Condux International, Inc. v. Haugum Doc. 17

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Condux International, Inc.,

Plaintiff,

v.

John Haugum,

Defendant.

MEMORANDUM OPINION AND ORDER
Civil No. 08-4824 ADM/JSM

Joseph M. Sokolowski, Fredrikson & Byron, PA, Minneapolis, MN, argued on behalf of Plaintiff.

Ryan B. Magnus, Zack, Jones and Magnus, Mankato, MN, argued on behalf of Defendant.

I. INTRODUCTION

On November 6, 2008, the undersigned United States District Judge heard oral argument on Defendant John Haugum's ("Haugum") Motion to Dismiss [Docket No. 5]. In its Amended Complaint [Docket No.7], Plaintiff Condux International, Inc. ("Condux") asserts a claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, as well as state law claims for breach of fiduciary duty, misappropriation of trade secrets, misappropriation of confidential information, and unfair competition. For the reasons set forth below, Haugum's Motion is granted.

II. BACKGROUND[1]

Condux, a Minnesota corporation with its principal place of business in Mankato, Minnesota, manufactures and installs tools and equipment used in the electrical utility, electrical

[1] In considering a motion to dismiss, the pleadings are construed in the light most favorable to the nonmoving party, and the facts alleged in the complaint must be taken as true. Hamm v. Groose, 15 F.3d 110, 112 (8th Cir. 1994).

Dockets.Justia.com

contracting, telecommunications, and cable television industries. Am. Compl. ¶ 1. Haugum, a resident of Mankato, Minnesota, worked for Condux in a variety of positions, most recently as the Vice President of Global Sales. Id. ¶¶ 1, 5. As vice president, Haugum was responsible for overseeing sales and marketing for the company, and accordingly, was authorized to access "confidential business information" (such as Condux's customer lists, pricing and sales data, profit-margin data, and engineering drawings of Condux's products) stored on Condux's computer system. Id. ¶¶ 5-7. Condux's employee handbook provides that confidential business information owned by Condux is not to be misappropriated by employees for their own personal benefit. Id. ¶ 9.

In November 2007, Haugum exchanged emails with a former Condux employee indicating that Haugum was considering quitting his job at Condux and starting his own competing business. Id. ¶10. Condux alleges that in December 2007, Haugum requested that an employee in Condux's information technology department send him an electronic list of Condux's customers and their contact information. Id. ¶ 11. Also, Condux asserts, Haugum downloaded over forty engineering drawings from Condux's computer system in January 2008. Id. ¶ 12. Soon thereafter, Haugum announced his resignation and left Condux on February 15, 2008. Id. ¶ 13.

Condux asserts that since Hagum's departure, it has learned that Haugum "attempted to delete evidence of his download of the engineering drawings" and discovered a document drafted by Haugum that included a resolution to develop a business to compete with Condux. Id. ¶ 14. Condux alleges further that Haugum has (1) approached one of Condux's distributors about doing business directly with Haugum; (2) exchanged emails with a former Condux employee in

May 2008 in which the former employee agreed to send Condux's confidential business information to Haugum; and (3) "directed" the former employee to delete evidence of those emails and the accompanying transfer of confidential business information. Id. ¶¶ 15-17, 25-26. Condux claims that Haugum's activities in obtaining the confidential business information were wrongful, that Haugum misappropriated the confidential business information for his own benefit in competition with Condux, and that Condux has suffered damages as a result. Id. ¶¶ 23-25, 28, 31-33.

III. DISCUSSION

A. Motion to Dismiss Standard

Haugum argues that Condux's claim under the CFAA must be dismissed for failure to state a claim on which relief can be granted. Consequently, Haugum argues, Condux's related state law claims must also be dismissed because, without the CFAA claim, supplemental jurisdiction to consider the state law claims is lacking.

