

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

MATHEY DEARMAN, INC.,)	
)	
Plaintiff,)	
v.)	
)	Case No. 18-cv-250-GKF-JFJ
H&M PIPE BEVELING MACHINE CO.,)	
JOSHUA WILSON, BRANDON BOYD,)	
and RYAN DAY,)	
)	
Defendants.)	

OPINION AND ORDER

This matter comes before the Court on the Motion to Dismiss Certain Claims in the First Amended Complaint for Failure to State a Claim [Doc. No. 61] of defendants H&M Pipe Beveling Machine Co., Joshua Wilson, Brandon Boyd, and Ryan Day. For reasons discussed below, the motion is granted in part and denied in part.

I. Allegations of the First Amended Complaint¹

Mathey manufactures and markets cutting and beveling machines, as well as clamping, aligning, and reforming systems for pipe and tubing applications. Its products are used in the construction and maintenance of pipelines, power plants, refineries, petrochemical plants, marine and offshore facilities, food and beverage plants and other projects. [Doc. No. 54, ¶ 11]. The market is highly competitive and secretive and therefore Mathey depends on its ability to maintain the secrecy of its confidential, proprietary, and trade secret information, including pricing information, cost information, and sales and market strategies (“Confidential Information”). [Id. ¶ 13]. To that end, Mathey expends significant effort and expense to protect

¹ The First Amended Complaint is over fifty (50) pages long and includes over three hundred and fifty (350) paragraphs. For the sake of brevity, the court summarizes only those allegations relevant to the Motion to Dismiss.

its Confidential Information. [Id. ¶¶ 16-21]. For example, Mathey’s corporate “Dropbox” account is password protected and only certain employees are provided access to the account. [Id. ¶¶ 20-21].

Brandon Boyd began working for Mathey in August 2008. From July 15, 2015 to his voluntary resignation on March 29, 2018, Boyd served as Mathey’s Global Sales Director. [Id. ¶ 23]. In the course of his employment, Mathey provided Boyd with password-protected, administrator access to its corporate Drop Box account and other Confidential Information. [Id. ¶¶ 26-27]. Mathey also provided Boyd a password-protected laptop and smartphone to use in connection with his Mathey employment. [Id. ¶ 42].

Joshua Wilson began working for Mathey in November of 2012. [Id. ¶ 31]. Beginning in September of 2016 until his voluntary resignation on March 29, 2018, Wilson served as Area Sales Manager. [Id. ¶ 31]. From November of 2017 until his resignation, Wilson also served as the Technical Sales Manager. [Id. ¶ 32]. In the course of his employment, Mathey provided Wilson access to “Team Folders” on Dropbox, including “Quotes,” “Custom Layouts,” “Sales Mangers” and “Mathey Rep Resource.” [Id. ¶¶ 34-35]. Mathey also provided Wilson a password-protected laptop and smartphone to use in connection with his employment with Mathey. [Id. ¶¶ 43-44].

In mid-January 2018, Boyd and Wilson met and/or communicated with Ryan Day, H&M’s Vice President of Sales and Marketing, regarding potential employment with H&M—Mathey’s direct competitor. [Id. ¶¶ 45-46]. Although H&M did not have any open positions for Boyd and Wilson due to the company’s smaller sales volume, Day and H&M decided to hire Boyd and Wilson to gain access to Mathey’s Confidential Information and competitive advantages. [Id. ¶¶ 47-50]. On February 23, 2018, H&M made written offers of employment to

Boyd and Wilson. [Id. ¶ 67]. However, Boyd rejected the first offer, asserting he was not in a position to regress from his current position and compensation package with Mathey. [Id. ¶¶ 69-70]. Wilson also rejected H&M's first offer of employment. [Id. ¶ 72]. Day continued to negotiate with Boyd and Wilson. [Id. ¶¶ 74-76]. During this time, Boyd and Wilson began copying Mathey's Confidential Information for later use. On March 5, 2018, Boyd created a folder in Mathey's corporate Dropbox entitled "Transition," and eventually moved thousands of confidential documents into the folder. [Id. ¶¶ 81-86]. Boyd and Wilson utilized their Mathey-provided Dropbox account credentials, laptop, and smartphone to gain access to Mathey's Confidential Information. [Id. ¶¶ 81-82, 86, 120-21, and 124].

