IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

SUNIL GUPTA, M.D., LLC,	**)**	
(d/b/a RETINA SPECIALITY	**)**	
INSTITUTE)	**)**	
Plaintiff,	**)**	
	)	
v.	**)**	**CIVIL ACTION NO. 17-00335-N**
	)	
ALAN FRANKLIN,	**)**	
TRACY WILSON, and	**)**	
MONICA PAYTON	**)**	
Defendants.	**)**	

MEMORANDUM OPINION AND ORDER

On July 21, 2017, Plaintiff Sunil Gupta, M.D. LLC d/b/a Retina Specialty Institute (herein after "Plaintiff" or "RSI") filed a two count complaint against Defendants Dr. Alan Franklin, Tracy Wilson, and Monica Payton (herein after referred to by their last names or as "Defendants"). (Doc. 1). According to the Complaint, this Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1331, as Count One asserts a claim arising under the laws of the United States. The Court has supplemental jurisdiction over Count Two, a state law claim, pursuant to 28 U.S.C. §1367(a). The Complaint also states that this Court has diversity jurisdiction pursuant to 28 U.S.C. § 1332 as the amount in controversy exceeds $75,000 and the parties are citizens of different states.

With the consent of the parties, the Court has designated the undersigned Magistrate Judge to conduct all proceedings and order the entry of judgment in this civil action, in accordance with 28 U.S.C. § 636(c), Federal Rule of Civil Procedure 73, and S.D. Ala. GenLR 73. (See Docs. 27-28).

Pursuant to Federal Rule of Civil Procedure 12(b)(6), Franklin filed a motion to dismiss both counts. (Doc. 12). *Pro se* Defendants Wilson and Payton have adopted Defendant Franklin's motion. (Docs. 13-14). Plaintiff and Defendants filed a timely response and reply. (Doc. 18-19). Upon consideration, and for the reasons discussed herein, the motions to dismiss (Docs. 12, 13, and 14) are **DENIED**.

BACKGROUND

RSI is a Delaware limited liability corporation, formed by Sunil Gupta, M.D. Its principal place of business is in Escambia County, Florida. (Doc. 1 at 2). The membership of RSI is comprised of three physicians who are Florida citizens. (Doc. 1 at 2-3). RSI also employs a number of other physicians (ophthalmologists) specializing in the treatment of retina disease and injury. (*Id.*).

Defendant Franklin, is a physician, former employee, former member, former and manager of RSI. (Doc. 1 at 3, ¶ 12). Defendants Wilson and Payton, both ophthalmic technicians, were formerly employed by RSI. (*Id.* at ¶¶ 13-14). All Defendants were employed at RSI's Mobile, Alabama location. (Doc. 1 at 3).

In February 2017, following an interview process and other preparations, Franklin accepted employment with Mobile Infirmary Medical Center, Diagnostic and Medical Clinic ("DMC"). In early March 2017, Wilson and Payton applied for employment with DMC. According to the Complaint, before resigning from employment with RSI, "…Franklin instructed Wilson and Payton to download confidential RSI patient data from RSI's practice management system on a portable hard drive provided by Franklin." (Doc. 1 at 4, ¶19). Per the Complaint:

> Wilson and Payton used an RSI computer to log into RSI's practice management system, which required a password and/or login credentials, and download confidential RSI patient data and other confidential RSI data. The confidential RSI patient information included patient names, addresses, phone numbers, medical notes, insurance information, and appointment schedules for tens of thousands of RSI patients....Franklin also downloaded, with the assistance of Payton and Wilson, retinal scans of a number of RSI patients from RSI's network onto a portable hard drive supplied by Franklin....On the same day that Franklin, Wilson, and Payton downloaded the confidential RSI patient data from RSI's practice management system, they provided the information to DMC so DMC would have contact information to use in communicating with patients after Dr. Franklin moved to DMC.

(Doc. 1 at 4-5, ¶¶ 20-21). The Complaint alleges that there were RSI policies prohibiting such access and use, and that the Defendants knew about these policies. (Doc. 1 at 5, ¶¶ 22-23).

Plaintiff alleges that Defendants' conduct amounts to violations of the Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030 (Count One) and the Alabama Digital Crime Act, codified at Ala. Code §13A-8-112 (Count Two).