In considering a motion to dismiss under Rules 12(b)(1) and 12(b)(6), courts must construe the pleadings in the light most favorable to the nonmoving party and view the facts alleged in the complaint as true. Hamm v. Groose, 15 F.3d 110, 112 (8th Cir. 1994); Ossman v. Diana Corp., 825 F. Supp. 870, 879-80 (D. Minn. 1993). Any ambiguities concerning the sufficiency of the claims must be resolved in favor of the nonmoving party. Ossman, 825 F. Supp. at 880. "A motion to dismiss should be granted as a practical matter . . . only in the unusual case in which the plaintiff includes allegations that show on the face of the complaint that there is some insuperable bar to relief." Frey v. City of Herculaneum, 44 F.3d 667, 671 (8th Cir. 1995). Under Rule 8(a) of the Federal Rules of Civil Procedure, pleadings "shall contain a

short and plain statement of the claim showing that the pleader is entitled to relief." A pleading must contain "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 127 S. Ct. 1955, 1974 (2007).

B. CFAA Claim

Count One of the Amended Complaint alleges that Haugum's activities in obtaining the confidential business information, using that information to compete with Condux, and attempting to delete evidence on Condux's computer system showing that he had obtained the confidential business information constituted violations of 18 U.S.C. § 1030. Am. Compl. ¶¶ 19-30. Specifically, Condux claims that Haugum violated susbections (a)(2), (a)(4), and (a)(5)(A) of § 1030. See Pl.'s Mem. in Opp'n to Mot. to Dismiss [Docket No. 11] at 6.

The CFAA provides criminal liability for any one of seven prohibited activities, which, broadly speaking, involve computer hacking. See 18 U.S.C. § 1030(a)(1)-(7). Although the CFAA is primarily a criminal statute, § 1030(g) provides:

> 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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B).

Courts have found the CFAA authorizes a civil cause of action for violations of specific substantive provisions in § 1030(a). Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1156 (5th Cir. 2006); see also P.C. Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, LLC, 428 F.3d 504, 511 (3d Cir. 2005) (holding that § 1030(g) authorizes civil causes of action); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2003) (holding that § 1030(g) creates a civil remedy for any person who suffers damage or loss due to a violation of the CFAA).

As an initial matter, Haugum argues that the second sentence in § 1030(g) expressly limites civil actions under the CFAA to violations of subsection (a)(5) of § 1030. Therefore, Haugum maintains, to the extent that Condux's CFAA claim is based on violations of subsections (a)(2) and (a)(4) of § 1030, those portions of his claim must be dismissed. In support, Haugum cites two decisions from this district holding that civil actions under the CFAA cannot be based on violations of subsections other than subsection (a)(5). See Cenveo Corp. v. Celumsolutions Software GMBH & Co. KG, 504 F. Supp. 2d 574, 580 (D. Minn. 2007); McLean v. Mortgage One & Finance Corp., No. Civ. 04-1158, 2004 WL 898440, at *2 (D. Minn. 2004). Condux responds that Cenveo and McLean were wrongly decided and that "the CFAA permits civil actions to be brought not only under subsection (a)(5), but also under subsections (a)(2) and (a)(4)." Pl.'s Mem. in Opp'n to Mot. to Dismiss at 7. While a civil action must allege conduct that involves one of the five factors in subsection (a)(5)(B), Condux explains, "nowhere does the statute limit civil actions to only the conduct listed under subsection (a)(5)(A)." Id. at 8.

