its face," *Bell Atlantic Corp. v. Twombly*, 127 S. Ct. 1955, 1974 (2007), or when an issue of law is dispositive. *Neitzke v. Williams*, 490 U.S. 319, 326 (1989). The complaint need not contain detailed factual allegations, but a plaintiff's obligation to provide the grounds of entitlement to relief requires more than labels and conclusions; a formulaic recitation of the elements of a cause of action will not do. *Bell Atlantic*, 127 S. Ct. at 1964-65. The court must accept the facts alleged in the complaint as true, even if doubtful in fact, *id.* at 1965, and view all reasonable inferences from those facts in favor of the plaintiff, *Tal v. Hogan*, 453 F.3d 1244, 1252 (10th Cir. 2006). Viewed as such, the "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Bell Atlantic*, 127 S. Ct. at 1965 (citations omitted). The issue in resolving a motion such as this is "not whether [the] plaintiff will ultimately prevail, but whether the claimant is

entitled to offer evidence to support the claims." *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 511 (2002) (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)).

II. CFAA Claims

Plaintiffs have asserted claims against defendants Lugo and Groman under paragraphs (a)(2)(C), (a)(4), (a)(5)(A)(ii), and (a)(5)(A)(iii) of the CFAA (Count IV of the second amended complaint). Those provisions create civil liability against whoever does the following:

> (2) intentionally *accesses a computer without authorization or exceeds authorized access*, and thereby obtains –
>
> . . .
>
> (C) information from any protected computer[1] if the conduct involved an interstate or foreign communication; [or]
>
> . . .
>
> (4) 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 . . .; [or]
>
> . . .
>
> (5)(A)(ii) intentionally *accesses a protected computer without authorization*, and as a result of such conduct, recklessly causes damage[2];

---

[1]The term "protected computer" includes any computer used in interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2)(B).

[2]The term "damage" means "any impairment to the integrity or availability of (continued...)

or

(iii) intentionally *accesses a protected computer without authorization*, and as a result of such conduct, causes damage.

18 U.S.C. § 1030(a)(2), (4), (5)(A)(ii) and (iii) (emphasis added); *see also id.* § 1030(g) (providing for civil liability for violations involving certain conduct, including conduct causing a loss of at least $5,000 in value). Thus, paragraphs (a)(2) and (a)(4) apply only if the defendant accesses the computer "without authorization" or "exceeds authorized access," while paragraph (a)(5)(A)(ii) or (iii) applies only if the defendant accesses the computer "without authorization."

The individual defendants argue that in committing the allegedly wrongful acts—obtaining confidential information on their work computers, e-mailing it to their personal e-mails, and later disclosing it to their new employer—they did not access plaintiffs' computers without authorization or exceed their authorized access, as required for liability, because they were authorized to access that particular information in their employment with plaintiffs. Thus, they seek dismissal of plaintiffs' claims under the CFAA.

Plaintiffs argue in response that a person acts without authorization or exceeds

---

[2](...continued)
data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Plaintiffs, in alleging a violation of paragraph (a)(5), have generally alleged that defendants "caused damage," but they have not alleged specifically how their information or system was impaired by defendants' conduct in accessing plaintiffs' computers. Defendants have not challenged the sufficiency of that allegation, however.

his authorization when he obtains information from his employer's computer system for a wrongful purpose, such as the disclosure of confidential information to a competitor. Indeed, a few courts have focused on the defendant's intent or his use of the information in finding liability under the CFAA. *See, e.g.*, *International Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000). In *Shurgard*, the court, in concluding that the plaintiff had stated a claim under paragraph (a)(2)(C) of the CFAA, held that the plaintiff's former employees had acted without authorization when they obtained information from the plaintiff's computers because, under Restatement (Second) of Agency § 112, their authorization terminated when they allegedly became agents of the defendant competitor during the act. *See Shurgard*, 119 F. Supp. 2d at 1124. In *Citrin*, the court similarly held that the defendant's authorization to access the plaintiff's computer files had terminated when he violated his duty of loyalty to his employer imposed by agency law. *See Citrin*, 440 F.3d at 420-21.

