UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION
CASE NO.: 6:14-cv-1109-Orl-40TBS

STIRLING INTERNATIONAL REALTY, INC., a Florida corporation d/b/a STIRLING SOTHEBY'S INTERNATIONAL REALTY and ROGER SODERSTROM,

Plaintiffs,

vs.

TANSEY SODERSTROM,

Defendant.
_____/

PLAINTIFFS' RESPONSE, WITH INCORPORATED MEMORANDUM OF LAW, IN OPPOSITION TO PRO SE DEFENDANT'S 'FIRST AMENDED MOTION TO DISMISS'

Plaintiffs, STIRLING INTERNATIONAL REALTY, INC. d/b/a STIRLING SOTHEBY'S INTERNATIONAL REALTY ("SSIR") and ROGER SODERSTROM ("Mr. Soderstrom"), by and through undersigned counsel, hereby respond to *pro se* Defendant's 'First Amended Motion to Dismiss"[1], and state:

[1] Notwithstanding the caption of *pro se* Defendant's instant motion (Doc. 32), Plaintiffs understand the filing to be a motion to dismiss Plaintiffs' Amended Complaint and will refer to the instant motion as such in their Response.

I. PROCEDURAL BACKGROUND[2]

Plaintiffs filed their original Complaint in this action on July 10, 2014 (Doc. 1), alleging therein claims against Defendant for violation of the Computer Fraud and Abuse Act (Count I); violation of the Stored Communications Act (Count II); invasion of privacy (Count III); and seeking declaratory judgment (Count IV). Defendant filed her Motion to Dismiss the Plaintiffs original Complaint (Doc. 9) on September 18, 2014. Plaintiffs filed their Response to Defendant's Motion to Dismiss (Doc. 12) on October 2, 2014.

On January 28, 2015, this Court entered its Order (Doc. 28) granting in part, and denying in part, Defendant's Motion to Dismiss ("the Order"). Specifically, the Court dismissed Counts I and II of the original Complaint without prejudice, with

[2]Plaintiffs note that Defendant's Motion to Dismiss the Amended Complaint includes a 'Statement of Facts' wherein Defendant once again both disputes factual allegations and makes argument. *See, e.g.* Doc. 32 at ¶7 (therein Defendant asserts that the subject computer was "purchased from SSIR's Dr. Phillips' office," citing to Exhibit 1 to the Amended Complaint, which is a letter from Defendant's attorney in the state action. That letter plainly states the computer was purchased **for** the Dr. Phillips office and in no way indicates that the computer was purchased **from** Plaintiff, SSIR. In the same paragraph, Defendant argues that correspondence from Plaintiff Soderstrom's attorney in the state action responsive to Exhibit 1, wherein Plaintiffs sought to ensure the preservation of electronically stored information (*see* **Exhibit 2** to the Amended Complaint), "was clearly overbroad [*sic*], burdensome, and sent for the purpose of harassment."). For purposes of responding to Defendant's Motion to Dismiss the Amended Complaint (Doc. 32), Plaintiffs rely on the factual allegations as stated in their Amended Complaint (Doc. 31). In the interests of efficiency, Plaintiff will refrain from re-alleging a statement of the facts once again in this Response as it trusts that the Court is well acquainted with them at this stage of the proceedings. Plaintiffs reserve the right to respond to Defendant's disputed facts and arguments at such time as those are raised in a proper pleading such as an Answer and Affirmative Defenses.

leave for Plaintiffs to Amend (Doc. 28 at 15). The Court denied the Defendant's Motion to Dismiss as to Counts III and IV of the original Complaint (Doc. 28 at 15).

On February 11, 2015, Plaintiffs filed their Amended Complaint (Doc 31). Plaintiffs' Amended Complaint addresses the pleading deficiencies of the original Complaint that were noted in the Order. As amended, Plaintiffs' Complaint states claims against Defendant for violation of the Computer Fraud and Abuse Act (Count I) and violation of the Stored Communications Act (Count II). Plaintiffs' Amended Complaint reasserts Mr. Soderstrom's claim for invasion of privacy (Counts III) and maintains an action for declaratory judgment (Count IV). On February 25, 2015 Defendant filed her Motion to Dismiss the Amended Complaint (Doc. 32).[3]

II. RESPONSE AND ARGUMENT

a. Plaintiffs have sufficiently alleged a plausible cause of action under the Computer Fraud and Abuse Act ("CFAA").