Although the Eighth Circuit has yet to address the issue of which violations of the CFAA may support a civil action, other circuit courts have held that civil actions under the CFAA can be based on a violation of any of the subsections of § 1030(a). See Fiber Sys., 470 F.3d at 1156-57 (rejecting the argument that § 1030(g) authorizes civil actions only for violations of subsection (a)(5) as being "at odds with the language of the statute" and holding that the CFAA authorizes a civil action for violations of the other subsections of § 1030(a), so long as one of the five factors in subsection (a)(5) is "involved"); P.C. Yonkers, 428 F.3d at 512-13 ("We do not read [§ 1030(g)] . . . as limiting relief to claims that are entirely based only on subsection (a)(5),

but, rather, as requiring that claims brought under other [sub]sections must meet, in addition, one of the five number (a)(5)(B) 'tests.'"); Theofel, 359 F.3d at 1078 n.5 (holding that § 1030(g) "applies to any violation of 'this section' and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A)"). The Court recognizes that these circuit court decisions appear to conflict with the decisions in Cenveo and McLean. However, the apparent conflict in the case law need not be resolved here. Even assuming that the CFAA authorizes civil actions for violations of any of the subsections in § 1030(a), Condux has failed to allege sufficient facts to support its CFAA claim for violations of subsections (a)(2), (a)(4), and (a)(5)(A).

1. Alleged Violations of Subsections (a)(2), (a)(4), and (a)(5)(A)(ii) and (iii)

A violation of subsection (a)(2)(C)[2] occurs when a person intentionally accesses a computer without authorization or in excess of authorized access and thereby obtains information from a "protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C). Subsection (a)(4) is violated if a person knowingly and with intent to defraud, accesses a protected computer without authorization or in excess of authorized access and by means of such conduct obtains anything of value. 18 U.S.C. § 1030(a)(4). And a violation of subsection (a)(5)(A) occurs when a person intentionally accesses a protected computer without authorization and as a result of such conduct causes or recklessly causes damage. 18 U.S.C. § 1030(a)(5)(A)(ii)-(iii). Thus, violations of subsections

[2] Because there is nothing to suggest that the facts here involve computer information obtained from a financial institution, card issuer, consumer reporting agency, or department or agency of the United States, subparagraphs (A) and (B) of subsection (a)(2) are not applicable. See 18 U.S.C. § 1030(a)(2).

(a)(2) and (a)(4) require allegations that Haugum accessed Condux's computers either *without authorization or in excess of authorized access*, while violations of subsection (a)(5)(A)(ii) and (iii) require an allegation that Haugum accessed a protected computer *without authorization*.

Haugum argues his position as vice president "authorized" him to access Condux's computer system and specifically to access the confidential business information and, therefore, Condux is unable to allege that he acted without authorization or in excess of authorized access. Def.'s Mem. in Supp. of Mot. to Dismiss [Docket No. 9] at 6-7. Condux does not dispute that Haugum was permitted to access the confidential business information; instead, Condux contends that Haugum was without authorization or exceeded his authorized access because he was "never authorized . . . to access its computer system to misappropriate confidential business information for his personal competitive use." Pl.'s Mem. in Opp'n to Mot. to Dismiss at 12. In other words, Haugum was without authorization or exceeded his authorized access because of his wrongful intended use of the confidential business information.

The dispute regarding the proper interpretation of the terms "without authorization" and "exceeds authorized access" has been addressed by courts in other jurisdictions, and the courts have split on the question of whether an employee with an improper purpose may be held civilly liable under the CFAA for accessing computer information that he is otherwise permitted to access within the scope of his employment. Several courts (hereinafter referred to as the "Shurgard/Citrin line of cases") have agreed with Condux and have concluded that an employee may act "without authorization" or "in excess of authorized access" when he accesses confidential or proprietary business information from his employer's computers that he has

permission to access but then uses that information in a manner that is inconsistent with the employer's interests or in violation of contractual obligations or fiduciary duties.[3] Other courts (hereinafter referred to as the "Lockheed line of cases") have adopted a much narrower interpretation and have held that the CFAA is implicated only by the unauthorized access, obtainment, or alteration of information, not the misuse or misappropriation of information obtained with permission.[4] For the reasons discussed below, the Court concludes that the Lockheed line of cases reflects a more correct interpretation of the meaning of the terms "without authorization" and "exceeds authorized access."