A number of courts have rejected the *Shurgard* and *Citrin* courts' reliance on agency law in applying the authorization provisions of the CFAA, instead applying those provisions in the manner urged by defendants here. *See, e.g.*, *Condux Int'l, Inc. v. Haugum*, 2008 WL 5244818, at *4-6 (D. Minn. Dec. 15, 2008); *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 933-36 (W.D. Tenn. 2008); *Shamock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963-68 (D. Ariz. 2008); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1341-43 (N.D. Ga. 2007); *Brett Senior & Assocs., P.C.*

v. Fitzgerald, 2007 WL 2043377, at *3-4 (E.D. Pa. July 13, 2007); *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, at *4-7 (M.D. Fla. Aug. 1, 2006); *International Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 498-99 (D. Md. 2005). Neither side to the present dispute has acknowledged this clear split in the caselaw or argued why this court should favor one line of cases over the other; instead, each side merely attempts to distinguish factually the "non-controlling" cases cited by the other. Thus, the parties have offered little help in resolving this conflict.

After reviewing the cases, this court finds persuasive the reasoning of the courts in the latter line of cases. Accordingly, the court follows their lead in holding that, under these provisions of the CFAA, access to a protected computer occurs "without authorization" only when initial access is not permitted, and a violation for "exceeding authorized access" occurs only when initial access to the computer is permitted but the access of certain information is not permitted. *See, e.g.*, *Shamrock*, 535 F. Supp. 2d at 963.

The court particularly adopts the synthesis of the arguments and caselaw and the analysis of the court in *Shamrock*, which the court will summarize here. First, the plain language of the CFAA compels this interpretation. "Without authorization" is not defined in the CFAA, but "authorization" is commonly equated with permission. *See id.* at 965 (quoting *Lockheed*, 2006 WL 2683058, at *5). The CFAA defines "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." 18 U.S.C. § 1030(e)(6). Thus, under the clear language of the statute, a violation for exceeding authorized access occurs when the defendant has permission to access the computer in the first place, but then accesses certain information to which he is not entitled. Under *Citrin* and *Shurgard*, on which plaintiffs rely, a person who has initial authorization to use the computer but then, with an improper purpose and in breach of his duty of loyalty, acquires information to which he is not entitled has acted "without authorization"—despite the statute's contemplation that such conduct constitutes "exceeding authorized access". In that way, the *Citrin* and *Shurgard* courts have overlooked the distinction between, and thereby conflated, the "without authorization" and "exceeds authorized access" prongs of the statute. *See Shamrock*, 535 F. Supp. 2d at 965 (quoting *Diamond Power*, 540 F. Supp. 2d at 1342-43). Accordingly, the language of the CFAA targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Id.* (quoting *Fitzgerald*, 2007 WL 2043377, at *3). There is no basis to graft a portion of the Restatement or other agency law onto the statute.[3]

---

[3]The court is further persuaded by the detailed analysis and ultimate rejection of the *Citrin* rationale performed by the court in *Lockheed*. *See* 2006 WL 2683058, at *5-6. Moreover, the *Citrin* court's reasoning might even be considered dicta, as it reached the issue in concluding that, although the plaintiff asserted a violation of paragraph (a)(5)(A)(I) of the CFAA (which contains no authorization language), the alleged conduct would also violate paragraph (a)(5)(A)(ii); thus, it is not clear that the authorization issue was fully presented to that court.

In addition, the legislative history of the statute supports the court's narrow interpretation. The CFAA was intended as a criminal statute focused on "hackers" who trespass into computers, and the statute deals with unauthorized access in committing computer fraud rather than the mere use of a computer. *See id.* at 965-66 (citing legislative history). Moreover, in 1986 Congress amended the CFAA to substitute "exceeds authorized access" for the phrase "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." The stated intent of that change was to eliminate the reference to the defendant's "purpose", thereby removing a murky ground for liability. *See id.* at 966 (quoting *Werner-Masuda*, 390 F. Supp. 2d at 499 n.12 (quoting legislative history)). As noted by the court in *Shamrock*, this core language, focusing on access instead of purpose, remains unchanged today. *See id.*[4]

An interpretation based on agency principles would inappropriately expand federal jurisdiction by broadly sweeping in conduct in which a defendant accesses a company computer with "adverse interests." *See Shamrock*, 535 F. Supp. 2d at 967. The court is particularly persuaded by the following discussion in *Fitzgerald* concerning the vast reach of the statute under plaintiffs' interpretation:

---

[4]As another court has noted, although *Shurgard* relied heavily on legislative history, that court examined that history to reject (correctly) the argument that the CFAA applied only to "outsiders" and not to "insiders" such as present and former employees; the history cited in *Shurgard* did not address how authorization should be defined. *See Black & Decker*, 568 F. Supp. 2d at 936 n.3.