On March 18, 2018 and March 19, 2018, Boyd and Wilson, respectively, accepted employment with H&M. [Id. ¶¶ 91 and 96]. Neither Boyd nor Wilson informed Mathey of their future employment plans. [Id. ¶¶ 94 and 100]. In fact, during their final days of employment with Mathey, Boyd and Wilson began operating in H&M's interests and directly contrary to Mathey's interests. [Id. ¶ 102]. On March 22, 2018, Boyd used his personal e-mail account to send to Day's personal e-mail account Mathey's Confidential Information. [Id. ¶¶ 103-107]. Upon receiving the documents, Day saved them to his H&M computer, then copied the "Mathey Dearman" folder from that computer to a thumb drive with identification number 90008254654B8E24&0, and deleted the folder from his H&M computer. [Id. ¶¶ 109-111]. Mathey alleges that Day subsequently instructed Wilson and Boyd regarding the additional types of confidential information and trade secrets that he would like to receive. [Id. ¶ 109]. Between March 22, 2018 and March 29, 2018, Boyd and Wilson allegedly copied more than 80,000 Mathey confidential files to external hard drives to take with them to H&M. [Id. ¶¶ 112-118].

In addition to copying files, prior to returning his company-provided laptop computer to Mathey, Boyd deleted thousands of Mathey files and deleted significant amounts of e-mail data from his Mathey-provided e-mail account. [Id. ¶¶ 137 and 140]. Boyd also purposefully reset his company-provided smartphone to factory settings before returning it to Mathey, resulting in the erasure of Mathey information. [Id. ¶ 139]. Boyd was not authorized to permanently delete Mathey's documents. [Id. ¶ 362].

On April 2, 2018, Boyd and Wilson officially began working for H&M as Director of Sales Marketing and Technical Director, respectively. [Id. ¶ 155]. That day, with Day's and H&M's approval, Boyd accessed and copied Mathey's Confidential Information to H&M computers. [Id. ¶¶ 157-159]. Mathey alleges that Boyd, Wilson, and Day used the misappropriated Mathey Confidential Information and trade secrets to restructure H&M's business, including pricing, discounts, and sales representative relationships to H&M's benefit and Mathey's detriment. [Id. ¶ 142].

Based on these allegations, the Amended Complaint asserts the following claims against all defendants: (1) misappropriation of trade secrets under the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836; (2) misappropriation of trade secrets under the Oklahoma Uniform Trade Secrets Act, 78 OKLA. STAT. § 85 et seq.; (3) common law misappropriation of business information; and (4) civil conspiracy. Additionally, the Amended Complaint asserts claims for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and breach of fiduciary duty against Boyd and Wilson.

II. Motion to Dismiss Standard

In considering a motion to dismiss under FED. R. CIV. P. 12(b)(6), a court must determine whether the plaintiff has stated a claim upon which relief can be granted. 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, 570 (2007). The plausibility requirement “does not impose a probability requirement at the pleading stage; it simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence” of the conduct necessary to make out the claim. *Id.* at 556. “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*, 556 U.S. 662, 678 (2009). The court “must determine whether the complaint sufficiently alleges facts supporting all the elements necessary to establish an entitlement to relief under the legal theory proposed.” *Lane v. Simon*, 495 F.3d 1182, 1186 (10th Cir. 2007) (quoting *Forest Guardians v. Forsgren*, 478 F.3d 1149, 1160 (10th Cir. 2007)).

III. Analysis

Defendants move to dismiss the injunctive relief requested in paragraphs 6(d) and 6(e) of the Amended Complaint’s Prayer for Relief, as well as Count V, plaintiff’s claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The court will separately consider each request.

A. Injunctive Relief Pursuant to the Defend Trade Secrets Act

Defendants ask the court to dismiss the injunctive relief requested in paragraphs 6(d) and 6(e) of the Amended Complaint’s Prayer for Relief, which seek the following relief:

- d. Boyd and Wilson refrain from working for any competitor of Mathey, including H&M, in the same or similar capacity as their employment with Mathey, or in any capacity in which Boyd and Wilson inevitably would disclose Mathey’s confidential, proprietary, or trade secret information.
- e. Day to cease his employment with H&M and refrain from working for any competitor of Mathey in any capacity in which he inevitably or necessarily would disclose Mathey’s confidential, proprietary or trade secret information.

