UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

STIRLING INTERNATIONAL REALTY, INC. D/B/A STIRLING SOTHEBY'S INTERNATIONAL REALTY and ROGER SODERSTROM,

Plaintiffs,

v. Case No: 6:14-cv-1109-Orl-40TBS

TANSEY SODERSTROM,

Defendant.

ORDER

This cause comes before the Court on Defendant's First Amended Motion to Dismiss (Doc. 32), filed February 25, 2015. On March 11, 2015, Plaintiffs responded in opposition (Doc. 34). Upon consideration, the Court denies Defendant's motion.

I. BACKGROUND[1]

This dispute arises from the deteriorated marriage and business relationship of Plaintiff, Roger Soderstrom ("Mr. Soderstrom"), and Defendant, Tansey Soderstrom ("Ms. Soderstrom"), the details of which are more fully recounted in the Court's January 28, 2015 Order granting in part and denying in part Ms. Soderstrom's motion to dismiss Plaintiffs' original complaint. (Doc. 28, pp. 1–4). In essence, Mr. Soderstrom and co-

[1] This account of the facts is taken from Plaintiffs' Amended Complaint (Doc. 31), the allegations of which the Court must accept as true in considering Defendant's motion to dismiss. *See Linder v. Portocarrero*, 963 F.2d 332, 334 (11th Cir. 1992); *Quality Foods de Centro Am., S.A. v. Latin Am. Agribusiness Dev. Corp. S.A.*, 711 F.2d 989, 994 (11th Cir. 1983).

Plaintiff, Stirling International Realty, Inc. d/b/a Stirling Sotheby's International Realty ("SSIR"), allege that Ms. Soderstrom accessed Mr. Soderstrom's and SSIR's private email accounts without authorization and forwarded emails to third parties in order to gain a tactical advantage in the Soderstroms' divorce proceedings.

Plaintiffs filed their original complaint on July 10, 2014. (Doc. 1). On January 28, 2015, the Court partially dismissed that complaint with leave for Plaintiffs to amend Counts 1 and 2. (Doc. 28). On February 11, 2015, Plaintiffs timely filed their Amended Complaint. (Doc. 31). Ms. Soderstrom, proceeding *pro se*, now moves to dismiss Plaintiffs' Amended Complaint for failing to state claims upon which relief can be granted. (Doc. 32).

II. STANDARD OF REVIEW

In order to survive a motion to dismiss made pursuant to Rule 12(b)(6), the complaint must "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007). A claim is plausible on its face when the plaintiff alleges facts that "allow[] 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). Mere legal conclusions or recitation of the elements of a claim are not enough. *Twombly*, 550 U.S. at 555. District courts must accept all well-pleaded factual allegations within the complaint as true. *Id.* Courts must also view the complaint in the light most favorable to the plaintiff and must resolve any doubts as to the sufficiency of the complaint in the plaintiff's favor. *Hunnings v. Texaco, Inc.*, 29 F.3d 1480, 1483 (11th Cir. 1994).

III. DISCUSSION

A. Count 1: The Computer Fraud and Abuse Act

Count 1 alleges a private right of action under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(g). Plaintiffs assert that Ms. Soderstrom violated § 1030(a)(2)(C) of the CFAA. In order to state a claim under that provision, Plaintiffs must establish four elements: (1) Ms. Soderstrom intentionally accessed a protected computer, (2) Ms. Soderstrom lacked authorization or exceeded her authorized access to the computer, (3) Ms. Soderstrom obtained information from the computer, and (4) Ms. Soderstrom caused at least $5,000 in loss to Plaintiffs. *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1313 (M.D. Fla. 2010).

Ms. Soderstrom challenges Count 1 on three grounds. First, Ms. Soderstrom contends that Plaintiffs have not alleged at least $5,000 in loss. (Doc. 32, ¶¶ 16–23). Second, Ms. Soderstrom claims that the computer at issue is not a "protected computer" within the meaning of the CFAA. (*Id.* ¶¶ 25–28). Third, Ms. Soderstrom asserts that Plaintiffs have not sufficiently alleged that she intentionally accessed or exceeded her authority to the computer system at issue. (*Id.* ¶¶ 29–34). The Court addresses each argument in turn.