STANDARD OF REVIEW

When considering a Rule 12(b)(6) motion to dismiss, the Court must accept as true the allegations set forth in the complaint drawing all reasonable inferences in the light most favorable to the plaintiff. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007). Even so, a complaint offering mere "labels and conclusions" or "a formulaic recitation of the elements of a cause of action" is insufficient. *Ashcroft v. Iqbal*, 556 U.S 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 555); *accord Fin. Sec.*

Assurance. Inc. v. Stephens, Inc., 500 F.3d 1276, 1282–83 (11th Cir. 2007). Further, the complaint must "contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face." ' *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 570). Put another way, a plaintiff must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* This so-called "plausibility standard" is not akin to a probability requirement; rather, the plaintiff must allege sufficient facts such that it is reasonable to expect that discovery will lead to evidence supporting the claim. *Id.*

ANALYSIS

I. Computer Fraud and Abuse Act (Count One)

Count One alleges that all Defendants have violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030 *et seq.,* as follows:

> 28. Defendants intentionally accessed and downloaded confidential RSI patient information from RSI's practice management system using RSI computers without authorization.
>
> 29. Defendants acted in concert with DMC to use the information for an improper purpose and in violation of RSI policies and procedures and applicable state and federal laws, including HIPAA
>
> 30. RSI's computer network and practice management system that were wrongfully accessed by Defendants are used in interstate commerce.
>
> 31. Defendants' unlawful actions have caused RSI to suffer loss and damages, including without limitation costs of responding to Defendants' conduct, conducting a damage assessment, and other costs. RSI's losses resulting from Defendants' conduct exceed $5,000.00.

(Doc. 1, Complaint at 6). The Complaint also contains allegations that the Defendants were aware of RSI's policies prohibiting RSI employees from downloading patient information for personal use or for use by anyone other than a RSI employee. (Doc. 1 at 5, ¶22-23). The policy prohibited RSI employees from downloading patient information without express approval from practice management. (*Id.*).

The CFAA defines seven categories of conduct that can give rise to civil or criminal liability. Those seven categories of conduct are contained within § 1030(a)(1)-(7). Construing the allegations liberally, as detailed in its Complaint and response brief it appears Plaintiff is asserting that Defendants accessed a protected computer in excess of their authority to do so, with resulting damage and/or loss. (Docs. 1 and 18 at 4-5). Thus, the Court assumes Plaintiff is alleging that Defendants violated subsections (a)(2)(C), (a)(4), (a)(5) and/or (a)(6) of 18 U.S.C. § 1030, which provide in relevant part that civil liability may be imposed upon whoever:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> …
>
> (C) information from any protected computer
>
> -or-
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

-or-

(5)

> **(A)** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> **(B)** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> **(C)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

> (A) such trafficking affects interstate or foreign commerce….

18 U.S.C. § 1030(a)(2)(C), (a)(4), (a)(5) and (a)(6).

Though the CFAA is primarily a criminal statute, a civil cause of action may be brought under the CFAA pursuant to § 1030(g), which states:

> 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 subclause[] (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. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g). Plaintiff's complaint appears to rely upon subclause (I), which permits an action only if the plaintiff incurs a minimum "loss to 1 or more persons during any 1-year period…aggregating at least $5,000 in value[]" as a result of the defendant's violation of the CFAA. 18 U.S.C. § 1030(c)(4)(A)(i)(I). (*See* Doc. 1, Complaint at ¶ 31).

The CFAA provides that:

> the term "loss" means 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 offenses, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). With regard to "loss," The Court of Appeals for the Eleventh Circuit has held that

> The plain language of the statutory definition includes two separate types of loss: (1) reasonable costs incurred in connection with such activities as responding to a violation, assessing the damage done, and restoring the affected data, program system, or information to its condition prior to the violation; and (2) any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. *See* 18 U.S.C. § 1030(e)(11). The statute is written in the disjunctive, making the first type of loss independent of an interruption of service. *Yoder*, 774 F.3d at 1073. Contrary to the assertion of the court in *Continental Group*, this interpretation does not reduce "interruption of service" to surplusage. *See Cont'l Grp.*, 622 F.Supp.2d at 1371. "Loss" includes the direct costs of responding to the violation in the first portion of the definition, and consequential damages resulting from interruption of service in the second. Thus, under a plain reading of the statute, [Plaintiff's] loss from [Defendant's] violation of the CFAA does not need to be related to an interruption of service in order to be compensable.

Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167, 1174 (11th Cir. 2017). The Complaint alleges costs in excess of $5,000 associated with responding to Defendants' conduct. (Doc. 1 at 6).