As with any question of statutory interpretation, a court's starting point is the statute's plain language. Watson v. Ray, 192 F.3d 1153, 1155 (8th Cir. 1999). The CFAA defines

---

[3] See, e.g., Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006); Pac. Aerospace & Elec., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1195-97 (E.D. Wash. 2003); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000); see also Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241, 2007 WL 2618658, at *1 (S.D.N.Y. July 24, 2007); Pharmerica, Inc. v. Arledge, No. 8:07-cv-486-T-26MAP, 2007 WL 865510, at *7-8 (M.D. Fla. Mar. 21, 2007); Int'l Sec. Mgmt. Group, Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537, at *20-21 (M.D. Tenn. June 6, 2006); Nilfisk-Advance, Inc. v. Mitchell, No. 05-5179, 2006 WL 827073, at *2 (W.D. Ark. Mar. 28, 2006); HUB Group, Inc. v. Clancy, No. 05-2046, 2006 WL 208684, at *3-4 (E.D. Pa. Jan. 25, 2006).

[4] See, e.g., Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933 (W.D. Tenn. 2008); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964 (D. Ariz. 2008); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1341-43 (N.D. Ga. 2007); B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 498-99 (D. Md. 2005); SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593,608-10 (E.D. Va. 2005); In re America Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1370-71 (S.D. Fla. 2001); see also Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006).

"exceeds authorized access" as "access[ing] a computer with authorization and [using] 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). The plain language contemplates persons who "go beyond the permitted access granted to them—typically insiders exceeding whatever access is permitted to them." Lockheed Martin, 2006 WL 2683058, at * 5; see also Black & Decker, 568 F. Supp. 2d at 935. By contrast, "without authorization" is not defined in the CFAA, but "'authorization' is commonly understood as '[t]he act of conferring authority; permission.'" Lockheed Martin, 2006 WL 2683058, at * 5 (quoting The American Heritage Dictionary 89 (1976)); see also Shamrock Foods, 535 F. Supp. 2d at 965. "[W]ithout authorization" refers to persons "below authorization, meaning those having no permission to access whatsoever." Lockheed Martin, 2006 WL 2683058, at * 5.

Relying on these understandings of the plain meaning of "exceeds authorized access" and "without authorization," the court in Diamond Power explained that both of the terms depend not on the "unauthorized *use of information,* but rather upon the . . . unauthorized *use of access*." 540 F. Supp. 2d at 1343 (emphasis added). The interpretation advanced by Condux and articulated in the Shurgard/Citrin line of cases incorrectly focuses on what a defendant did with the information after he accessed it (use of information), rather than on the appropriate question of whether he was permitted to access the information in the first place (use of access). As one court explained, "this interpretation reads section (a)(4) as if it said 'exceeds authorized use' instead of 'exceeds authorized access.'" Brett Senior, 2007 WL 2043377, at *4. Had Congress intended to target how a person makes use of information, it would have explicitly provided language to that effect. Indeed, one need look no further than to another subsection of § 1030 to

see such explicit language that targets a person's use of information. See 18 U.S.C. § 1030(a)(1) (prohibiting the access without authorization or in excess of authorized access and subsequent "communicat[ion], deliver[y], or transmi[ssion]" of certain information.) Thus,"the plain language of [subsections (a)(2), (a)(4), and (a)(5)(A)(ii) and (iii)] target 'unauthorized procurement or alteration of information, not its misuse or misappropriation.'" Shamrock Foods, 535 F. Supp. 2d at 965 (quoting Brett Senior, 2007 WL 2043377, at *3).

The legislative history of the CFAA supports this interpretation, which focuses on the propriety of the access of information rather than on the propriety of the use of information. The 1984 House Committee explained that the conduct prohibited by the CFAA is "analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense." H.R. Rep. No. 98-894, at 20 (1984). In 1986, Congress amended the CFAA to substitute the term "exceeds authorized access" for the term "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." S. Rep. No. 99-342, at 9. The stated intent of the amendment was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,'" and to thereby "remove[] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.'" S. Rep. No. 99-432, at 21.

