IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

ESTES FORWARDING WORLDWIDE LLC,	)	
Plaintiff,	)	
v.	)	Civil Action No. 3:16-CV-853–HEH
MARCELO S. CUELLAR,	)	
Defendant.	)	

MEMORANDUM OPINION
(Denying Defendant's Motion to Dismiss)

THIS MATTER is before the Court on Defendant Marcelo S. Cuellar's Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6), filed on December 29, 2016. (ECF No. 8.) Both parties have filed memoranda supporting their respective positions. Oral argument followed on February 8, 2017.

For the reasons stated herein, the Court will deny the Motion.

I. BACKGROUND

As required by Rule 12(b)(6) of the Federal Rules of Civil Procedure, the Court assumes Plaintiff's well-pleaded allegations to be true and views all facts in the light most favorable to him. *T.G. Slater & Son v. Donald P. & Patricia A. Brennan LLC*, 385 F.3d 836, 841 (4th Cir. 2004) (citing *Mylan Labs, Inc. v. Matkari*, 7 F.3d 1130, 1134 (4th Cir. 1993)). At this stage, the Court's analysis is both informed and constrained by the four corners of Plaintiff's Complaint. Viewed through this lens, the facts are as follows.

Plaintiff Estes Forwarding Worldwide LLC ("EFW"), a Virginia citizen, is a

transportation logistics company. (Compl. ¶¶ 3, 5, ECF No. 1.) For many of its shipments, EFW relies on "at least three different vendors: a vendor to pick up the shipment from the customer and deliver it to the airport, a vendor to transport the shipment from airport to airport, and a vendor to transport the shipment from the airport to the delivery address." (*Id.* ¶ 7.) EFW has "invested significant time and expense, and years' worth of trial, error, and experience into its decision-making processes for determining the best transportation solution for any particular shipment," which constitutes trade secrets. (*Id.* ¶ 10.) These trade secrets "are memorialized at EFW in spreadsheets and other computer information that reflect the decisions EFW has made when choosing transportation solutions for shipments, which information includes shipment information, type of freight and freight dimensions, routing decisions, vendor selection, vendor costs, and transit times." (*Id.* ¶ 11.)

In early 2010, EFW hired Cuellar to work in its new operations unit in the San Francisco area. (*Id.* ¶ 18.) In connection with his hiring, EFW required Cuellar to sign a Confidentiality Agreement wherein he "agreed to protect EFW's confidential information, which included information regarding EFW's suppliers, the details of the manner in which EFW conducts its business, pricing and billing information, work in process, computer data, and financial information." (*Id.*; *see also id.* Ex. A.)

Due to certain restrictions placed upon EFW by a customer, EFW was not permitted to install its own IT infrastructure on-site at its customer's location in San Francisco. (*See id.* ¶ 20.) Therefore, EFW "needed an alternate way for [its] representatives to share information about shipments from the location." (*Id.*) Filling

this void would serve two purposes: (1) it would allow "EFW representatives to communicate regarding each and every shipment, thereby ensuring the shipment would be delivered in accordance with the customer's requirements"; and (2) it would facilitate "recording shipment details, routing decisions, vendor selection, costs, and other shipment information further developed EFW's trade secrets." (*Id.* ¶ 21.)

Consequently, "*[a]cting on behalf of EFW and in furtherance of its business*, [Cuellar] created a Google Drive account [(the "account")] to further these purposes." (*Id.* ¶ 22 (emphasis added).) This account "was to be used by EFW's on-site representatives, each of whom had signed confidentiality agreements similar to the" one signed by Cuellar. (*Id.*) "These employees accessed the [a]ccount by logging into efwsfo@gmail.com." (*Id.* ¶ 23.) "Each day, [Cuellar] and other EFW employees on site used the [a]ccount to record information such as the shipments being handled, the routing decisions being made, the selection of vendors, and cost information." (*Id.* ¶ 24.) Cuellar and others "recorded this information in a spreadsheet, one for each day" from 2009 to 2016, when EFW ceased doing work out of its San Francisco operation.[1] (*Id.* ¶¶ 24, 30.)