1. $5,000 in Loss

In its Order dismissing Count 1 of Plaintiffs' original complaint, the Court determined that Plaintiffs failed to allege at least $5,000 in loss. (Doc. 28, pp. 5–6). The Court found that Plaintiffs' original complaint lacked sufficient facts through which the Court could reasonably infer at least $5,000 in loss. Additionally, the Court was unwilling to accept that all violations of the CFAA would produce at least $5,000 in loss. Plaintiffs

clarify in their Amended Complaint the amount of loss they have sustained due to Ms. Soderstrom's alleged conduct. Ms. Soderstrom again moves to dismiss Count 1 for failing to allege sufficient loss.

In order for Plaintiffs to establish a prima facie CFAA case, they must show that they have incurred "loss . . . during any 1-year period . . . aggregating at least $5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I). The CFAA defines "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). District courts within Florida's Middle District interpret this definition of "loss" to include two subtypes of loss that may be alleged: (1) costs incurred due to investigating, responding to, and correcting damage caused by a violation, and (2) costs incurred, revenue lost, or other damages resulting from an interruption of service. *E.g.*, *Aquent LLC v. Stapleton*, No. 6:13-cv-1889-Orl-28DAB, 2014 WL 5780293, at *3 & n.6 (M.D. Fla. Nov. 5, 2014); *Klein & Heuchan, Inc. v. Costar Realty Info., Inc.*, No. 8:08-cv-1227-T-30EAJ, 2009 WL 963130, at *3 (M.D. Fla. Apr. 8, 2009). In any case, the total sum of loss alleged must equal or exceed $5,000. *Stapleton*, 2014 WL 5780293, at *3.

Plaintiffs allege that they have incurred losses exceeding $5,000 due to Ms. Soderstrom's alleged unauthorized access to Plaintiffs' email system, including costs associated with responding to Ms. Soderstrom's breach and conducting a forensic computer examination to identify the source and damage caused by the breach. (Doc. 31, ¶¶ 39, 71, 79). In support, Plaintiffs attach to their Amended Complaint an invoice which

shows $5,100 worth of forensic computer services rendered as of May 27, 2014. (Doc. 31-4).

Ms. Soderstrom disputes Plaintiffs' loss allegations on two grounds. First, she contends that losses incurred to one's personal email account are not contemplated by the CFAA. (Doc. 32, ¶ 20). Second, she asserts that incurring loss or damages without an interruption of service is not enough under the CFAA. (*Id.* ¶ 19). Ms. Soderstrom is off-base on both arguments, as it is clear from the Complaint that the email accounts at issue are business accounts and costs incurred from an interruption of service are not the only "loss" or "damages" recognized by the CFAA. *See, e.g.*, *Stapleton*, 2014 WL 5780293, at *3 & n.6; *Klein & Heuchan*, 2009 WL 963130, at *3. Accordingly, the Court finds that Plaintiffs sufficiently allege at least $5,000 in loss.

2. "Protected Computer"

Next, Ms. Soderstrom challenges Count 1 on the grounds that Plaintiffs have failed to allege that the computer in dispute is a "protected computer" under the CFAA. The CFAA defines "protected computer" as any computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. §1030(e)(2)(B). Generally, a computer that is connected to the Internet sufficiently affects interstate commerce and is considered a protected computer under the CFAA. *Cont'l Grp. Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009); *Dedalus Found. v. Banach*, No. 09 Civ. 2842(LAP), 2009 WL 3398595, at *2 (S.D.N.Y. Oct. 16, 2009) ("[C]omputers that access the Internet through programs such as email qualify as protected computers [under the CFAA]."); *cf. United States v. Walters*, 182 F. App'x 944, 945 (11th Cir. 2006) (per curiam) ("[T]he internet is an instrumentality of interstate commerce . . . .").