[Doc. No. 54, p. 56]. Defendants argue that the requested relief exceeds the scope of the federal Defend Trade Secrets Act, 18 U.S.C. § 1836, and the Oklahoma Uniform Trade Secrets Act, 78 OKLA. STAT. § 85 et seq. and therefore dismissal is appropriate under FED. R. CIV. P. 12(b)(6).

However, “[t]he Tenth Circuit has held that a motion to dismiss is not a proper vehicle for addressing a prayer for relief, which is not part of the cause of action.” *Reininger v. Oklahoma*, 292 F. Supp. 3d 1254, 1266 (W.D. Okla. 2017) (citing *Coll v. First Am. Title Ins. Co.*, 642 F.3d 876, 901 (10th Cir. 2011)). See also *U.S. Commodity Futures Trading Comm’n v. Bradley*, 408 F. Supp. 2d 1214, 1223 (N.D. Okla. 2006) (“[T]he only issue on a motion to dismiss is whether the claim as stated would give the plaintiff a right to any relief, rather than to the particular relief demanded.”) (quoting *Cassidy v. Millers Cas. Ins. Co. of Texas*, 1 F. Supp. 2d 1200, 1214 (D. Colo. 1998)); *Autry v. Cleveland Cnty. Sheriff’s Dep’t*, No. CIV-15-1167-D, 2018 WL 719044, at *3 n.6 (W.D. Okla. Feb. 5, 2018). Defendants do not challenge the adequacy of plaintiff’s DTSA or OUTSA claims. Rather, defendants’ Rule 12(b)(6) motion only challenges the requested relief. Because a Rule 12(b)(6) is not the proper vehicle for addressing a prayer for relief, dismissing plaintiff’s requested injunctive relief at this time would be premature and is not warranted. Thus, defendants’ motion to dismiss the injunctive relief requested in paragraphs 6(d) and 6(e) of the Amended Complaint’s Prayer for Relief is denied.

B. Count V – Computer Fraud and Abuse Act, 18 U.S.C. § 1030

Defendants also seek dismissal of Count V, plaintiff’s claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“CFAA”). Although primarily a criminal statute, “[s]ection 1030 allows a person who suffers damage or loss to maintain a civil action for compensatory damages against the violator if the offense caused loss to the victim of at least \$5,000.” *Tank Connection, LLC v. Haight*, 161 F. Supp. 3d 957, 968 (D. Kan. 2016). “[E]ach subsection of §

1030 addresses a different type of harm.” *United States v. Willis*, 476 F.3d 1121, 1126 (10th Cir. 2007). Plaintiff asserts Boyd and Wilson violated §§ 1030(a)(4) and 1030(a)(5). These sections provide as follows:

(a) Whoever –

- (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, 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;
- (5) (A) 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;
- (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
- (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

shall be punished as provided in subsection (c) of this section.

Defendants argue that the Amended Complaint fails to state a plausible CFAA claim because plaintiff fails to allege that Boyd or Wilson accessed a protected computer “without authorization.” See [Doc. No. 61, pp. 4-6]. Subsection (a)(4) of § 1030 applies only where a defendant knowingly accesses a protected computer “without authorization” or if the access “exceeds authorized access.” 18 U.S.C. § 1030(a)(4). Similarly, subsections (a)(5)(B) and (a)(5)(C) apply only to access “without authorization.” 18 U.S.C. § 1030(a)(5). The court will separately consider whether the Amended Complaint plausibly alleges that Boyd and Wilson

acted “without authorization” for purposes of §§ 1030(a)(4), (a)(5)(B), (a)(5)(C), and whether they “exceed[ed] authorized access” pursuant to § 1030(a)(4).