i. *Plaintiffs' Amended Complaint sufficiently alleges Plaintiffs suffered specified loss exceeding $5,000.00 in a one-year period as a result of investigating and responding to Defendant's conduct in violation of the CFAA.*

Count I of Plaintiffs' Amended Complaint seeks compensatory and other relief pursuant to 18 U.S.C. §1030(g) of the CFAA, which provides in pertinent part:

[3] Plaintiffs note that Defendant's Motion to Dismiss the Amended Complaint refers to allegations made by Plaintiffs in their original Complaint. See, e.g., Doc. 32 at ¶14. To the extent that the instant motion is premised upon any allegations made in the original Complaint, those arguments are improper and should not be considered by the Court in determining the instant motion.

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.

In order to maintain a civil action under the CFAA, Plaintiffs must demonstrate that they suffered damage or loss by reason of a violation that involved 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i) of 18 USC §1030. *See* 18 U.S.C. §1030(g). 'Loss' under the CFAA is defined to include "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" as well as "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." §18 U.S.C. §1030(e)(11).

This Court considered that the only relevant factor of CFAA to determining the motion to dismiss the original Complaint was whether Plaintiffs incurred loss during any 1-year period aggregating at least $5,000 in value (Doc. 28 at p. 5, internal quotation and citation omitted). Plaintiffs alleged in their Original Complaint that they were damaged by Defendant's wrongful conduct resulting in damages that amounted to an aggregated loss of over $5,000 during a one year period. *See, e.g.* Doc. 1,¶ 56. However, the Court found that Plaintiffs failure to specifically allege

whether their loss occurred as a result of investigating, responding to, or correcting damage caused by a violation of the CFAA was fatal to their ability to maintain their claim under the CFAA. *See* Doc. 28 at p. 6.

In explaining the basis for dismissing the Plaintiffs' CFAA claim, the Court stated:

> Based on the lack of factual content in the Complaint suggesting that Plaintiffs investigated, responded to, or corrected damage from Defendant's alleged violation of the CFAA and that these corrective efforts cost Plaintiffs at least $5,000, the Court cannot conclude Plaintiffs have raised their losses above a speculative level.

The Court also stated that it was "unable to accept that every violation of the CFAA results in investigative and corrective costs of $5,000 or more." (Doc. 28 at p. 6).

The Amended Complaint specifically alleges that Plaintiffs have incurred losses in excess of $5,000.00 as a result of responding to the unauthorized access to, and transfer of, information in Roger's SSRI email account. (Doc. 31 at ¶39). The Amended Complaint details Plaintiffs' response to the violations. (Doc. 31 at ¶¶41-45). Plaintiffs engaged legal counsel to respond to the notice received from Defendant's attorney in the state court action concerning her interception of Mr. Soderstrom's email communications. (Doc. 31 at ¶41). Plaintiffs also responded by engaging legal counsel in order to formally respond to the state court proceedings that Defendant initiated upon the information she obtained from her unauthorized access and interception of Mr. Soderstrom's email communications. (Doc. 31 at ¶41).

Additionally, Plaintiffs engaged the services of ESI Consulting, a computer and digital forensic services consulting firm, to investigate how Roger's emails had been "transferred," as described in the letter Plaintiffs received from Defendant's attorney in the state action. (Doc. 31 at ¶43). The Amended Complaint describes their investigation in response to Defendant's conduct in violation of the CFAA, including the forensic examination of computers performed by ESI Consulting. (Doc. 31 at ¶¶ 44-45). Plaintiffs have incurred loss in excess of $5,000.00 in a one-year period due to responding to Tansey's unauthorized access and interception of Roger's email communications, which response caused Plaintiffs to pay attorney's fees and costs, including investigative costs. (Doc. 31 at ¶71; Doc. 31-4).

ii. *Plaintiffs' Amended Complaint sufficiently alleges Defendant unlawfully accessed a protected computer.*

A "protected computer" includes any computer "which is used in or affecting interstate or foreign commerce or communication." *See, e.g. Deman Data Sys. v. Schessel*, Case No. 8:12-cv-2580-T-24 EAJ; 2013 U.S. Dist. LEXIS 81851 (M.D. Fla. 2013) *citing* 18 U.S.C. §1030(e)(2)(B). Computers connected to the internet are "protected computers" within the meaning of 18 U.S.C. §1030(a)(2)(C). *See, e.g. Cont'l Group, Inc. v. Kw Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009)(where evidence showed plaintiff's computer was connected to the internet, the Court found that plaintiff could defeat defendant's motion to dismiss on the "protected

computer" issue because "there is more than enough evidence to raise its claims beyond a speculative level . . . [p]laintiff has shown a substantial likelihood of success that its computers are in fact "protected computers" under the CFAA.").

