

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

Cenveo, Inc.,
Plaintiff,

v.

Sheila Rao,
Defendant.

Civil No. 3:08cv1831 (JBA)

September 30, 2009

RULING ON DEFENDANT’S MOTION TO DISMISS [Doc. # 18]

Plaintiff Cenveo, Inc., a graphics communication company headquartered in Connecticut, brings this action against its former employee, Defendant Sheila Rao, for libel, breach of fiduciary duty and the duty of loyalty, and violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030. In its Amended Complaint, Cenveo alleges that Rao obtained confidential and proprietary information that she was not authorized to access and transmitted that information by computer outside of the company for improper purposes. Defendant has moved to dismiss all the claims against her under Federal Rule of Civil Procedure 12(b)(6). For the reasons stated below, this motion will be granted as to the CFAA claim, and supplemental jurisdiction over the state-law claims will be declined.

I. Background

The Amended Complaint alleges the following facts. Ms. Rao was hired by Cenveo in 2005 as its Director of Income Taxes, and “[i]n accordance with her job responsibilities, [Ms.] Rao had access to highly sensitive, confidential information belonging to Cenveo.”

(Am. Compl. [Doc. # 17] at ¶¶ 5, 6.) The employee handbook, to which Rao acknowledges that she agreed, includes an “Electronic Resources Policy” that prohibits Cenveo employees from using its “computers, computer networks, e-mail systems and internet services” for “personal gain, . . . any other improper purpose, . . . political activity[,] . . . any other inappropriate behavior, including but not limited to transmission of . . . defamatory remarks[.]” (*Id.* ¶¶ at 7–11.) The employee handbook also contains a “Code of Ethics,” to which Rao also acknowledges that she agreed, that prohibits employees “from using, publishing or otherwise disclosing to others, either during or subsequent to their tenure with Cenveo, any confidential or proprietary information of Cenveo or its customers or suppliers.” (*Id.* at ¶ 12.)

On July 10, 2008 Ms. Rao wrote an e-mail to the Hillary Clinton presidential campaign and attached to that e-mail a letter she had written on June 10, 2008 to personal acquaintances detailing her situation at work and urging them to donate to the campaign. (*Id.* at ¶ 15 & Ex. A.) In the June 10th letter Ms. Rao stated that she was passed over for promotion “for no reason other than that [she is] a woman and the other men at the executive table would have been uncomfortable working with me.” (*Id.*) The letter lists the salary of her former supervisor and states that he “was let go” and replaced by “a new boss” who Ms. Rao said she “find[s]” to be “utterly incompetent,” at least in part because he has lesser credentials than her and is unable to use a computer efficiently. She further stated that she was upset about “this discrimination problem” and the lack of “answer” to it. (*Id.*)

According to Cenveo, on November 12, 2008—before it learned of the June 10th letter or July 10th e-mail—Ms. Rao’s attorney sent a letter to Cenveo that “contained confidential and competitive information regarding the compensation of other Cenveo employees [that] Rao was not authorized to access.” (*Id.* at ¶ 13.) On November 20th Cenveo placed Rao on paid administrative leave and launched an investigation into her computer use, during which it discovered Rao’s June 10th letter and July 10th e-mail. (*Id.* at ¶¶ 13, 15.)

Specifically, Cenveo asserts:

Cenveo brings these claims against Sheila Rao as a result of her unauthorized use of Cenveo’s computer and e-mail system for improper purposes that included her external transmission of a defamatory statement and of Cenveo’s confidential information. . . .

[The November 12th letter] contained confidential and competitive information regarding the compensation of other Cenveo employees [that] [Ms.] Rao was not authorized to access. As a result, Cenveo had reason to believe that [Ms.] Rao had accessed, disclosed and/or transmitted confidential and competitive information [that] she was not authorized to access. Accordingly, on November 20, 2008, Cenveo placed [Ms.] Rao on paid administrative leave to conduct an investigation.