EFW fired Cuellar on February 10, 2015, after which he moved to the State of Washington, where he now resides. (*Id.* ¶ 27.) In April 2015, Cuellar began working for AES Logistics, one of EFW's competitors. (*Id.* ¶ 29.) On May 19, 2016—over one year after his termination from EFW—Cuellar accessed the account from his home in Washington at approximately 2:25 a.m. local time. (*Id.* ¶ 31.) When accessing the

[1] "EFW continues to serve many other customers whose shipments originate in [San Francisco], and the [a]ccount, with its [c]onfidential [i]nformation and [t]rade [s]ecrets, continues to be of great benefit and importance to EFW." (Compl. ¶ 30.)

account without having received prior authorization to do so, Cuellar removed both a recovery phone number associated with the account and a secondary email address on file "that went directly to EFW." (*Id.* ¶ 33.) Cuellar also changed the password for the account and created an archive of the spreadsheets that it contained. (*Id.* ¶¶ 34–35.)

Later that day, after Cuellar arrived at his job at AES Logistics, he once again accessed the account at 6:28 a.m. (*Id.* ¶ 37.) He downloaded the entire archive that he created earlier that morning—containing more than 1,900 spreadsheets generated by EFW employees in the San Francisco area—deleted the account, and logged off. (*Id.* ¶¶ 37–40.) "The following month, [Cuellar] went to work at CTE Logistics, also a competitor of EFW." (*Id.* ¶ 41.) Cuellar "is still in possession of the information from the [a]ccount." (*Id.* ¶ 42.)

EFW officials received notice from Google about the unauthorized access, but that notice "only provided EFW with IP addresses for the devices or networks from which the access came, as well as approximate location information." (*Id.* ¶ 48.) Using that information, EFW was able to ascertain that the person who had accessed the account was a Comcast subscriber. (*Id.* ¶ 49.) In June 2016, EFW filed an action against Comcast in order to determine that subscriber's identity. (*Id.* ¶ 50.) Comcast sent Cuellar notice of EFW's attempt to identify the person who accessed the account in late June 2016. (*Id.* ¶ 53.) However, Cuellar's counsel made no attempt to offer any explanation to EFW for his client's unauthorized access until July 29, 2016. (*Id.* ¶ 54.)

Plaintiff filed the present action on October 21, 2016 (ECF No. 1), alleging: (Count 1) breach of contract; (Count 2) violation of the Computer Fraud and Abuse Act

("CFAA"), 18 U.S.C. § 1030; (Count 3) violation of the Defend Trade Secrets Act of 2016, 18 U.S.C. §1836; (Count 4) unlawful access to stored communications, in violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701; (Count 5) misappropriation of trade secrets pursuant to Va. Code Ann. §§ 59.1-336, *et seq.*; (Count 6) violation of the Virginia Computer Crimes Act, Va. Code Ann. §§ 18.2-152.1, *et seq.*; and (Counts 7 and 8) seeking a preliminary and permanent injunction.

The Court finds that it has subject-matter jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331, 1332, and 1367.

Defendant filed this Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6) (ECF No. 8) on December 29, 2016, specifically challenging the sufficiency of Counts 2 and 4 of the Complaint.

II. LEGAL STANDARD

"A motion to dismiss under Rule 12(b)(6) tests the sufficiency of a complaint; importantly, it does not resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses." *Republican Party of N.C. v. Martin*, 980 F.2d 943, 952 (4th Cir. 1992) (citation omitted). The Federal Rules of Civil Procedure "require[] only 'a short and plain statement of the claim showing that the pleader is entitled to relief,' in order to 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.'" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). A complaint need not assert "detailed factual allegations," but must contain "more than labels and conclusions" or a "formulaic recitation of the elements of a cause of action." *Twombly*, 550 U.S. at 555 (citations

omitted). Thus, the "[f]actual allegations must be enough to raise a right to relief above the speculative level" to one that is "plausible on its face," rather than merely "conceivable." *Id.* at 555, 570.