Here, Plaintiffs have stated a plausible claim that information Defendant unlawfully accessed and/or obtained by Defendant was accessed on and/or obtained from a protected computer. Although Defendant argues that the facts stated by Plaintiff's do not support the definition of "protected computer" (Doc. 32 at ¶25)[4], the Amended Complaint specifically alleges that the information contained in SSIR's employee emails, including the information in Mr. Soderstrom's email account, is maintained on a computer that is used in and/or affects interstate and foreign commerce or communication. (Doc. 31 at ¶73-74). The Amended Complaint also alleges that the Microsoft facility that hosts SSIR's computer mail system, email accounts, electronic information and communications is accessed by SSIR and its employees on-line *via* an internet connection. (Doc. 31 at ¶¶ 15-16). Moreover, this Court may reasonably infer from Plaintiffs' allegations concerning Defendant accessing Mr. Soderstrom's email, *via* SSIR's computer mail facility, from the Dr.

[4] Defendant also argues "there is nothing in the CFAA that considers 'cloud-based storage' to be a 'protected computer' as defined by the CFAA." (Doc. 32 at ¶26). Defendant cites a proposed legislation of the 112th Congress that died in committee as support for her argument that Congress has "rejected" efforts to include cloud-based computing facilities within the protection of the CFAA. (Doc. 32 at ¶27). As this Court is well aware, the fact that proposed legislation is not ultimately ratified by the Congress is far from a rejection by Congress of that proposal. The Defendant's argument is a red herring and the Court should not find it persuasive.

Phillips office and then forwarding Mr. Soderstrom's email to Dr. Jacobo at the 'jakeddoc@mac.com' email address that all of the computers involved in the exchange of information obtained from Mr. Soderstrom's email account were connected to the internet.

iii. *Plaintiffs' Amended Complaint sufficiently alleges Plaintiffs suffered damage as a result of Defendant's conduct in violation of the CFAA.*

18 U.S.C. §1030 (e)(8) defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." Plaintiffs' Amended Complaint sufficiently alleges Plaintiffs suffered damage when Defendant intentionally accessed, without authorization and/or exceeded her authorized access, SSIR's protected cloud-based computer mail facility and, as a result, obtained information contained in Roger's SSIR email account. (Doc. 31 at ¶¶72-80). The Amended Complaint clarifies that SSIR's employee emails, including Mr. Soderstrom's emails belong to SSIR although they are hosted and maintained on a Microsoft facility. (Doc. 32 at ¶¶15-17). SSIR and its employees access the facility through an internet connection. (Doc. 32 at ¶16).

From Plaintiffs' specific allegations, this Court may reasonably infer that Defendant's unauthorized access damaged the integrity of SSIR's, information and data, as well as its electronic communication system and the protected cloud-based computer mail facility that hosts SSIR employee email accounts. Likewise, the Court

may infer that the integrity of the information in Mr. Soderstrom's emails was impaired by Defendant's misconduct.[5] *See, e.g., Trademotion, LLC v. Marketcliq, Inc*., 857 F. Supp. 2d 1285, 1289 (M.D. Fla. 2012) *quoting Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 1949, 173 L. Ed. 2d 868 (2009) and *citing Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 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."). Plaintiffs have alleged a plausible claim for their damages incurred as a result of Defendant's wrongful conduct to the extent that Defendant's conduct impaired the integrity of SSIR's electronic communication system, information and data, as well as the integrity of the protected cloud-based computer mail facility that hosts SSIR employee email accounts – including the information in Mr. Soderstrom's emails.