Furthermore, the Court agrees with the Lockheed line of cases that principles of statutory construction require the adoption of a narrow view of the CFAA. When a court is confronted with two rational readings of a criminal statute, it is required to construe the statute in favor of

the defendant. See United States v. Santos, ___ U.S. ___, 128 S. Ct. 2020, 2025 (2008). This rule of lenity applies to civil statutes that have criminal applications because courts are required to interpret such statutes consistently, regardless of whether the court encounters the statute in a criminal or noncriminal context. Clark v. Martinez, 543 U.S. 371, 380 (2005). The CFAA has both civil and criminal applications and given the two proposed readings of the statute—(1) the broad interpretation of "without authorization" and "exceeds authorization" articulated in the Shurgard/Citrin line of cases and (2) the narrower interpretation advanced by the Lockheed line of cases—the rule of lenity requires the Court to favor the narrower interpretation.

Finally, but of equal importance, the interpretation adopted by the Shurgard/Citrin line of cases would create a federal cause of action for an employer whenever an employee accesses information on the company computer with intentions of using that information in a manner adverse to the employer's interests or in violation of a duty of loyalty. See Citrin, 440 F.3d at 420-21. "The Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA." Shamrock Foods, 535 F. Supp. 2d at 967; see also Cleveland v. United States, 531 U.S. 12, 24-25 (2000) (rejecting a "sweeping expansion of federal criminal jurisdiction in the absence of a clear statement by Congress").

There is no dispute that Haugum, as Vice President of Global Sales, was permitted to access Condux's computers. Therefore, he was not "without authorization" when he accessed the computers. Additionally, because he was permitted to access the specific confidential business information, he did not "exceed authorized access." In Werner-Masuda, the court noted that "the gravamen of [the] complaint is not so much that [the defendant] accessed the

information . . ., but rather what she did with the information once she obtained it. The . . . CFAA, however, do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access." 390 F. Supp. 2d at 499. Similarly, the court in Black & Decker explained:

> Clearly, the Plaintiff objects not to [the] accessing of the information, but to [the] later misuse thereof. Thus, while the Complaint includes claims that the Defendant breached both the Employee Access Agreement and the confidentiality agreements by allegedly disclosing . . . trade secrets and proprietary information, . . . no facts alleged indicate that Smith exceeded the access he was granted by the Plaintiff or that he accessed the data without authorization.

568 F. Supp. 2d at 936. Here too, the conduct at the heart of the dispute is not the access of the confidential business information but rather the alleged subsequent misuse or misappropriation of that information. Such allegations, however, are not sufficient to state a claim for violations of subsections (a)(2), (a)(4), or (a)(5)(ii) or (iii).

2. Alleged Violations of subsections (a)(5)(A)(i)

A violation of subsection (a)(5)(A) also occurs when a person knowingly causes the transmission of a program, information, code, or command, and as a result, intentionally causes damage without authorization to a protected computer. 18 U.S.C. § 1030(a)(5)(A)(i). Unlike subsections (a)(2), (a)(4), and (a)(5)(ii) and (iii), which are all predicated on unauthorized *access*, a violation of subsection (a)(5)(A)(i) is predicated on unauthorized *damage*. Haugum argues that Condux has not and cannot allege such damage, as that term is defined by the CFAA, and, therefore, Condux cannot state a claim based on a violation of subsection (a)(5)(A)(i).