In considering such a motion, a plaintiff's well-pleaded allegations are taken as true and the complaint is viewed in the light most favorable to the plaintiff. *T.G. Slater*, 385 F.3d at 841 (citation omitted). Legal conclusions enjoy no such deference. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

III. ANALYSIS

Because Cuellar does not appear to challenge Counts 1, 3, 5, 6, 7, or 8, the Court will deny his Motion as to those claims and will limit its analysis only to Counts 2 and 4.

A. Count Two: Violation of the Computer Fraud and Abuse Act

In an effort to deter computer crime, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Pub. L. No. 98-473, 98 Stat. 2190. Two years later, it expanded the Act with a revised version, the CFAA, Pub. L. No. 99-474, 100 Stat. 1213, which remains in effect today. While the CFAA is primarily a criminal statute designed to combat hacking, *see A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009), it grants "[a]ny person who suffers damage or loss by reason of a violation of this section" the ability to bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). "Notably, although proof of at least one of five additional factors is necessary

to maintain a civil action,[2] a violation of any of the statute's provisions exposes the offender to both civil and criminal liability." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012).

Though EFW's Complaint is unclear as to which specific provision of the CFAA it alleges Cuellar violated, it appears to the Court that Plaintiff's claims fall under 18 U.S.C. §§ 1030 (a)(2)(C), 1030 (a)(4), and 1030 (a)(5)(C). (*See* Compl. ¶¶ 63–65.) To successfully state a claim under § 1030(g) based on a violation of § 1030(a)(2)(C), EFW must allege that Cuellar: (1) intentionally (2) accessed a computer (3) without authorization or in such a way that exceeded his authorized access, and (4) obtained information (5) from any "protected computer," (6) resulting in a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

Similarly, to bring an action under § 1030(g) based on a violation of § 1030(a)(4), EFW must plead that Cuellar: (1) knowingly and with the intent to defraud (2) accessed a "protected computer" (3) without authorization or exceeding such authorization that was granted and (4) furthered the intended fraud by obtaining anything of value, (5) causing a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

And finally, to sufficiently state a claim under § 1030(g) based on a violation of §

[2] To bring a civil action, a plaintiff must allege one of the factors set forth in 18 U.S.C. § 1030(c)(4)(A)(i): (I) "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value"; (II) "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals"; (III) "physical injury to any person"; (IV) "a threat to public health or safety"; or (V) "damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security." Here, EFW alleges that its losses exceed $5,000, which is sufficient to satisfy 18 U.S.C. § 1030(c)(4)(A)(i)(I). (*See* Compl. ¶ 64.)

1030(a)(5)(C), EFW must assert that Cuellar: (1) intentionally (2) accessed a "protected computer" (3) without authorization, and, as a result of such conduct, (4) caused damage and loss (5) to one or more persons during any one-year period aggregating at least $5,000 in value.

In his Motion to Dismiss, Cuellar asserts that EFW's claims under the CFAA fail as a matter of law because: (1) he was authorized by Google or, alternatively, EFW to access the account; (2) the account does not qualify as a "protected computer" under the statute; and (3) EFW has not properly alleged "damages" or "losses." (*See generally* Def.'s Mot. to Dismiss 2–10, ECF No. 8.) Because each of these elements is present in 18 U.S.C. §§ 1030 (a)(2)(C), 1030 (a)(4), and 1030 (a)(5)(C), and Cuellar does not appear to challenge any of the other requisite factors in those provisions, the Court will address these three contentions in turn.

i. "Without Authorization" and "Exceeds Authorized Access"

Though Congress did not expressly define the term "without authorization" within the context of the CFAA,[3] it did specify that the phrase "exceeds authorized access" means "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). In determining what limitations to give these two terms, the Fourth Circuit has joined the Ninth Circuit's view that they should be construed narrowly. *See WEC Carolina Energy Sols. LLC*, 687 F.3d at 204 ("Where, as here, our analysis

[3] When construing the term, the Fourth Circuit has cited to the Oxford English Dictionary's definition of "authorization" as "formal warrant, or sanction." *WEC Carolina Energy Sols. LLC*, 687 F.3d at 204 (citing *Oxford English Dictionary* (2d ed. 1989; online version 2012)).

involves a statute whose provisions have both civil and criminal application, our task merits special attention because our interpretation applies uniformly in both contexts. Thus, we follow the canon of strict construction of criminal statutes or rule of lenity. In other words, in the interest of providing fair warning of what the law intends to do if a certain line is passed, we will construe this criminal statute strictly and avoid interpretations not clearly warranted by the text." (internal citations and quotation marks omitted)).