Although Ms. Soderstrom claims that the Amended Complaint fails to identify the particular program Plaintiffs use to access their email accounts and cloud-based storage system, Plaintiffs more than adequately show that their computers affect interstate commerce by being connected to the Internet. Plaintiffs state that they subscribe to a computer mail and cloud-based storage system that is hosted by Microsoft. (Doc. 31, ¶¶ 15–17, 49, 53). Through this service, Microsoft provides Plaintiffs and SSIR's employees with email accounts and access to the cloud-based storage system through the Internet. (*Id.*). Accordingly, Plaintiffs sufficiently allege that Ms. Soderstrom accessed a protected computer under the CFAA.

3. Unauthorized Access/Exceeded Authority

In order to state a claim for a violation of the CFAA, Plaintiffs must show that Ms. Soderstrom either intentionally accessed a protected computer without authorization or exceeded her authorized access to the protected computer. *Barney*, 698 F. Supp. 2d at 1313. The CFAA therefore contemplates two types of "accessers": those without authorization and those with authorization who exceed that authorization. *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006). An individual acts without authorization where they do not have permission to use the computer system at issue. *See id.* An individual exceeds their authorization to a computer system where he or she has authorization to access the computer, but uses the computer system to "go beyond the permitted access granted to them." *Id.*

Ms. Soderstrom disputes that Plaintiffs are able to identify her as the individual who accessed Mr. Soderstrom's email without authorization or in excess of authorization. (Doc. 32, ¶¶ 30–33). However, Plaintiffs need not conclusively show that it was Ms.

Soderstrom who accessed the email at this stage of the proceedings, only that it is *plausible* that it was her. *Iqbal*, 556 U.S. at 678. Plaintiffs allege sufficient facts to raise such a reasonable inference. Plaintiffs show that the timing of the breach is suspect, as the transition period during which Ms. Soderstrom was required to fully extricate herself from SSIR was to conclude four days later, meaning that Ms. Soderstrom would no longer have access to her SSIR accounts thereafter. (Doc. 31, ¶¶ 24, 57). Next, all of the intercepted emails were forwarded to Ms. Soderstrom's love interest. (Doc. 31, ¶¶ 65–67; Doc. 31-3). Further, thousands of Mr. Soderstrom's emails ended up in the hands of Ms. Soderstrom's attorney and were subsequently used against Mr. Soderstrom in the parties' state court divorce proceedings. (Doc. 31, ¶¶ 31, 69, 70; Doc. 31-1). Finally, the SSIR employee whose computer was used to access Mr. Soderstrom's email account advised Plaintiffs that she had no involvement in the breach and that Ms. Soderstrom had informed her previously that she had found a way to access and read Mr. Soderstrom's emails despite the fact that SSIR's employees are only given access to their own accounts. (Doc. 31, ¶¶ 17, 48, 57–59). These factual allegations are enough to allege that Ms. Soderstrom at least intentionally exceeded her authorization to the SSIR computer system. Accordingly, Ms. Soderstrom's motion to dismiss will be denied as to Count 1.

B. Count 2: The Stored Communications Act

Count 2 alleges a private right of action under the Stored Communications Act ("SCA"), 18 U.S.C. § 2707(a). In order to state a claim under the SCA, a plaintiff must establish two elements: (1) the defendant "intentionally access[ed] without authorization a facility through which an electronic communication service is provided" or "intentionally

exceed[ed] an authorization to access that facility," and (2) the defendant "obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in electronic storage in such system." *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) (quoting 18 U.S.C. § 2701(a)) (internal quotation marks omitted); *Vista Mktg., LLC v. Burkett*, 39 F. Supp. 3d 1367, 1369–70 (M.D. Fla. 2014).

Ms. Soderstrom challenges Count 2 on three grounds. First, Ms. Soderstrom states that Plaintiffs cannot establish liability under the SCA because the material in dispute was readily accessible to the public. (Doc. 32, ¶¶ 37–39). Second, Ms. Soderstrom contends that Plaintiffs have failed to allege a "facility" protected by the SCA. (*Id.* ¶¶ 41–42). Third, Ms. Soderstrom asserts that Plaintiffs have not sufficiently alleged that she intentionally accessed or exceeded her authority to SSIR's computer system. (*Id.* ¶¶ 43–44). The Court addresses each argument in turn.