The CFAA does not define “without authorization.” However, courts generally interpret the phrase to mean “without permission.” See *Tank Connection, LLC*, 161 F. Supp. 3d at 968-69. Thus, an employee “accesses a computer ‘without authorization’ when he gains admission to a computer without approval.” *Cent. Bank & Trust v. Smith*, 215 F. Supp. 3d 1226, 1232 (D. Wyo. 2016). The Amended Complaint includes bare recitals that Boyd and Wilson accessed plaintiff’s Confidential Information “without authorization.” See, e.g., [Doc. No. 54, ¶ 355]. However, the Amended Complaint includes no factual averments in support thereof. Rather, the Amended Complaint alleges:

27. Among other things, Mathey provided Boyd with password-protected, administrator access to its corporate Dropbox account. As the administrator, Boyd was the only sales employee, and one of the few Mathey employees, with access to all files and folders in the Dropbox account, including Board of Directors documents, extensive sales documents such as performance, strategy, and forecast documents, employee and contractor performance and compensation documents, and pricing and profit information.

34. In the course of his Mathey employment, Wilson had access to and benefitted from Mathey’s highly sensitive, proprietary and trade secret information, including, for example, quotes and bids, pricing worksheets, cost information, customer information and engineering and technical information. Wilson also had access to Mathey’s equipment schematics, including custom layouts Mathey designed for customers.

35. Wilson had full access to Mathey’s “Team Folders” on Dropbox, including Team Folders entitled: “Quotes,” “Custom Layouts,” “Sales Managers” and “Mathey Rep Resource,” and all of the resources contained therein.

42. Mathey provided Boyd with a password-protected laptop computer and smartphone to use in connection with his employment with Mathey. Mathey owned the account for the smartphone it provided Boyd.

43. Mathey similarly provided Wilson with a password-protected laptop computer and smartphone to use in connection with his employment with Mathey. Mathey owned the account for the smartphone it provided Wilson.

[Doc. No. 54, ¶¶ 27, 34, 35, 42, 43]. The Amended Complaint alleges that Boyd and Wilson utilized their Mathey-provided Dropbox credentials, laptop, and smartphone to gain access to plaintiff's Confidential Information. [Id. ¶¶ 81-82, 86, 120-21, and 124]. The Amended Complaint includes no allegations from which the court may reasonably infer that, during their Mathey employment, plaintiff did not permit Boyd or Wilson access to the Dropbox account, laptop, or smartphone. Rather, the court can infer only that plaintiff permitted Boyd and Wilson's access. Thus, the Amended Complaint fails to state a plausible claim pursuant to § 1030(a)(5)(B) and § 1030(a)(5)(C).

Plaintiff argues, however, that Boyd and Wilson exceeded the scope of their authorization by accessing Mathey's Confidential Information for an improper purpose—specifically, to benefit H&M. See [Doc. No. 68, pp. 9-10]. With regard to “exceeds authorized access,” the statute defines the phrase to mean “access[ing] 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). As recognized by the parties, the meaning of that definition created a Circuit split relative to which the Tenth Circuit has expressed no opinion. Defendants urge the court to adopt the narrow approach articulated by the Second, Fourth, and Ninth Circuits that focuses on the objective grant of access by the employer, not on the defendant's intent or purpose in accessing the information. See *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 980 (D. Colo. 2016). Not surprisingly, plaintiff argues the court should adopt the broader approach utilized by the First, Fifth, Seventh, and Eleventh Circuits, pursuant to which an employee may be liable under the CFAA for accessing a protected computer for an improper purpose. See *id.*

The court is persuaded by those cases adopting the narrow approach, and applies this approach to determine whether the Amended Complaint states a plausible claim under § 1030(a)(4). Although not binding upon this court, the court notes that district courts in this Circuit uniformly apply the narrow inquiry to determine whether a defendant exceeded his authorization for purposes of the CFAA. See *Tank Connection, LLC*, 161 F. Supp. 3d at 969; *US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009); *Cloudpath Networks, Inc.*, 157 F. Supp. 3d at 983; *Cent. Bank & Trust*, 215 F. Supp. 3d at 1232-33; *Farmers Bank & Trust v. Witthuhn, N.A.*, No. 11-2011-JAR, 2011 WL 4857926, at **4-5 (D. Kan. Oct. 13, 2011); *Giles Constr., LLC v. Tooele Inventory Sols, Inc.*, No. 12-CV-37, 2015 WL 3755863, at *3 (D. Utah June 16, 2015); *Koch Indus., Inc. v. Does*, No. 10-CV-1275-DAK, 2011 WL 1775765, at *8 (D. Utah May 9, 2011). The court is further persuaded by, and agrees with, District Judge Martinez who concluded the plain language of the statute suggests “that Congress only meant to deter certain means of access (such as through hacking), not certain purposes for access.” *Cloudpath Networks, Inc.*, 157 F. Supp. 3d at 983 (emphasis in original); see also *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (“The plain language of the statute therefore indicates that ‘authorization’ depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant’s liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer.”). Finally, the court shares the Ninth Circuit’s concern that, because § 1030 is primarily a criminal statute, applying a broad interpretation would impose unexpected criminal liability on defendants. See *Brekka*, 581 F.3d at 1134-35.