Thus, the Fourth Circuit has held that within the employment context, "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer." *Id.* Therefore, "he accesses a computer 'without authorization' when he gains admission to a computer without approval." *Id.* (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). Similarly, the Fourth Circuit has concluded that "an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." *Id.* (citing *Brekka*, 581 F.3d at 1133). "Notably, neither of these definitions extends to the improper *use* of information validly accessed." *Id.*

Cuellar's principal argument regarding authorization rests on his assertion that "[w]hen a person provides personal information to register an email account with a service provider like Google or Yahoo, and establishes a password, it is the service provider that authorizes that person's access to the account and not the employer." (Mot. to Dismiss 3 (citing *Hoofnagle v. Smyth-Wythe Airport Comm'n*, Case No. 1:15CV8,

2016 WL 3014702 (W.D. Va. May 24, 2016) and *Role Models Am., Inc. v. Jones*, 305 F. Supp. 2d 564 (D. Md. Feb. 25, 2004)).) Cuellar maintains that because he created the account, "[i]t was the authorization of Google, and not EFW, that mattered for purposes of determining [his] access rights under the CFAA." (*Id.*) In other words, Cuellar contends that "[f]or purposes of unauthorized access to the [account] under the CFAA, EFW does not get to create [the] rules [governing authorization]; only the Google Terms of Use can do that." (Reply 2, ECF No. 16.)

Cuellar is certainly correct that EFW has pleaded that he was the one who initially created the account. (*See* Compl. ¶ 22.) However, Cuellar's principal argument conspicuously ignores the fact that he only did so while acting in the course and scope of his employment and for the benefit of EFW, not for personal use. (*Id.* ¶¶ 20–25.) In an effort to overcome this deficiency, Cuellar cites to *Hoofnagle v. Smyth-Wythe Airport*, a decision out of the Western District of Virginia.[4]

In *Hoofnagle*, the Plaintiff created a Yahoo! Mail email account soon after he began working as an Operations Manager at the Mountain Empire Airport. *Hoofnagle*, 2016 WL 3014702, at *1. Throughout his employment, the Airport did not maintain an email address for its employees, and Hoofnagle "understood that when he communicated with the public [using the Yahoo! email address], he was speaking on behalf of the Airport." *Id.* Significantly, the Plaintiff used the email account for both personal and business purposes. *Id.*

[4] Cuellar also cites *Role Models America, Inc. v. Jones*, 305 F. Supp. 2d 564 (D. Md. 2004); however, that case has no bearing on the present issue. Unlike Cuellar, the Defendant in *Role Models America* merely *received* trade secret information from another party and never accessed the information itself. *Id.* at 566.

After sending an inflammatory email to a United States Senator, the Airport fired Hoofnagle. *Id.* at *2. Subsequent to his termination, Hoofnagle's former employer accessed his Yahoo! email account without his permission in order to retrieve business records. *Id.* As a result, Hoofnagle brought suit alleging various claims against his former employer, including one for violating the SCA. *Id.* at *1; *see also Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 636 (E.D. Va. 2009) (employing the same analysis to assess the "without authorization" requirement for both CFAA and SCA claims).

In denying the Defendant's Motion for Summary Judgment, the Court stated "[i]t is true that Hoofnagle created the account, in part, as a means to conduct Airport business, a purpose for which the account was in fact used. However, as the individual who used his personal information to create the account and establish a password, Hoofnagle was clearly the person duly authorized by Yahoo! to use and access the account, not the [Defendant]." *Id.* at *11.

The immediate case is clearly distinguishable from *Hoofnagle* if, for no other reason, than the simple fact that Cuellar did not create the account unilaterally, but rather did so within the scope of his employment for, and at the direction of, EFW. In other words, this was not Cuellar's personal account. The Complaint makes clear that the account belonged to EFW, who then authorized its employees to use it. What is more, at no point in the Complaint does EFW allege that Cuellar—or any other employee, for that matter—utilized the account for personal use like the Plaintiff in *Hoofnagle*.