Cenveo’s investigation revealed [Ms.] Rao’s unauthorized use of Cenveo’s computer and e-mail system for improper purposes that included her transmission of a defamatory statement and of Cenveo’s confidential information externally and her use of Cenveo’s computer and e-mail system for political activity. [Ms.] Rao’s transmission was without Cenveo’s approval, not in furtherance of Cenveo’s business, in contravention of Cenveo’s wishes and interests, and in violation of Cenveo’s Electronic Resources Policy and Code of Ethics.

(Am. Compl. ¶¶ 1, 13–14.) Four days later, and “[a]s a result of what Cenveo’s investigation revealed, Cenveo terminated Rao’s employment on November 24, 2008.” (*Id.* at ¶ 17.)

After it received the November 12th letter from Rao’s attorney and discovered her June 10th letter and July 10th e-mail, Cenveo hired a computer forensics expert to “investigate Rao’s actions and damage to Cenveo’s data, computers and computer networks.” (*Id.* at ¶ 18.) Cenveo does not specify the results of that investigation, but it does allege that “Ms. Rao’s actions caused loss of at least \$5,000 in value in the aggregate.” (*Id.*) At oral argument, Plaintiff’s counsel clarified Cenveo’s allegation to be that it hired the computer forensics expert to investigate how Ms. Rao obtained the confidential salary information that appeared in both counsel’s letter and her e-mail, and to be sure no damage had been done to its computer system by Ms. Rao’s conduct.

II. Discussion¹

A. Count One: Computer Fraud and Abuse Act

Cenveo claims that Ms. Rao violated the CFAA, which, in pertinent part, prohibits knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] 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.

18 U.S.C. § 1030(a)(4). Pursuant to sub-section (g), the statute’s civil enforcement mechanism, a plaintiff may only maintain an action under the CFAA if it has suffered one

¹ The Court applies the familiar Rule 12(b)(6) standard without recitation in detail. “To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Even without detailed allegations, a claim will be found facially plausible so long as “the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 129 S. Ct. at 1949. Conclusory allegations are not sufficient. *Id.* at 1949–50.

of the five harms set forth in section 1030(c)(4)(A)(i). The only harm applicable here is “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” *Id.* § 1030(c)(4)(A)(i)(I).

To state a claim for relief under the plain words of 18 U.S.C. § 1030(a)(4) Cenveo must plead factual content showing that (1) Ms. Rao accessed a protected computer without authorization or in excess of her authorization; (2) she did so knowingly and with intent to defraud; (3) through such access Ms. Rao both furthered her intended fraud and obtained something of value; and (4) Ms. Rao’s conduct caused Cenveo to suffer losses “aggregating at least \$5,000 in value.”

The CFAA defines “exceed[ing] authorized access” as “access[ing] a computer with authorization and . . . us[ing] 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). It is clear from the Amended Complaint that Ms. Rao had access to computer systems, and was authorized to access Cenveo computers (*see, e.g.*, Am. Compl. at ¶¶ 6–12), so her violation of the CFAA, if any, must be predicated on her “exceed[ing] [her] authorized access” rather than operating “without authorization.” However, Cenveo has failed to allege any facts from which an inference can be drawn that Ms. Rao accessed *by computer* the information that Cenveo alleges was in excess of her authority to access. The statute makes clear that where, as here, a claim is predicated on a defendant’s access in *excess* of authority, the CFAA prohibits use of information that is “in the computer” and “that the accesser is not entitled to so obtain or alter.” In other words, “the plain language of the statute seems to contemplate that, whatever else, . . . ‘exceeds authorized access’ would include an employee who is accessing

documents *on a computer system*[.]” *Calyon v. Mizuho Secs. USA, Inc.*, No. 07 Civ. 2241(RO), 2007 WL 2618658, * 1 (S.D.N.Y. Sep. 5, 2007) (emphasis added).²

Therefore, even if courts have split on how broadly to construe the term “authorized,”³ there is no doubt that the information obtained must be “in a computer.” Cenvéo has pleaded no facts from which it can be inferred that the confidential information

² Neither *Calyon* nor *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) is to the contrary. In both cases, the defendants–employees accessed the computer system *without authority*, either because company policy forbade access, see *Calyon*, 2007 WL 2618658, *1, or because the defendant–employee’s misappropriation of confidential information violated his duty of loyalty and thereby “terminat[ed] his agency relationship . . . and with it his authority to access the laptop,” see *Int’l Airport Ctrs., LLC*, 440 F.3d at 420.