Based on the factual allegations of the Amended Complaint, the only reasonable inference to be drawn by this court is that Wilson and Boyd “exceed[ed] authorized access” by

accessing plaintiff's computers, drive, and information for an improper purpose. However, the defendants' purpose in accessing the information is irrelevant to liability pursuant to § 1030(a)(4). The Amended Complaint includes no allegations that either Boyd or Wilson accessed information for which plaintiff did not provide permission. Thus, the Amended Complaint fails to state a plausible claim for relief under § 1030(a)(4).

However, the Amended Complaint also alleges a general violation of § 1030(a)(5). Plaintiff argues that defendants' motion to dismiss improperly conflates the various subsections of (a)(5), and that the Amended Complaint states a plausible claim for relief pursuant to § 1030(a)(5)(A) because that subsection does not require access of a protected computer "without authorization." The court agrees.

Subsection 1030(a)(5)(A) prohibits conduct that "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." 18 U.S.C. § 1030(a)(5)(A). Plaintiff points to no Tenth Circuit authority considering whether unauthorized access constitutes an element of § 1030(a)(5)(A) liability. However, the majority of courts construing § 1030(a)(5)(A) have concluded that access "without authorization" is not an element of § 1030(a)(5)(A) liability. See *B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) ("Section 1030(a)(5)(A)[] is not predicated upon unauthorized access of a protected computer. Instead, it is predicated upon unauthorized damage to a computer.") (emphasis in original); *Wentworth-Douglas Hosp. v. Young & Novis Prof'l Ass'n*, No. 10-CV-120-SM, 2010 WL 3023331, at *3 (D.N.H. July 28, 2010) ("Unauthorized damage and/or unauthorized transmission are elements of a cause of action under § 1030(a)(5)(A); unauthorized access to the protected computer is not."); *United States v. Stratman*, No. 13-CR-3075, 2013 WL 5676874, at *2 (D. Neb. Oct. 18,

2013) (“There is, in fact, nothing in § 1030(a)(5)(A) to suggest that access to a protected computer is an element of the offense at all, whether or not it was authorized.”); *United States v. Thomas*, No. 13-CR-227, 2016 WL 10988775, at *2 (E.D. Tex. Nov. 8, 2016); *Cheney v. IPD Analytics, L.L.C.*, No. 08-23188-CIV, 2009 WL 1298405, at *7 (S.D. Fla. Apr. 16, 2009) (“Therefore, the fact that [defendant] may have had initial authorization to use the computer does not immune him from liability under subsection 1030(a)(5)(A) for causing damage to the computer.”) (emphasis in original); *Lifeline Anesthesia, PLLC v. Wolfe*, No. 12-CV-02662-JPM-CGC, 2012 WL 13026748, at *3 (W.D. Tenn. Nov. 1, 2012). But see *Advanced Aerofoil Techs., AG v. Todaro*, No. 11-CIV-9505-ALC-DCF, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013).²

Defendants argue that because both § 1030(a)(5)(A) and § 1030(a)(4) include the phrase “without authorization,” the same construction should be applied to both subsections. However, courts generally reason that, in the context of § 1030(a)(5)(A), “without authorization” modifies the phrase “intentionally causes damage.” Thus, “one who is authorized to access a system, but not authorized to damage it, violates the statute by intentionally damaging it ‘without authorization.’” *Stratman*, 2013 WL 5676874, at *1. The court is persuaded by *Stratman*’s construction of the statute, which distinguished § 1030(a)(5)(A)—prohibiting “intentionally caus[ing] damage without authorization”—and §§ 1030(a)(5)(B), (a)(5)(C), which prohibit “intentionally access[ing] a protected computer without authorization” that results in damage. *Id.* Viewing § 1030(a)(5)(A) in the context of the statute as a whole, the court concluded:

² In fact, in a case cited by defendants for the proposition that the action of an unauthorized user to improperly delete files does not state a claim for relief, the court recognized that “all of these provisions [18 U.S.C. § 1030(a)(2), (a)(4), and (a)(5)] (save for § 1030(a)(5)(A)) requires that access to the protected computer be obtained without authorization, or in excess of authorization initially granted.” *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285, 1290-91 (M.D. Fla. Mar. 2, 2012)).

It is apparent from § 1030(a)(5)(B) and (C) that Congress knew exactly how to require proof that a defendant's access to a computer was unauthorized. "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."

Id. (quoting *Dean v. United States*, 556 U.S. 568, 573 (2009)).

Based on the foregoing, the court concludes that construing § 1030(a)(5)(A) to require access "without authorization" is contrary to the statute's plain language. Therefore, the fact that Boyd and/or Wilson may have had initial authorization to access plaintiff's computers does not preclude § 1030(a)(5)(A) liability. Rather, in order to state a claim pursuant to § 1030(a)(5)(A), plaintiff need only plead "1) the knowing 'transmission' of a 'program, information, code, or command'; 2) the transmission is 'to a protected computer'; and 3) the transmission causes intentional 'damage without authorization.'" *Wentworth-Douglas Hosp.*, 2010 WL 3023331, at *3 (quoting *Hayes v. Packard Bell, NEC, Inc.*, 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001)).

Here, the court concludes that the Amended Complaint includes sufficient factual allegations to state a plausible claim for § 1030(a)(5)(A) liability against Boyd. Plaintiff alleges that Boyd "deleted thousands of Mathey documents in violation of his legal obligations to Mathey" and "returned his company-provided smartphone to factory settings thereby deleting the information contained on it in violation of his contractual and other obligations to Mathey." [Doc. No. 54, ¶¶ 137-140 and 356-57]. Thus, plaintiff asserts a knowing transmission of a command that resulted in alleged damage. Plaintiff further alleges that the smartphone and laptop were "protected computers." [Id. ¶¶ 353-54]. Finally, the Amended Complaint includes specific allegations that Boyd was not authorized to permanently delete Mathey's documents. [Id. ¶ 362]. Accordingly, the Amended Complaint states a plausible § 1030(a)(5)(A) claim against Boyd. See *N. Am. Ins. Agency, Inc. v. Bates*, No. CIV-12-544-M, 2013 WL 6150781, at *7 (W.D. Okla. Nov. 22, 2013).

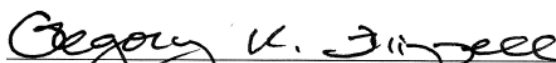
However, the Amended Complaint includes no allegations from which the court can infer that Wilson intentionally caused damage to a protected computer. See [Doc. No. 54, ¶¶ 351-362]. Thus, the Amended Complaint fails to state a plausible § 1030(a)(5)(A) claim against Wilson.

Accordingly, the court grants defendants' motion to dismiss count V, plaintiff's CFAA claim, against Wilson. Defendants' motion to dismiss plaintiff's CFAA claim against Boyd is denied as to the § 1030(a)(5)(A) claim, but is otherwise granted.

IV. Conclusion

WHEREFORE, Defendants H&M Pipe Beveling Machine Company, Inc., Joshua Wilson, Brandon Boyd, and Ryan Day's Motion to Dismiss Certain Claims in the First Amended Complaint for Failure to State a Claim [Doc. No. 61] is granted in part and denied in part. Defendants' motion is granted as to plaintiff's Computer Fraud and Abuse Act claim pursuant to 18 U.S.C. § 1030(a)(4), (a)(5)(B), and (a)(5)(C), and as to plaintiff's § 1030(a)(5)(A) claim against defendant Wilson. The motion is otherwise denied.

IT IS SO ORDERED this 5th day of September, 2018.


GREGORY K. GRIZZELL, CHIEF JUDGE