1. Material Readily Accessible to the Public

It is true that not all unauthorized access to private electronic communications violates the SCA. The Eleventh Circuit addressed the problem in *Snow v. DirecTV, Inc.*:

> Through the World Wide Web, individuals can easily and readily access websites hosted throughout the world. Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible.

Snow, 450 F.3d at 1321. Indeed, if all individuals who accessed an electronic communication without authorization were prosecuted, "the floodgates of litigation would open and the merely curious would be prosecuted." *Id.* Therefore, liability cannot be

imposed under the SCA where the electronic communication at issue was readily accessible to the public. *Id.*

Ms. Soderstrom claims that the emails which Plaintiffs accuse her of accessing were readily accessible to the public because she believes there was a "tunnel" or "vortex" between her computer and Mr. Soderstrom's computer which allowed access from one to the other. (Doc. 32, ¶ 37). Ms. Soderstrom therefore reasons that anyone who had access to the computer at issue would have been able to access Mr. Soderstrom's emails. (*Id.* ¶ 39).

Ms. Soderstrom's version of the facts implicates the merits of the case, which is beyond the scope of the Court's review under Rule 12(b)(6). Accepting Plaintiffs' version of the facts as true, as the Court must, Plaintiffs show that Mr. Soderstrom's email account was not readily accessible to the public. SSIR maintained its computer mail system, email accounts, electronic information, and electronic communications on a facility hosted by Microsoft. (Doc. 31, ¶ 15). SSIR utilized the Microsoft facility with Microsoft's permission and for the purpose of providing email and cloud-based support to SSIR's employees. (*Id.* ¶ 16). At no time did SSIR give access to its email accounts to the general public. (*See id.* ¶ 17). Therefore, the electronic communications in dispute were not readily accessible to the general public.

2. Facilities Protected by the SCA

In its Order dismissing Count 2 of Plaintiffs' original complaint, the Court determined that Plaintiffs failed to sufficiently allege a "facility" within the meaning of the SCA. (Doc. 28, pp. 7–9). The Court noted that the manner in which Plaintiffs had originally pleaded their SCA claim appeared as if Plaintiffs were trying to premise liability

on Ms. Soderstrom's unauthorized access of emails stored on a hard drive or personal computer. Because these types of devices are not facilities under the SCA, the Court dismissed Count 2 without prejudice. Plaintiffs have re-alleged their SCA claim against Ms. Soderstrom and clarify the scope of their allegations. Ms. Soderstrom challenges Count 2 for failing to allege a facility.

The SCA allows "any provider of electronic communication service, subscriber, or other person aggrieved" by a violation of its provisions to institute a civil action. 18 U.S.C. § 2707(a). As stated above, in order to impose liability under the SCA, Plaintiffs must show that Ms. Soderstrom intentionally accessed or exceeded her authorization to access a "facility" through which electronic communication services are provided. However, the SCA does not define "facility" and courts that have considered the matter have reached different conclusions.

As expressed in the Court's January 28, 2015 Order, this Court tends to side with the Fifth Circuit's analysis in *Garcia v. City of Laredo, Texas*, which explained:

> A number of district courts . . . have also concluded that "the relevant 'facilities' that the SCA is designed to protect are not computers that *enable* the use of an electronic communication service, but instead are facilities that are *operated by* electronic communication service providers and used to store and maintain electronic storage."
>
> . . . .
>
> Thus these courts agree that a "home computer of an end user is not protected by the SCA." As explained by Orin Kerr in his widely cited law review article, the words of the statute were carefully chosen: "[T]he statute envisions a *provider* (the ISP or other network service provider) and a *user* (the individual with an account with the provider), with the *user's communications in the possession of the provider*."

> This reading of the statute is consistent with legislative history, as "[Congress'] entire discussion of [the SCA] deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers . . . ."

702 F.3d 788, 792–93 (5th Cir. 2012) (emphasis in original) (citations and footnotes omitted), *cert. denied* 133 S. Ct. 2859 (2013). Therefore, Plaintiffs must show that the facility they allege Ms. Soderstrom breached is one which is operated by an electronic communication service provider, such as a computer mail or storage facility, and not an end user device like a personal computer, laptop, hard drive, or cell phone.