The CFAA defines the term "damage" as meaning "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Haugum

contends that there have been no allegations of such impairment to the integrity or availability of data, a program, a system, or information. Further, he claims, "it appears that [Condux] always was able to access the information alleged to have been misappropriated by [Haugum]." Def.'s Mem. in Supp. of Mot. to Dismiss [Docket No. 9] at 7-8. In response, Condux relies on cases holding that allegations of an employee's downloading or copying of confidential business information from an employer's secure computer system is sufficient to allege impairment to the integrity of data or information. See, e.g., Shurgard, 119 F. Supp. 2d at 1126-27 (concluding that allegations of infiltrating a computer network and gathering and disseminating confidential information impaired the integrity of data even though no data was physically changed or erased); Pac. Aerospace, 295 F. Supp. 2d at 1195-97 (concluding that "caselaw supports an employer's use of the CFAA's civil remedies to sue [its] former employees . . . who seek a competitive edge through wrongful use of information [obtained] from the former employer's computer systems").

Not surprisingly considering the previously discussed conflicts regarding the interpretation and application of the CFAA, there is disagreement among courts on whether the mere unauthorized copying, downloading, or emailing of confidential or proprietary information is sufficient to allege impairment of the integrity of data, a system, or information. In Garelli Wong & Assocs., Inc. v. Nichols, the court, disagreeing with Shurgard and Pac. Aerospace, held that the misappropriation of trade secrets through the use of a computer, by itself, is insufficient to allege impairment to the integrity or availability of data, a system, or information. 551 F. Supp. 2d 704, 709-710 (N.D. Ill. 2008); see also Sam's Wines & Liquors, Inc. v. Hartig, No. 08 C 570, 2008 WL 4394962, at *3 (N.D. Ill. Sept. 24, 2008) (finding the reasoning in Garelli

Wong persuasive and declining to follow Shurgard); Lockheed Martin, 2006 WL 2683058, at *3, 8 (concluding that "[t]he copying of information from a computer onto a CD or PDA is a relatively common function that typically does not, by itself, cause permanent deletion of the original computer files,"and thus, does not, by itself, constitute "damage" under the CFAA). In reaching this conclusion, the Garelli Wong court relied heavily on an unpublished case discussing the meaning of the term "integrity." See 551 F. Supp. 2d at 709 (citing Resdev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-CV-1374, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005). In Resdev, the court explained:

> Another thing that detracts from Shurgard is its heavy reliance on legislative history. For instance, based on legislative history, Shurgard adopted an unusual and extraordinary interpretation of the word "integrity" within the CFAA's definition of "damage" . . . . It found "integrity" to contemplate the loss of a trade secret's exclusivity value. "Integrity," however, ordinarily means "wholeness" or "soundness," Oxford English Reference Dictionary 731 (Rev. 2d ed. 2002), and contemplates, in this context, some diminution in the completeness or useability of data or information on a computer system. This Court finds no meaningful ambiguity that might weigh in favor of relying on legislative history . . . .

2005 WL 1924743, at *5 n.3 (quotations omitted); see also Worldspan, L.P. v. Orbitz, LLC, No. 05 C 5386, 2006 WL 1069128, at *5 (N.D. Ill. Apr. 19, 2006) (agreeing with Resdev regarding the ordinary meaning of "damage" and "integrity" and rejecting the argument that "the mere 'taking of information' constitutes 'damage' under the CFAA").

The Court finds the reasoning in Garelli Wong and Resdev persuasive. The "damage" contemplated by subsection (a)(5)(A)(i) requires some "diminution in the completeness or useability of data or information on a computer system." Resdev, 2005 WL 1924743, at *5 n.3. Here, there have been no allegations that Haugum diminished the "completeness or useability"

of the computer data or information he obtained. Haugum's alleged activities may well have compromised or diminished the confidentiality, exclusivity, or secrecy of the proprietary information that had been expressed in the form of computer data. But the plain language of the statute requires some alteration of or diminution to the integrity, stability, or accessibility of the computer data itself. In other words, the complained of activity must have an effect on the binary coding used to create, store, and access computerized representations of information.