[5] Additionally, Plaintiffs' Complaint alleges that one or more persons who was the subject of Plaintiffs' request to safeguard certain information that was unlawfully obtained by Defendant (as detailed in Exhibit 2 to Plaintiffs' Complaint) destroyed or secreted information that was the subject of that Complaint. (Doc. 31 at ¶45). Thus, this Court may reasonably infer that Defendant is liable to Plaintiffs for damages due to Defendant's unauthorized access of a protected computer and her unlawful obtaining of information from the protected computer that hosts SSIR employee email accounts to the extent that her doing so ultimately resulted in the impairment of the availability of data and information that was wrongfully accessed and/or obtained by Defendant.

iv. *Plaintiffs have alleged a plausible claim under 18 U.S.C. §1030(a)(2)(C).*

Pursuant to 18 U.S.C. §1030(a)(2)(C), whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer is a violator of the CFAA. *See, e.g. Deman Data Sys. v. Schessel*, Case No. 8:12-cv-2580-T-24 EAJ; 2013 U.S. Dist. LEXIS 81851 (M.D. Fla. 2013). The plausibility of Defendant's identity as the person who, on December 27, 2013, exceeded her authorized access by intentionally accessing and obtaining information contained in Mr. Soderstrom's email account that was maintained on an SSIR protected computer that hosted employee email accounts can be inferred from facts and circumstances surrounding the access:

a. The "transition period" under the dissolution Settlement Agreement was just four days from the specified December 31, 2013 conclusion at the time the access occurred. (Doc. 31 at ¶¶24, 57).

b. All of the forwarded emails were directed to Dr. Jacobo, with whom the Defendant was then involved in an intimate personal relationship. (Doc. 31-3).

c. Although the information was accessed and obtained through Ms. Dusing's email account, Ms. Dusing stated she had no involvement in accessing or forwarding Mr. Soderstrom's emails. (Doc. 31 at ¶¶57-59).

d. "Literally thousands" of Mr. Soderstrom's emails ultimately ended up in the possession of the Defendant's divorce attorney. (Doc. 31-1).

e. Information obtained from the accessed emails was used, or an attempt was made to use such information, to the advantage of Defendant in the divorce action.

As detailed above, the facts and circumstances under which the SSIR computer and the employee email accounts hosted on that computer were accessed and information in the email account of Mr. Soderstrom was obtained on December 27, 2013 are such as to make plausible Plaintiffs' allegation that Defendant was responsible for accessing the computer, accessing the email accounts, and obtaining the information.

The aforementioned facts and circumstances also make plausible Plaintiffs' allegations that Defendant's actions in doing so were intentional. Indeed, it is highly implausible that the December 27, 2013 access of Ms. Dusing's email account that was hosted on an SSIR computer, through which access was then made of Mr. Soderstrom's email account that is hosted on an SSIR computer, was the result of an unintentional act – particularly in light of the fact that information that was obtained by that access was ultimately provided to third parties who had relationships with Defendant. Further, that same unlawfully obtained information was used by Defendant in pleadings filed by her in the ongoing state court dispute with Mr. Soderstrom.

Plaintiffs' Amended Complaint sufficiently alleges that neither Defendant nor Ms. Dusing had authorization to access Mr. Soderstrom's email account. (Doc. 31 at

¶¶ 34-35, 50-51, 54, 56). Ms. Dusing was not authorized to access any SSIR email account other than the one assigned to her. (Doc. 31 at ¶¶47-49) Defendant was not authorized to access any SSIR email account other than the one assigned to her. (Doc. 31 at ¶¶52-56). Plaintiffs' Amended Complaint sufficiently alleges that Defendant's access to Plaintiffs' computer mail facility, by means of which she obtained the information from Mr. Soderstrom's email account, was either without authorization or exceeded her authorization.[6]

From the circumstances surrounding the aforementioned access, as alleged in the Amended Complaint, to-wit: that Mr. Soderstrom's email was accessed on December 27, 2013 by the Defendant from the Dr. Phillips office operated by Defendant and forwarded or otherwise provided to third persons with whom the Defendant had personal and/or professional relationships, this Court may reasonably infer that Defendant intentionally accessed SSIR's computer mail facility and employee email accounts other than her own that SSIR maintained on a protected computer. The Court may also reasonably infer that Defendant did so without authorization or in a manner that exceeded her authorized access, and thereby obtained information from any protected computer in violation of the CFAA. Thus, Plaintiffs' have sufficiently alleged that Defendant violated the CFAA by accessing – either without authorization or under circumstances that exceed her authorization –

[6] Pursuant to 18 U.S.C. §1030(e)(6), the term "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."

the SSIR computer mail facility and, in turn, accessing of the employee email accounts of Ms. Dusing and Mr. Soderstrom that were hosted on a protected computer.

b. Plaintiffs have sufficiently alleged a plausible cause of action under the Stored Communications Act ("SCA").