³ Compare *LVRC Holdings LCC v. Brekka*, --- F.3d ----, No. 07-17116, 2009 WL 2928952, at * 5 (9th Cir. Sep. 15, 2009) (former employee who had e-mailed sensitive company documents that he accessed with permission to his *personal* computer did not exceed his authorized access, even if he planned to use those documents to further his own business objectives) and *Jet One Group, Inc. v. Halcyon Jet Holdings*, No. 08cv3980, 2009 WL 2524864, * 5–6 (E.D.N.Y. Aug. 14, 2009) (dismissing complaint claiming that the defendants, who were permitted to access the client lists in question in the normal course of business even, later used those client lists to compete against the plaintiff), *with Int’l Airport*, 440 F.3d at 420 (employee’s misappropriation of confidential information violated his duty of loyalty, thereby “terminating his agency relationship . . . and with it his authority to access the laptop”) and *Calyon*, 2007 WL 2618658 at * 1 (holding that employees who copied their employer’s proprietary electronic documents before their termination must have known doing so was “in contravention of the wishes and interests of the employer” and therefore exceeded the scope of their authorized access).

This Court notes that where, in a civil case, “the governing standard is set forth in a criminal statute, it is appropriate to apply the rule of lenity in resolving any ambiguity in the ambit of the statute’s coverage,” *Crandon v. United States*, 494 U.S. 152, 158 (1990), but it need not take a position on this issue because it dismisses Cenvéo’s CFAA claim on other grounds.

accessed by Ms. Rao was “in a computer.”⁴ Cenvéo has pleaded that Ms. Rao used the computer, in excess of her authority, by *transmitting* confidential and proprietary information (*see* Am. Compl. ¶¶ 1, 14), and alleges that she “accessed . . . confidential and competitive information [that] she was not authorized to access (*id.* at ¶ 13), but nowhere does Cenvéo allege that she accessed, obtained, or altered any “information *in the computer*,” 18 U.S.C. § 1030(e)(6) (emphasis added). In the absence of any factual content that Ms. Rao accessed confidential information that was “in a computer,” or even that Cenvéo’s confidential information was stored “in a computer,” the Amended Complaint lacks “facial plausibility,” *Iqbal*, 129 S. Ct. at 1949, that the CFAA was violated. Therefore, Defendant’s Motion to Dismiss will be granted as to Count One.

B. State-Law Claims

Having dismissed Cenvéo’s federal-law claim, the Court declines to exercise supplemental jurisdiction over its state-law claims. “While the statute governing supplemental jurisdiction, 28 U.S.C. § 1367, does not require dismissal of pendent state-law claims where all of the federal claims have been dismissed, *see id.* § 1367(c)(3),” *Giordano v. City of New York*, 274 F.3d 740, 754 (2d Cir. 2001) (collecting cases), the Second Circuit

⁴ Indeed, when at oral argument Plaintiff’s counsel asserted that “the defendant somehow came across highly confidential company information,” the Court pointed out that “[t]he ‘somehow’ does not get us to the computer” and that Cenvéo “[does not] make any allegation that [the information] came from computer access,” in response to which Plaintiff’s counsel acknowledged that Cenvéo is “not certain at this point whether she accessed that confidential competitive information from her computer” and instead focused on Ms. Rao’s transmission of the information “to 40 of her closest friends.” (Oral Arg. Tr. at 5.) “However, ‘[t]he purpose of discovery is to find out additional facts about a well-pleaded claim, not to find out whether such a claim exists.’” *Jones v. Capital Cities/ABC Inc.*, 168 F.R.D. 477, 480 (S.D.N.Y. 1996) (citation omitted).