Upon review, the Court finds that the Ninth Circuit's decision in *LVRC Holdings,*

LLC v. Brekka is persuasive. *Cf. WEC Carolina Energy Sols. LLC*, 687 F.3d at 204 (adopting the Ninth Circuit's narrow reading of "without authorization" and "exceeds authorized access" in the CFAA). In *Brekka*, the Plaintiff, LVRC, maintained an account through a third party—like EFW did through Google in the present case—to provide email, website, and related services as well as to monitor internet traffic to its website and compile statistics about that traffic. 581 F.3d at 1129. The Defendant, Brekka, worked for LVRC and, as part of his duties, obtained an administrative log-in to access the Plaintiff's website and statistics gathered by the third party. *Id.* After negotiations regarding Brekka's attempt to purchase an ownership interest in LVRC dissipated, Brekka left the company. *Id.* at 1130. Nearly one year after Brekka's departure, LVRC noticed that someone had logged in to their website using Brekka's server name and accessed the third-party statistics. *Id.* LVRC subsequently brought an action against Brekka, alleging that he had violated the CFAA. *Id.*

The Ninth Circuit held that "[t]here is no dispute that if Brekka accessed LVRC's information on the [third party] website after he left the company . . ., Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136.[5] Similarly, there is no dispute in the immediate case that when Cuellar accessed the account after he was no longer employed by EFW, he did so without authorization.

Therefore, the Court does not find his primary argument compelling.

As an alternative theory for dismissal, Cuellar asserts that EFW cannot state a

[5] Unlike the present case, LVRC was unable to prove that Brekka accessed the account after he left the company. Here, there is no question in the Complaint, or otherwise, that Cuellar—and not someone else—accessed the account. He has freely admitted it.

claim against him under the CFAA because he "was given access to trade secrets and made use of those trade secrets as part of his work." (Mot. to Dismiss 5.) This argument is equally unavailing for one, obvious reason: Cuellar no longer worked for EFW at the time of his alleged unauthorized access. While the Complaint makes clear that Cuellar was authorized to use the account while he worked for EFW, any authorization undoubtedly was rescinded upon his termination. In fact, Cuellar aknowledged to as much in a Confidentiality Agreement that he signed during the course of his employment. (Compl. Ex. A.) As the Fourth Circuit noted in *United States v. Steele*, a similar case arising under the CFAA, the end of a defendant's employment "logically suggests that the authorization he enjoyed during his employment no longer existed." 595 Fed. App'x 208, 211(4th Cir. 2014) (unpublished opinion); *see also id.* ("Just because [the account holder] neglected to change a password . . . does not mean [it] intended for [a former employee] to have continued access to its information."). This case compels the same conclusion.[6]

Therefore, the Court finds that EFW has pleaded facts sufficient to assert that Cuellar accessed the account without authorization for purposes of the CFAA.

[6] Assuming *arguendo* that EFW had authorized Cuellar to access the account after he was fired, the Court would still find that EFW has sufficiently pleaded that he exceeded such authorization under the CFAA. EFW created the account and allowed its employees to access it for the limited purpose of "record[ing] information such as the shipments being handled, the routing decisions being made, the selection of vendors, and cost information." (Compl. ¶ 24.) At no point, according to the Complaint, were employees authorized to remove the recovery phone number or secondary email address associated with the account, change the password, create an archive of the account's spreadsheets, download those spreadsheets onto another computer, or delete the account. (*Id.* ¶¶ 33–40.) Therefore, even if Cuellar had authorization to access the account, he is alleged to have "use[d] his access to obtain or alter information that falls outside the bounds of his approved access." *WEC Carolina Energy Sols. LLC*, 687 F.3d at 204.

ii. "Protected Computer"

The CFAA defines the term "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). But, the term "does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." *Id.* A computer becomes a "protected computer" when it "is used in or affecting interstate or foreign commerce or communication." *Id.* §1030(e)(2)(B).