Count II of Plaintiffs' Amended Complaint seeks compensatory and other relief pursuant to the Stored Communications Act 18 U.S.C. §§ 2701, et seq., ("SCA"). As explained by this Court in the Order:

> In order to state a claim under the SCA, a plaintiff must demonstrate two elements: (1) the defendant intentionally accessed without authorization a facility through which an electronic communication service is provided or intentionally exceeded an authorization to access that facility, and (2) the defendant obtained, altered, or prevented authorized access to a wire or electronic communication while it is in electronic storage in such system.

(Doc. 28 at p. 7, internal quotation and citations omitted). The SCA incorporates the definitions set forth in the Wire and Electronic Communications Interception and Interception of Oral Communications Act (18 U.S.C. §§ 2510-2522)(the "Wiretap Act") found at 18 U.S.C. §2510. *See* 18 U.S.C. § 2711(1). The SCA and the Wiretap Act are two chapters within the Electronic Communications Privacy Act of 1986 (ECPA). 18 U.S. C. §2510(15) defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." An email communication is clearly encompassed within the definition of "electronic communication." *See, e.g.,*

Graf v. Zynga Game Network, Inc. (In re Zynga Privacy Litig.), 750 F.3d 1098, 1103 (9th Cir. 2014)("ECPA focused on two types of computer services that were prominent in the late 1980s: electronic communications services (e.g., the transfer of electronic messages, such as email, between computer users) and remote computing services (e.g., the provision of offsite computer storage or processing of data and files)") *citing generally Quon v. Arch Wireless Operating Co.*, 529 F. 3d 892, 895, 900-902 (9th Cir. 2008), *rev'd in nonrelevant part sub nom. City of Ontario v. Quon*, 560 U.S. 746, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010); Office of Tech. Assessment, U.S. Cong., Federal Government Information Technology: Electronic Surveillance and Civil Liberties 45-48 (1985).

This Court noted in the Order that the term "facility is not defined in the SCA and that there is disagreement among the district courts that have been asked to make a determination as to the meaning of the term. (Doc. 28 at p. 7). The Court cited decision of other district courts and the Eleventh Circuit Court tending to support a definition of the term "facility" as meaning some other than personal computers, laptops, and cellular phones. (Doc. 28. At pp. 7-8). The Order noted that Plaintiffs' original Complaint did not allege sufficient facts to demonstrate they are electronic communication service providers who operate a facility such as an electronic bulletin board or mail facility. (Doc. 28 at p. 9).

The Court's analysis relied, in part, on *Garcia v. City of Laredo, Tx*., 702 F. 3d 788 (5th Cir. 2012). Many other Courts have relied upon the *Garcia* rationale in determining that a "facility as defined by consistent case law, does not include computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers." *Shefts v. Petrakis*, No. 10 CV 1104, 2013 U.S. Dist. LEXIS 17213, 2013 WL 489610 at *4 (C.D. Ill. Feb. 8, 2013) (*citing Garcia*, 702 F. 3d 788, 792 (5th Cir. 2012)) (internal quotations and citations omitted); *see also Pascal Pour Elle, Ltd. v. Jin*, 2014 U.S. Dist. LEXIS 170486, 10-11 (N.D. Ill. 2014)(noting that the *Shefts* Court ultimately concluded that because the plaintiff's company provided him, along with the company's other employees, with an email service, it was a provider of an electronic communication service). Other courts have reached the same conclusion. *See, e.g. Expert Janitorial, LLC v. Williams*, 2010 U.S. Dist. LEXIS 23080 (E.D. Tenn. Mar. 12, 2010)(18 U.S.C §2701 does not require that a plaintiff's computers be electronic services providers but only that plaintiff's computers or workplace be a facility through which an electronic communication is provided); *IBEW, Local 134 v. Cunningham*, 2013 U.S. Dist. LEXIS 61083, 11-12 (N.D. Ill. Apr. 29, 2013)(agreeing with the reasoning of the Eleventh Circuit and the districts that have followed in concluding that simply accessing a personal computer to obtain stored data would not run afoul of 18 U.S.C. §2701 while noting that plaintiff's allegations that defendant

accessed a database stored on plaintiff's computer network and servers was sufficient to withstand a motion to dismiss its SCA claim because "[u]nlike a simple hard drive, networks and servers can provide an electronic communication service. For example, the server could run an e-mail client."); *see also Becker v. Toca*, No. 07 C 7202, 2008 U.S. Dist. LEXIS 89123, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008) (denying motion to dismiss as premature as law firm's computer network could potentially constitute a facility through which an electronic communication service is provided).