Condux also claims that it has sufficiently pleaded damage by its allegation that "[b]y deleting or attempting to delete evidence that he misappropriated Condux's Confidential Business Information, Haugum impaired both the integrity and availability of that data and information." Pl.'s Mem. in Opp'n to Mot. to Dismiss at 15. An allegation that Haugum did in fact delete computer data would perhaps be sufficient under the above interpretation of "damage." However, a review of Condux's Amended Complaint reveals no allegation of actual deletion. Condux repeatedly alleges that Haugum *attempted* to delete evidence of his computer activities, but at no time does Condux allege that Haugum accomplished a deletion of anything. See Am. Compl. ¶¶ 14, 26, 29, 30, 31, 32. In its brief submitted in opposition to Haugum's motion, Condux explains: "It appears that Haugum deleted evidence of his wrongful conduct, but evidence of the deletion and what Haugum was attempting to delete remained on the computer system." Pl.'s Mem. in Opp'n to Mot. to Dismiss at 15 n.7. To the extent that this could be viewed as an allegation that Haugum succeeding in deleting data (rather than merely attempting to do so), there is no similar allegation in the Amended Complaint, which refers only to attempted deletions. Accordingly, the allegation in the briefing may not be considered in

deciding a Rule 12 motion to dismiss.[5] See Enervations, Inc. v. Minn. Mining & Mfg. Co., 380 F.3d 1066, 1069 (8th Cir. 2004).

In sum, Condux is unable to allege that Haugum was "without authorization" or that he "exceeded authorized access," and, thus, the claim for violations of §§ 1030(a)(2), (a)(4), and (a)(5)(ii) and (iii) fail. And because there is no allegation of the "damage" contemplated by the CFAA, the claim for a violation of § 1030(a)(5)(A)(i) likewise fails. Condux's allegations that Haugum acted wrongfully in accessing the confidential business information to later use for his own benefit may very well support other claims; indeed, they are the basis for the state law claims of misappropriation of trade secrets, misappropriation of confidential business information, breach of fiduciary duties, and unfair competition. But they are not allegations that will support a CFAA claim.

C. State Law Claims

The sole jurisdictional basis asserted for Counts Two through Five is 28 U.S.C. § 1367(a), which permits a district court to exercise supplemental jurisdiction over claims that are part of the same case or controversy as claims that fall within its original jurisdiction. See Am. Compl. ¶ 3; Pl.'s Mem. in Opp'n to Mot. to Dismiss at 18-19. When a district court has dismissed all claims over which it has original jurisdiction, the court may in its discretion decline to exercise supplemental jurisdiction over the remaining claims. 28 U.S.C. § 1367(c)(3); Gibson v. Weber, 433 F.3d 642, 647 (8th Cir. 2006). Having dismissed Count One (the CFAA claim), the sole count within the Court's original jurisdiction, the Court declines to exercise

[5] Even if the allegation had been properly raised, it is unclear whether it would be sufficient to show "damage." See Lockheed Martin, 2006 WL 2683058, at *8 (suggesting that an allegation of "*permanent* deletion or removal" is necessary to satisfy the CFAA's definition of "damage") (emphasis added).

supplemental jurisdiction over Condux's state law claims and dismisses those claims without prejudice.

IV. CONCLUSION

Based upon the foregoing, and all the files, records, and proceedings herein, **IT IS HEREBY ORDERED** that:

1. Defendant John Haugum's Motion to Dismiss [Docket No. 5] is **GRANTED**;
2. Count One of Plaintiff Condux International, Inc.'s Amended Complaint [Docket No. 7] is **DISMISSED WITH PREJUDICE**; and
3. Counts Two, Three, Four, and Five of the Amended Complaint [Docket No. 7] are **DISMISSED WITHOUT PREJUDICE**.

LET JUDGMENT BE ENTERED ACCORDINGLY.

BY THE COURT:

s/Ann D. Montgomery
ANN D. MONTGOMERY
U.S. DISTRICT JUDGE

Dated: December 15, 2008.