In their Amended Complaint, Plaintiffs illuminate that they subscribe to a computer mail and cloud-based storage system that is hosted by Microsoft. (Doc. 31, ¶¶ 15–17, 49, 53). Through this service, Microsoft provides Plaintiffs and SSIR's employees with email accounts and access to the cloud-based storage system through the Internet. (*Id.*). This is exactly the type of computer mail or storage facility which the SCA contemplates. *See Garcia*, 702 F.3d at 792–93; *Burkett*, 39 F. Supp. 3d at 1370 (holding that a wife accessed a protected facility when she access her husband's work email). Because the emails which Ms. Soderstrom allegedly intercepted were stored on this system, Plaintiffs sufficiently demonstrate that Ms. Soderstrom accessed a facility under the SCA without sufficient authorization.

3. Unauthorized Access/Exceeded Authority

Like the CFAA, the SCA requires Plaintiffs to show that Ms. Soderstrom either intentionally accessed SSIR's computer system without authorization or in excess of authorization. *Snow*, 450 F.3d at 1321. Similar to her arguments under Count 1, Ms.

Soderstrom disputes that Plaintiffs are able to identify her as the one who accessed SSIR's computer system and Mr. Soderstrom's emails. (Doc. 32, ¶ 43). For the same reasons stated by the Court in Section III.A.3, *supra*, Ms. Soderstrom's argument fails. Alternatively, Ms. Soderstrom states that it was SSIR's IT person who accessed Mr. Soderstrom's email account without authorization, not her. (*Id.* ¶ 44). However, determinations of liability are beyond the scope of the Court's review under Rule 12(b)(6).[2] Ms. Soderstrom's motion to dismiss will therefore be denied as to Count 2.

C. Counts 3 and 4

Counts 3 and 4 of Plaintiffs' Amended Complaint state claims for invasion of privacy under Florida common law and for declaratory judgment, respectively.[3] Ms. Soderstrom attacks both claims for various reasons. (Doc. 32, ¶¶ 46–57). However, the Court has already determined that Counts 3 and 4 of the Amended Complaint state claims for relief. (Doc. 28, pp. 10–15). Ms. Soderstrom is therefore foreclosed from attacking those claims under Rule 12(b)(6) a second time.[4] Accordingly, Ms. Soderstrom's motion to dismiss will be denied as to Counts 3 and 4.

---

[2] To the extent Ms. Soderstrom's argument could be construed as a motion to dismiss for failing to join a required party under Rule 12(b)(7), the Court denies her motion. "It has long been the rule that it is not necessary for all joint tortfeasors to be named as defendants in a single lawsuit." *Temple v. Synthes Corp.*, 498 U.S. 5, 7 (1990). A defendant who complains of an absent tortfeasor may seek contribution for their share of liability through impleader. Fed. R. Civ. P. 14(a).

[3] Count 3 is asserted by Mr. Soderstrom only.

[4] To the extent Ms. Soderstrom's challenges to Counts 3 and 4 could be construed as a motion for reconsideration, the Court denies her motion. Ms. Soderstrom makes no showing of new evidence that was previously unknown, an intervening change in controlling law, or that this Court clearly erred in its analysis; rather, Ms. Soderstrom improperly "rehash[es] arguments previously made." *Parker v. Midland Credit Mgmt., Inc.*, 874 F. Supp. 2d 1353, 1359 (M.D. Fla. 2012).

IV. CONCLUSION

For the aforementioned reasons, it is **ORDERED AND ADJUDGED** that Defendant's First Amended Motion to Dismiss (Doc. 32) is **DENIED**. Defendant, Tansey Soderstrom, shall answer Plaintiffs' Amended Complaint (Doc. 31) **within fourteen (14) days** of this Order.

DONE AND ORDERED in Orlando, Florida on May 15, 2015.

PAUL G. BYRON
UNITED STATES DISTRICT JUDGE

Copies furnished to:

Counsel of Record
Unrepresented Parties