As alleged in Plaintiffs' Amended Complaint, Defendant knowingly and intentionally accessed SSIR's computer mail facility without authorization and/or under circumstances exceeding her authorization. (Doc. 31 at ¶¶85-86). In the course of doing so, Defendant willfully and intentionally obtained access to wire or electronic communications belonging to SSIR and Mr. Soderstrom while those communications were in electronic storage. (Doc. 31 at ¶¶86 – 87).

The Amended Complaint clarifies that the facility accessed by Defendant was not a personal computer or device belonging to Mr. Soderstrom or SSIR. Instead, SSIR's computer mail system, email accounts, electronic information and communications were, at all times material, stored and maintained on a facility hosted by Microsoft. (Doc. 31 at ¶15). Through an arrangement with Microsoft, SSIR maintains a computer mail system that is utilized for all of SSIR's e-mail accounts.

(Doc. 31 at ¶16). SSIR and its employees accessed the facility on-line via an internet connection. (Doc. 31 at ¶16). SSIR's remote computing services are precisely the type of electronic communication services that the ECPA was intended to protect. *See In re Zynga Privacy Litig*.), 750 F. 3d at 1103.

As alleged in the Amended complaint, Defendant unlawfully accessed, or exceeded her authorization to access, SSIR's cloud-based computer mail facility, through which SSIR provided an electronic communication service. (Doc. 31. ¶¶47-64). The Amended Complaint alleges that Defendant acted without authorization in using Ms. Dusing's SSIR credentials to log in to Ms. Dusing's SSIR email account in order to access SSIR's computer mail facility and thereby access Mr. Soderstrom's SSIR email account and information in Mr. Soderstrom's email account. (Doc. 31. ¶¶61-62). In the course of the foregoing unlawful conduct access, Defendant obtained access to electronic communications while they were in electronic storage in SSIR's computer mail facility. (Doc. 31. ¶¶86-87).

Additionally, this Court can reasonably infer from the factual allegations in Plaintiff's Amended Complaint pertaining to the SSIR arrangement with the Microsoft facility that all information maintained and/or hosted on the SSIR computer mail facility is maintained on a protected computer through which an electronic communication service is provided. This Court may also infer, from the same facts and circumstances detailed in connection with Plaintiffs' allegations concerning

Defendant's intentional and unauthorized access in violation of the CFAA, that Defendant took certain intentional actions, through Ms. Dusing's email account, that resulted her intentional and unlawful access of SSIR's computer mail facility – either without authorization or under circumstances in which she clearly exceeded any authority she may have had to make such access and, as a result of doing so, Defendant obtained Mr. Soderstrom's electronic communications while they were in electronic storage in a system that provided an electronic communications service. *See, e.g.*, Doc. 31 at ¶¶61-66 and ¶¶83-87).

IV. CONCLUSION

Plaintiffs' pleadings are sufficient to put Defendant on notice of their claims and have sufficient factual content to survive the motion to dismiss.[7] For the reasons stated herein, *pro se* Defendant's Motion to Dismiss should be denied.

[7] Plaintiffs note *pro se* Defendant's arguments for dismissal of Count III (invasion of privacy) (Doc. 32 at ¶¶ 46-56) and Count IV (seeking declaratory relief) (Doc. 32 at ¶57). Plaintiffs have not responded to those arguments due to the fact that the Court has already denied Defendant's Motion to Dismiss these Counts. (Doc. 28 at p. 15).

DATED this 11th day of March, 2015.

Respectfully submitted,

s/ Victor L. Chapman
Victor L. Chapman
Florida Bar No.: 0407429
Attorneys for Plaintiffs
Barrett, Chapman & Ruta, P.A
18 Wall Street
Orlando, FL 32801
Telephone: 407/839-6227
Fax: 407/648-1190
victor@bcrlaw.net

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on March 11, 2015, I **electronically** filed the foregoing with the Clerk of the Court by using the CM/ECF system and served same *via* email delivery to TANSEY SODERSTROM (tsoderstrom@reforlando.com).

s/ Victor L. Chapman
Victor L. Chapman