1. The meaning of "exceeds authorized access"

Each of the CFAA provisions upon which it appears Plaintiff is relying, *i.e.* (a)(2)(C), (a)(4), (a)(5) and/or (a)(6), (save for § 1030(a)(5)(A)) require that access to the protected computer be obtained without authorization or in excess of authorization. *See* 18 U.S.C. § 1030(e)(6). Defendants' grounds for their motions to dismiss Count One are summarized as follows:

> RSI' s Count I alleges that Dr. Franklin, and defendants Wilson and Payton (collectively "Defendants"), violated the CFAA by accessing RSI's practice management system "without authorization". See RSI Complaint, ¶ 28. RSI alleges that Defendants "used an RSI computer to log into RSI's practice management system, which required a password and/or login credentials, and download[ed] confidential RSI patient data and other confidential RSI data" along with "retinal scans of a number of RSI patients". See RSI Complaint, ¶ 19-20. RSI alleges that Defendants "were not authorized to download the confidential RSI patient information." See RSI Complaint, ¶ 22 (Emphasis added). RSI's claims are due to be dismissed because the alleged conduct does not violate CFAA.... RSI has not alleged that Defendants acted either "without authorization" or in excess of their "authorized access".

(Doc. 12 at 2-3)(emphasis in original).

The parties seem to agree that the Defendants were authorized to access the protected computers[1], as well as the medical records contained therein. However,

[1] Pursuant to § 1030(e)(2) the term "protected computer" means a computer—

> **(A)** exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> **(B)** which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

Plaintiff argues that accessing these records, in violation of company policies, and for an unauthorized purpose amounts to access in excess of Defendants' authorization under the CFAA.

The CFAA does not define the phrase "without authorization," but it defines "exceeds authorized access." "[T]he 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. 18 U.S.C. § 1030(e)(6). As the Middle District of Florida observed in *Enhanced Recovery, LLC v. Frady*:

> …[T]he application of this term and its definition have bedeviled the courts. Some have interpreted the definition broadly, reading into it a theory of agency, such that an employee's authorization is revoked, and thus she "exceeds authorized access," whenever she obtains information with a subjective intent that is unlawful or contrary to her employer's interests, even though the employee actually had authorization to access the information. *See, e.g., United States v. John,* 597 F.3d 263, 271–72 (5th Cir.2010) ("authorization" as used in the CFAA "may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system" if the use is in furtherance of a crime); *Int'l Airport Centers, LLC v. Citrin,* 440 F.3d 418, 420–21 (7th Cir.2006) (employee's authorization to access a computer ended, for purposes of 18 U.S.C. § 1030(a)(5), once the employee breached his duty of loyalty to the employer); *Aquent LLC,* 2014 WL 5780293, at *4–5 (employee exceeded authorized access by abusing access to confidential information to share it with a competitor). Under this theory, where an employee accesses confidential information for personal purposes inconsistent with the employer's interests, that employee has exceeded her authorized access to the information.…Other courts, including the majority of district courts in this Circuit that have considered the question, have adopted a narrower definition of "exceeds authorized access." As one put it, "[q]uite simply, without authorization means exactly that: the employee was not granted access by his employer.

18 U.S.C. § 1030.

> Similarly, exceeds authorized access simply means that, while an employee's initial access was permitted, the employee accessed information for which the employer had not provided permission." *AIRCO,* 953 F.Supp.2d at 1296; *see also, e.g., Clarity Services, Inc.,* 698 F.Supp.2d at 1315; *Trademotion,* 857 F.Supp.2d at 1289–91; *Diamond Power Int'l, Inc. v. Davidson,* 540 F.Supp.2d 1322, 1343 (N.D.Ga.2007). Many courts outside of the Eleventh Circuit have also adopted this narrower interpretation. *E.g., WEC Carolina Energy Solutions LLC v. Miller,* 687 F.3d 199, 203–07 (4th Cir.2012); *United States v. Nosal,* 676 F.3d 854, 858 (9th Cir.2012); *Shamrock Foods Co. v. Gast,* 535 F.Supp.2d 962, 968 (D.Ariz.2008). Under the narrow interpretation, an employee who has actually been granted access to information does not "exceed authorized access" by virtue of the employee's subjective intent or by subsequently violating company policies on the use of the information. *AIRCO,* 953 F.Supp.2d at 1296; *WEC Carolina,* 687 F.3d at 206–07; *Bell Aerospace Services, Inc. v. U.S. Aero Services, Inc.,* 690 F.Supp.2d 1267, 1272 (M.D.Ala.2010) (" 'Exceeds authorized access' should not be confused with exceeds authorized use.") (citing *Diamond Power Int'l,* 540 F.Supp.2d at 1343). Nor does an employee "exceed authorized access" by obtaining information that she is permitted to access, but "in a manner" that is not authorized. *WEC Carolina,* 687 F.3d at 205–07; *Nosal,* 676 F.3d at 856–63. Rather, an individual "exceeds authorized access" by gaining access to specific information that her employer simply did not give her permission to access. *Diamond Power Int'l,* 540 F.Supp.2d at 1343….