Several courts have held that "any computer with Internet access" is a "protected computer" and, thus, is "a subject of the [CFAA's] protection." *Big Rock Sports, LLC v. AcuSport Corp.*, Case No. 4:08-CV-159, 2011 WL 4459189, at *1 (E.D. N.C. Sept. 26, 2011); *see also United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (holding that the accessed computer was "protected" because the defendant "admitted the computers were connected to the Internet"); *Simmonds Equp., LLC v. GGR Int'l, Inc.*, 126 F. Supp. 3d 855, 863 (S.D. Tex. 2015) ("Pleading specific facts that the defendant accessed a computer connected to the internet is sufficient to stablish that the accessed computer was 'protected.'") (quoting *Merritt Hawkins & Assoc. v. Gresham*, 948 F. Supp. 2d 671, 674 (N.D. Tex. 2013)).

Cuellar claims that EFW has failed to plead that he accessed or obtained information from a "protected computer" because "there are no allegations pertaining to internet usage or other forms of interstate commerce." (Mot. to Dismiss 4.) Instead,

Cuellar asserts, EFW's Complaint "alleges numerous times that [he] created the [account] at the direction of EFW for EFW's representatives *on-site* to share information about shipments from the location." (*Id.*)

In his argument, Cuellar appears to have overlooked the fact that the account itself was located exclusively on the Internet, in the cloud. In other words, while EFW's on-site employees were using it primarily as an intra-office database, the entirety of the communications took place on the Internet.

Therefore, since the account was connected to—and entirely contained within—the Internet, the Court finds that EFW has sufficiently pleaded that Cuellar accessed a "protected computer" under the CFAA.

iii. "Damages" or "Losses"

Within the context of the CFAA, Congress defined the term "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The CFAA further defines the term "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11).

Cuellar argues that EFW has suffered no "loss" under the statute because "[t]here is no allegation of a disruption of service in the Complaint." (Mot. to Dismiss 6.) Additionally, he contends that "EFW has not alleged reasonable damages in the form of its legal fees for filing the miscellaneous action against Comcast." (*Id.* at 7.) In support

of this claim, Cuellar avers that

> The Google account created by Cuellar and used during his employment with [EFW] was, as [EFW] notes, password protected. The universe of individuals who had the password to access the account was limited, because the account was to be used by EFW's on-site representatives. EFW alleges that each of these individuals had signed a confidentiality agreement like the one signed by Cuellar, so there can be no doubt that EFW knew who they were. Had defendants wished to know who accessed the account and deleted the information, they could have simply asked Cuellar and the other employees before filing a miscellaneous action. . . . The Complaint alleges that on or about July 29, 2016, Cuellar, through his counsel, offered an explanation. Had EFW [reached out to Cuellar] earlier, the costs of the miscellaneous action would have been avoided.

(*Id.* at 7–8 (internal citations omitted).) Thus, Cuellar concludes, "[o]n the facts of this case, the costs incurred filing and litigating the miscellaneous action to obtain the name of the individual who deleted the account is not a reasonable cost." (*Id.* at 8; *see also id.* at 8–10 (arguing that an alleged loss of trade secrets is insufficient to satisfy the CFAA's requirement and that the legal fees alleged in the Complaint were not reasonable).)

In sum, Cuellar appears to be making a hindsight argument: If EFW, knowing then what it knows now, had merely asked Cuellar outright whether he accessed the account, he would have confessed, saving EFW the time and expense of the Comcast litigation. This contention, however, lacks support in both the facts as alleged in this case and in the legal framework provided by the CFAA and pertinent case law.

When EFW received notice from Google in May 2016 (*see* Compl. ¶ 48), it certainly had reason to believe that whoever accessed the account did so without authorization and with the intent to delete, steal, or alter its trade secrets contained therein. Because Google's notice "only provided EFW with IP addresses for the devices

or networks from which the access came, as well as the approximate location information" (*id.*), EFW had no way of knowing who accessed the account—whether it was an act of corporate espionage, a third-party hacker, or a former employee. Therefore, it is reasonable that they would take some form of action to investigate and respond to the incident.[7]

While Cuellar may contend that filing a lawsuit was neither reasonably foreseeable nor necessary, as this Court has previously noted, "an investigation is often required to determine the cause and scope of a computer intrusion, and the financial impact of even a relatively narrow intrusion can be extensive." *Animators at Law, Inc. v. Capital Legal Solutions, LLC*, 786 F. Supp. 2d 1114, 1121 (E.D. Va. 2011). The Fourth Circuit has similarly stated that the broadly worded provision defining "loss"—which includes "the cost of responding to an offense"—"plainly contemplates consequential damages of the type sought by [EFW]—costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *Vanderhye*, 562 F.3d at 646.