> [T]he point of access requirement, as explained by the Senate Committee, is to ensure that the use of the computer is integral to the perpetration of a fraud, in contrast to the more expansive definitions of mail and wire fraud. In the plaintiff's reading, however, the computer is not the locus of the wrongful conduct, but merely the fortuitous place where the information was obtained.
>
> Under the plaintiff's view, turning over information to a competitor would be a violation of the CFAA if obtained from a computer but not, for example, from a wastebasket, even though the defendant was permitted to access the information in the computer.

Fitzgerald, 2007 WL 2043377, at *4 & n.7 (citation omitted).

The court agrees that the CFAA cannot be read to encompass (and criminalize) frauds that happen to involve the use of a computer someplace during the course of its commission, as plaintiffs' interpretation would seem to require. Plaintiffs have not cited any authority addressing and overcoming these arguments against adoption of the *Citrin* and *Shurgard* approach. Accordingly, the court follows the line of cases that have rejected a reading of the CFAA by which the defendant's intent may determine whether he has acted without authorization or has exceeded his authorized access.[5]

The court thus turns to the particular allegations made by plaintiffs in this case. Plaintiffs note that their complaint includes allegations that Ms. Lugo and Mr. Groman both accessed a protected computer without authorization and exceeded their authorized

---

[5]As the other courts have noted, this interpretation "has the added benefit of comporting with the rule of lenity," which might apply in light of the CFAA's criminal provisions. *Lockheed*, 2006 WL 2683058, at *7 & n.11; *see also House v. Hatch*, 527 F.3d 1010, 1028 (10th Cir. 2008) ("Ambiguity concerning the ambit of criminal statutes shall be resolved in favor of lenity.") (quoting *United States v. Bass*, 404 U.S. 336, 347 (1971)).

access. It is clear from the complaint, however, that these defendants did have at least some access to plaintiffs' computer systems in their jobs at the time of the alleged wrongdoing. For instance, plaintiffs have alleged that Ms. Lugo had "limited access" to plaintiffs' confidential information; that she had access to various types of reports containing confidential information in the course of her employment; that she accessed such reports in the two months prior to her resignation; that the "manner" in which she accessed the reports was "without authorization or otherwise beyond the scope of her authorized access;" that certain reports that she accessed contained information on patients outside the geographic scope of her duties, and those reports were therefore "beyond the scope of her authorized access;" and that she "exceeded her authorized access" when she e-mailed one report to her personal e-mail account. Similarly, plaintiffs have alleged that Mr. Groman was given "limited access" to plaintiffs' confidential information; that he had access to various types of confidential information in the course of his employment; and that he "exceeded his authorized access" when he e-mailed confidential information to his personal e-mail account. These allegations make clear that the two defendants did at least have initial access to confidential information in plaintiffs' computer system in the course of their employment. Plaintiffs have certainly not alleged that the defendants had no access whatsoever to plaintiffs' computer system at the time of their allegedly wrongful acts.

Accordingly, plaintiffs have not stated a claim under the CFAA based on any instances in which Ms. Lugo or Mr. Groman accessed a protected computer without

authorization. Because a violation of paragraph (a)(5)(A)(ii) or (iii) requires such a showing, plaintiffs have not stated a cognizable claim for such a violation. Defendants' motion is therefore granted with respect to plaintiffs' claims under paragraph (a)(5) of the CFAA, and any such claims are hereby dismissed.

As noted above, a person may violate paragraphs (a)(2)(C) and (a)(4) of the CFAA if he exceeds his intially-authorized access to a protected computer by accessing particular information that he is not authorized to access. Although plaintiffs' allegations make clear that Ms. Lugo and Mr. Groman had initial authorization to access plaintiffs' computer system, plaintiffs have also alleged that their access was limited, including, with respect to Ms. Lugo, based on patients' locations. Therefore, the court concludes that plaintiffs have adequately stated a claim for violations of paragraphs (a)(2)(C) and (a)(4) of the CFAA. Plaintiffs must eventually show that Ms. Lugo and Mr. Groman were not authorized to access the particular information that they are accused of obtaining. At this stage, however, those claims survive, and defendants' motion to dismiss is denied to that extent.

III. Remaining Claims

A. Misappropriation of Trade Secrets

The court has little difficulty denying defendants' motion to dismiss as it relates to the remaining claims in plaintiffs' second amended complaint. First, the court rejects defendants' argument that plaintiffs have not sufficiently alleged a claim for

misappropriation of trade secrets, in violation of the Kansas Trade Secrets Act, K.S.A. § 60-3320 *et seq*. (Count I). "Trade secret" is defined in that statute to mean information that "(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." K.S.A. § 60-3320(4).