2015 WL 1470852, at *6 (M.D. Fla. Mar. 31, 2015). Not surprisingly, Plaintiff urges the Court to adopt the broad interpretation and Defendants urge the Court to adopt the narrow interpretation In *Enhanced Recovery*, the Court granted a motion to dismiss a CFAA claim holding,

> …[T]he Court concludes that "[u]nder the more reasoned view, a violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." *Diamond Power Int'l,* 540 F.Supp.2d at 1343. "The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation." *Id.* In this regard, the narrower interpretation is a "sensible reading of the text and legislative history of a statute whose general purpose is to punish

> hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere." *Nosal,* 676 F.3d at 863. As such, in this Court's view, the CFAA's definition of "exceeds authorized access" does not reach an employee who has actually been granted access to confidential information, but who accesses that information for the improper purpose of removing or disclosing the employer's information.

2015 WL 1470852, at *9 (M.D. Fla. Mar. 31, 2015).

The Court has reviewed the cases submitted by both parties, and Defendants are correct that several district courts within this circuit have held that conduct similar to that alleged here does not meet the definition of "exceeds authorized access" under the CFAA. *See e.g. Bell Aerospace Services, Inc. v. U.S. Aero Services, Inc.,* 690 F.Supp.2d 1267 (M.D.Ala.2010); *Lockheed Martin Corp. v. Speed*, 2006 WL 2683050 (M.D. Fla. Aug 1., 2006); *Diamond Power Intern. Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); *Enhanced Recovery Co., LLC v. Frady*, 2015 WL 1470852, at *1 (M.D. Fla. Mar. 31, 2015). Though persuasive, the decisions of district courts within this circuit are not binding on the other district courts within the circuit, nor are cases from other circuits. *McGinley v. Houston*, 361 F. 3d 1328, 1331 (11th Cir. 2004)(internal citations omitted)("The general rule is that a district judge's decision neither binds another district judge nor binds him, although a judge ought to give great weight to his own prior decisions….A circuit court's decision binds the district courts sitting within its jurisdiction while a decision by the Supreme Court binds all circuit and district courts."). The only applicable binding case the Court has found addressing the meaning of "exceeds authorized access" under the CFAA is *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In

Rodriguez, an employee of the Social Security Administration ("SSA") appealed his conviction under § 1030(a)(2)(B) of the CFAA for accessing sensitive personal information on certain individuals via the SSA's computer systems. 628 F.3d at 1260. The SSA had established a policy that prohibited an employee from obtaining information from its databases without a business reason. Id. The appellate court upheld the CFAA conviction because the employee accessed personal information that was not related to SSA's business purposes. Id. at 1263. While distinguishing the facts before it from other cases, the appellate court specifically noted that the employer informed the employee that he was not "authorized to obtain personal information for nonbusiness reasons." *Id.*

Similarly, in this case, the Complaint alleges as follows:

> On January 16, 2017, RSI distributed a memorandum to all employees regarding uses and disclosure of the company's proprietary information and trade secrets (the "Memorandum"). The Memorandum reminded the employees of their obligations under HIPAA. It stated that it was impermissible for employees to download patient information for personal use or for use by anyone other than an RSI employee. It also stated than no employee should download any patient information without express approval from practice management.... All employees were directed to sign the Memorandum acknowledging they had received it, read it, understood its provisions, and would adhere to RSI's policies and procedures regarding access to confidential patient information.

(Doc. 1 at 5, ¶¶ 22-23).[2] It appears that some of the conduct Plaintiff alleges violates the CFAA, would be in direct violation of this policy. For example, if a defendant

[2] Plaintiff submitted what appears to be a copy of the referenced Memorandum with its response to sthe motion to dismiss. (Doc. 18 at 23). This exhibit was not considered "As a general rule, the district court must 'limit[ ] its consideration to the pleadings and exhibits attached thereto' when deciding a Rule 12(b)(6) motion to dismiss." *Lewis v. Asplundh Tree Expert Co.*, 305 F. App'x 623, 627 (11th Cir. 2008) (*per curiam*) (quoting *Grossman v. Nationsbank, N.A.,* 225 F.3d 1228, 1231

downloaded patient information for personal use or without express approval from management, the access would be unauthorized.