Therefore, the Court finds that EFW's actions were not unreasonable as a matter of law. Consequently, the Court determines that EFW has adequately pleaded "damages" or "losses" pursuant to the CFAA.

---

[7] EFW's need to take drastic action in order to determine who accessed the account without authorization was amplified by Cuellar's own actions. He "did not tell EFW ahead of time that he was going to be accessing the [a]ccount. [He] did not ask permission to access the [a]ccount, nor did he reach out to EFW in any way ahead of time about it." (Compl. ¶ 45.) Further, he did not contact EFW at any time in the month of May after he accessed the account. (*Id.* ¶ 47.) Subsequent to the lawsuit filed in June, Comcast sent notice to Cuellar alerting him of EFW's efforts to identify the person who accessed the account, at which time he still did not contact EFW regarding his access. (*Id.* ¶ 53.) In fact, Cuellar waited nearly one additional month, until July 29, 2016, to contact EFW in order to offer an explanation for his access. (*Id.* ¶ 54.) Therefore, the Court finds that Cuellar's claims that he would have gladly confessed to his actions had EFW merely asked are belied by his conduct during the intervening time between accessing the account and when he contacted EFW.

iv. Conclusion

For the foregoing reasons, the Court will deny Cuellar's Motion to Dismiss as to EFW's CFAA claims alleged in Count 2.

B. Count Four: Violation of the Stored Communications Act

The SCA, 18 U.S.C. §§ 2701–2712, establishes a criminal offense for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility." 18 U.S.C. § 2701(a)(1)–(2). Like the CFAA, the SCA provides a civil cause of action for "any provider of electronic communications service, subscriber, or other person aggrieved" by an intentional violation of the Act. 18 U.S.C. § 2707(a).

Cuellar presents two arguments regarding why he believes EFW's SCA claim should be dismissed. First, he contends that because the Complaint fails to mention "any form of e-mail or other communication" related to the account, the spreadsheets on the shared Google drive do not amount to an electronic communication under the SCA. (*Id.* at 10.)

The Court finds that this assertion misses the mark. Instead of confining the term "electronic communication" to refer solely to emails as Cuellar asserts, Congress broadly defines it as "any transfer of signs, signals . . . data, or intelligence of any nature transmitted in whole or in part by a wire . . . system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). Because EFW alleges that information was transferred from one employee to another via updating the spreadsheet on the shared account—which existed in its entirety on the Internet—the Court is unpersuaded by

Cuellar's first argument.

In Cuellar's second argument, he claims that he qualifies for one of the exceptions from liability under the SCA because he was authorized to access the account. (*See* Mot. to Dismiss 11 (citing 18 U.S.C. § 2701(c)(1) (stating that the SCA "does not apply with respect to conduct authorized by the person or entity providing a wire or electronic communications service").) However, this argument fails for the same reasons stated above in the Court's analysis of Cuellar's similar contention regarding the CFAA. *See supra* Part III.A.i; *see also Global Policy Partners, LLC*, 686 F. Supp. 2d at 636 (employing the same analysis to assess the "without authorization" requirement for both CFAA and SCA claims).

Therefore, the Court will deny Cuellar's Motion to Dismiss Count 4 of EFW's Complaint.

IV. CONCLUSION

For the reasons stated above, the Defendant's Motion to Dismiss will be DENIED. (ECF No. 8.)

An appropriate Order will accompany this Memorandum Opinion.

The Clerk is DIRECTED to send a copy of this Memorandum Opinion to all counsel of record.

/s/
Henry E. Hudson
United States District Judge

Date: March 9, 2017
Richmond, VA