Defendants concede that customer lists and other information about customers can constitute trade secrets under the act, *see, e.g.*, *Dodson Int'l Parts, Inc. v. Altendorf*, 347 F. Supp. 2d 997, 1010 (D. Kan. 2004); they argue, however, that such precedent does not authorize this claim because plaintiffs have alleged only patient lists and information as trade secrets, not customer lists. This argument has no merit. The act's protection is not *limited* to customer lists, as defendants appear to suggest. Plaintiffs have sufficiently alleged that defendants misappropriated information concerning patients (not merely the patients' identities), including specifically-described reports, and that such information would be valuable to competitors; and plaintiffs have included patients among their customers at any rate. *See id.* (existence of trade secret is question of fact; relevant consideration includes information compiled with customer lists). Plaintiffs have also sufficiently (and not merely conclusorily) alleged reasonable efforts to maintain the secrecy of that information.

Finally, the court flatly rejects defendants' argument based on their response to

the court's temporary restraining order. Defendants claim that their lack of liability for misappropriation is demonstrated by the fact that they did not have any copies of two specific reports to return to plaintiffs, as required by the order. At this stage, however, defendants' own plea of innocence is not dispositive. Plaintiffs have properly alleged a violation of the trade secrets act; accordingly, the claim is not subject to dismissal at this time under Rule 12(b)(6).[6]

B. *Tortious Interference*

Defendants argue that plaintiffs have not properly alleged a claim for tortious interference with contract because plaintiffs have only "vaguely" alleged the existence of contractual relationships and have not attached those contracts to the complaint. Plaintiffs have alleged that they engaged in contractual relationships with patients, physicians, and payors, and that defendants knowingly caused contractual breaches. Defendants have not identified any authority requiring greater detail in plaintiffs' pleading. Accordingly, the court rejects this basis for dismissal.

Defendants also argue that plaintiffs' tortious interference claims (Count II) should be dismissed because plaintiffs have improperly conflated the two separate torts of tortious interference with existing contract and tortious interference with prospective

---

[6]Defendants have also repeated their argument from the injunction proceedings based on a patient's right to choose his medical provider. Defendants have never explained, however, how plaintiffs' claim trespasses upon that right. Plaintiffs' secrecy regarding information they have compiled about certain patients and their medical histories and needs does not prevent those patients from freely choosing their medical providers.

business relations. *See, e.g.*, *Sunlight Saunas, Inc. v. Sundance Sauna, Inc.*, 427 F. Supp. 2d 1032, 1070 (D. Kan. 2006) (setting forth elements for tortious interference claims under Kansas law). The court also rejects this argument. Although plaintiffs might better have pleaded the two causes of action in separate counts, they have sufficiently stated each claim. The court denies defendants' motion to dismiss this count of plaintiffs' complaint.

C. Breach of Contract

Finally, defendants' sole argument for dismissal of plaintiffs' claim against defendant Leticia Lugo for breach of contract (Count V) is based on plaintiffs' failure to rebut Ms. Lugo's affidavit (from the preliminary injunction briefing), in which she denies having used or disclosed plaintiffs' confidential information. Of course, at the pleading stage, plaintiffs have no obligation to prove its claim or rebut defendants' evidence. Plaintiffs have sufficiently alleged a breach of contract by Ms. Lugo; therefore, defendants are not entitled to dismissal of that claim under Rule 12(b)(6).[7] Defendants' motion is denied as it relates to this claim.[8]

---

[7]Defendants have not requested or argued for conversion of the motion to one for summary judgment based on their reference to the affidavit. *See* Fed. R. Civ. P. 12(d). At any rate, the court declines at this time to entertain such a motion in advance of discovery.

[8]Defendants have also moved to dismiss plaintiffs' request for injunctive relief, which plaintiffs stated as a separate count (Count III), on the basis that such request could not survive on its own once the substantive claims had been dismissed. Because the court has not dismissed all of the substantive claims, defendants' motion to dismiss (continued...)

IT IS THEREFORE ORDERED BY THE COURT THAT Defendants' Motion to Dismiss the Second Amended Complaint (Doc. # 41) is **granted in part and denied in part**. The motion is granted with respect to plaintiffs' claims for violations of section 1030(a)(5) of the CFAA, and those claims are hereby dismissed. The motion is denied in all other respects.

IT IS SO ORDERED.

Dated this 21st day of January, 2009, in Kansas City, Kansas.

s/ John W. Lungstrum
John W. Lungstrum
United States District Judge

[8](...continued)
Count III is denied as well.