As recently as late July 2017, in an unpublished opinion, the Court of Appeals for the Eleventh Circuit examined the CFAA and its *Rodriguez* opinion:

> The CFAA does not define the phrase "without authorization," but it defines "exceeds authorized access" as "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). We have, in one published opinion, expounded on what it means to "exceed authorized access." *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In *Rodriguez*, the defendant had access, through his work as a TeleService representative for the Social Security Administration, to certain SSA databases containing sensitive personal information. SSA policy authorized the defendant's access to the databases only for official business purposes. The defendant knew this, but chose to access the database and obtain information for nonbusiness reasons. *See id.* at 1263. We concluded that the defendant's access, which had been in furtherance of nonbusiness purposes, exceeded the authorization the SSA had given him, and affirmed his conviction under the CFAA. *See id.* at 1263–64.
>
> Although it is not entirely clear, one of the lessons from *Rodriguez* may be that a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question. So, assuming that the OxBlue Defendants actually violated the [licensing agreement], there is an argument that downloading the screenshots "exceeded authorized access" under *Rodriguez*.

EarthCam, Inc. v. Oxblue Corp., 2017 WL 3188453, at *4 (11th Cir. July 27, 2017).

Importantly, a footnote two, found within this section of the *EarthCam* case states:

(11th Cir. 2000) (internal quotation marks omitted)). "If, on a motion under Rule 12(b)(6)…, matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56. All parties must be given a reasonable opportunity to present all the material that is pertinent to the motion." Fed. R. Civ. P. 12(d). *See also Finn v. Gunter*, 722 F.2d 711, 713 (11th Cir. 1984) ("The 12(b)(6) motion thus was converted into a summary judgment motion necessitating all the procedural safeguards of Rule 56.").

> We decided *Rodriguez* in 2010 without the benefit of a national discourse on the CFAA. Since then, several of our sister circuits have roundly criticized decisions like *Rodriguez* because, in their view, simply defining "authorized access" according to the terms of use of a software or program risks criminalizing everyday behavior. *See United States v. Valle*, 807 F.3d 508, 527 (2d Cir. 2015); *WEC Carolina Energy Sols.LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc). Neither the text, nor the purpose, nor the legislative history of the CFAA, those courts maintain, requires such a draconian outcome. We are, of course, bound by *Rodriguez*, but note its lack of acceptance.

Id. at *4, n.2.

While the Court may agree with *Enhanced Recovery*, the Court must consider the binding authority of *Rodriguez*, coupled with the observations made by the Court of Appeals in *EarthCam*. The inquiry here turns on whether Plaintiff's claims present a plausible claim for relief.

The facts here are similar to *Rodriguez* in that Plaintiff alleges that it had a policy that authorized access to its computerized records only for limited purposes. *See Rodriguez*, 628 F.3d at 1263 (company policy restricted employee's authorization to access certain information and the employee admitted that he accessed the information); *IPC Sys., Inc. v. Garrigan,* 2012 WL 12872028, at *6 (N.D. Ga. May 21, 2012) (relying on *Rodriguez* and denying dismissal of CFAA claim because fact questions remained about the purpose for which an employee accessed information and whether the employee exceeded his authorized access); *cf. Aquent LLC v. Stapleton*, 65 F.Supp.3d 1339, 1346 (M.D. Fla. 2014) (finding company policy that required the employee to keep information confidential and to use information for business purposes only akin to the policy in *Rodriguez* and concluding that the plaintiff stated a claim under the CFAA that the employee exceeded her authorization).

The allegations raised by Plaintiff, which the Court must accept as true at this stage contain a plausible claim for relief. Thus, the motions to dismiss, as to Count One, are **DENIED**.[3]

II. The Alabama Digital Crime Act (Count Two)

In Count Two of the Complaint, Plaintiff alleges that Defendants violated the Alabama Digital Crime Act ("ADCA"), codified at Ala. Code § 13A-8-112, when they "knowingly and exceeding their authorization for use, disclosed, used, controlled and took information or data residing in RSI's computers, computer system, and computer network." (Doc. 1 at 7, ¶33).

Pursuant to the ADCA, "[a] person who acts without authority or who exceeds authorization of use commits the crime of computer tampering by knowingly:"

> (1) Accessing and altering, damaging, or destroying any computer, computer system, or computer network.

[3] *See also Agilysys, Inc. v. Hall*, 2017 WL 2903364, at *5, n.2 (N.D. Ga. May 25, 2017)("The courts debating this issue refer oftentimes to the practical implications of viewing the CFAA so broadly. The Court is troubled by the practical implications of Agilysys' policy here. Pursuant to Agilysys' policy, Hall would be liable under the CFAA for every time in his 32 years of employment, that the policy was in place, he accessed the internet for a non-business purpose. This would include checking the news, sports scores, weather, or even an emergency alert. Every other employee of Agilysys would also be liable for the same. *See Valle*, 807 F.3d at 527 (discussing courts that have recognized the problems with an broad view of the CFAA; a broad view would mean that "any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems") (quotation omitted). After a review of the court split and the legislative history of the CFAA, the Court does not believe that Congress intended the CFAA to cover such situations. *Nevertheless, as noted above, the Court is limited by the Rodriguez opinion and by the Rule 12(b)(6) standard at this early stage of the case.")*(emphasis added).

> (2) Altering, damaging, deleting, or destroying computer programs or data.
>
> (3) Disclosing, using, controlling, or taking computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network.
>
> ***
>
> (7) Obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system, or network that is operated by this state, a political subdivision of this state, or a medical institution.
>
> (8) Giving a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data.

Ala. Code § 13A-8-112(a).

Plaintiff cites Ala. Code § 6-5-370 for the provision that "[f]or any injury, either to person or property, amounting to a felony, a civil action may be commenced by the party injured without prosecution of the offender." (Doc. 1 at 7, ¶ 35). As Defendants point out, "Section 6–5–370 does not create a cause of action; rather, it merely allows a plaintiff to commence a civil action even if the plaintiff does not pursue criminal prosecution of the defendant." *Lewis v. Fraunfelder,* 796 So.2d 1067, 1070 (Ala.2000); *see also Preskitt v. Lyons,* 865 So.2d 424, 429 (Ala.2003) ("§ 6–5–370 only eliminates an obstacle for plaintiffs with a valid cause of action; it does not *create a civil cause of action for any injury that amounts to a felony.*") (emphasis added); *Thomas v. McKee,* 205 F.Supp.2d 1275, 1291

(M.D.Ala.2002) (De Ment, J.) (Section 6–5–370 “was merely intended to abrogate the common law rule of suspension which precluded civil damages claims in these circumstances absent the prosecution of the felonious offender.”).

However, there may be a remedy under common law, as there is a remedy for criminal violations which result in injury to person or property. *See Lollar v. Poe,* 622 So.2d 902 (Ala. 1993). In Alabama, “civil liability for acts which constitute a crime ‘will ensue only if the acts complained of violate the legal rights of the plaintiff, constitute a breach of duty owed to the plaintiff, or constitute some cause of action for which relief may be granted.’” *Ages Group, L.P. v. Raytheon Aircraft Co., Inc.,* 22 F.Supp.2d 1310, 1320 (M.D.Ala.1998) (quoting *Smitherman v. McCafferty,* 622 So.2d 322 (Ala.1993)). Plaintiff argues that Defendants’ conduct violated RSI’s property rights in its computer system, RSI’s privacy rights, interfered with its business relations, and subjected it to the threat of criminal and civil liability due to HIPAA breaches. (Doc. 18 at 19-20; Doc. 1 at 1-2, ¶1; Doc. 1 at 6, ¶ 26).

Upon consideration, the Court finds that the facts as alleged present a plausible claim for relief under the Alabama Digital Crimes Act, as the Complaint alleges violations of the legal rights of the Plaintiff, and that the motions to dismiss Count Two pursuant to Fed.R.Civ.P. 12(b)(6) are **DENIED**. *See also D&J Optical, Inc. v. Wallace*, 2015 WL 1474146, at *8 (M.D. Ala. Mar. 31, 2015)(denying motion to dismiss a civil ADCA claim). The Court notes, however, that it has not found a single Alabama case, available on Westlaw, involving a civil action brought pursuant to the ADCA.

CONCLUSION

For the reasons discussed herein, Defendants' motions to dismiss (Docs. 12, 13, and 14) are **DENIED**.

DONE and **ORDERED** this the **9th** day of **November 2017**.

/s/ Katherine P. Nelson
KATHERINE P. NELSON
UNITED STATES MAGISTRATE JUDGE