IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

EPIC SYSTEMS CORPORATION,

Plaintiff,

v.

TATA CONSULTANCY SERVICES LIMITED and TATA AMERICA INTERNATIONAL CORPORATION d/b/a TCA America,

Defendants.

OPINION AND ORDER

14-cv-748-wmc

Plaintiff Epic Systems Corporation asserts state and federal law claims against defendants Tata Consultancy Services Limited and Tata America International Corporation (collectively "Tata"), all of which arise out of Tata's alleged unauthorized accessing and using of plaintiff's confidential information and trade secrets. Defendants have filed a motion to dismiss these claims, on a variety of grounds. (Dkt. #43.) For the reasons that follow, the court finds that plaintiff's complaint meets the requirements of Federal Rules of Civil Procedure 8, 9(b), and 12(b)(6). Accordingly, the court will deny defendants' motion in its entirety.[1]

[1] Also before the court is a recently-filed, unopposed motion by plaintiff to file a second amended complaint, adding or clarifying that it is seeking nominal damages and declaratory relief. (Dkt. #152.) That motion is granted, and the proposed pleading (dkt. #154-2) is now the operative one.

ALLEGATIONS OF FACT[2]

A. The Parties

Epic is a Wisconsin-based healthcare company. Epic makes software that manages the storage and collection of patient and care process data into a common database. Epic markets this software to mid-size and large medical groups, hospitals, and integrated healthcare organizations throughout the United States and the world.

Tata Consultancy Services Limited ("Tata India") is an Indian corporation that does over half of its business in America. Tata India specializes in information technology services, consulting, and business solutions; it also develops and markets software products, including the hospital management system "Med Mantra."

Tata America International Corporation ("Tata America") is a New York corporation registered to do business in Wisconsin. Tata America is a wholly-owned subsidiary of Tata India, which provides IT services, consulting, and computer systems integration services within the United States.

B. Epic's Licensing Agreement with Kaiser

Kaiser Permanente ("Kaiser") is one of the largest managed healthcare organizations in the United States. On February 4, 2003, Epic entered into a written agreement with Kaiser (the "Kaiser Agreement") under which Epic licensed software to Kaiser to support patient care delivery activities and to provide Kaiser with customer-

[2] The court accepts as true all well-pled factual allegations in the complaint, *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014), and views them in the light most favorable to the non-movant, Epic, *Santiago v. Walls*, 599 F.3d 749, 756 (7th Cir. 2010) (quoting *Zimmerman v. Tribble*, 226 F.3d 568, 571 (7th Cir. 2000)).

level access to Epic's UserWeb. The UserWeb is a protected electronic workspace created by Epic to aid customers in maintaining and implementing Epic products by providing training and other useful information. The Kaiser Agreement also provided protection for Epic's confidential information, permitting information to be disseminated from the UserWeb only on a need to know basis and to be used only to fulfill the purposes of the Kaiser Agreement. (Am. Compl. (dkt. #38) ¶ 17.)

C. Epic's Consultant Agreement with Tata

To access Epic's UserWeb, an individual must register as an employee of either an Epic customer or a consultant to an Epic customer. However, in order for a consultant employee to attain UserWeb access, two additional steps must be completed: (1) the individual attempting to register must sign the UserWeb Access Agreement and (2) the consulting firm must sign the Consultant Access Agreement. Once the applicable steps are completed, that individual attains UserWeb access with no further restrictions, except that a consultant employee's access is purposefully limited solely to the areas of the UserWeb necessary to support his or her customer.

Tata was hired by Kaiser to serve as a consultant. In August 2005, several Tata employees attempted to register for customer-level access. Though they used Tata email addresses when registering, they represented themselves to be customer employees. When Epic discovered the discrepancy, it removed the Tata employees from the UserWeb and informed them that Tata employees could not take training courses on the UserWeb until Tata entered into a Consultant Agreement with Epic.

On August 10, 2005, Epic and Tata America proceeded to enter into a Standard Consultant Agreement (the "Tata America Agreement"). (Robben Decl., Ex. B (dkt. #45-2).)[3] Through the Tata America Agreement, Epic allowed certain Tata employees to access training programs on the UserWeb for the purposes of providing consulting services to Kaiser on the implementation of "Epic Program Property," defined in the agreement as "computer program object and source code and the Documentation for all of Epic's computer programs." (Am. Compl. (dkt. #38) ¶ 27.) In return, Tata America agreed to certain obligations:

1. Tata America will "limit access to the Program Property to those of Your employees who must have access to the Program Property in order to implement the Program Property on Epic's or its customer's behalf;"

2. Tata America will not "[u]se the Program Property . . . for any purpose other than in-house training of Your employees to assist Epic customers in the implementation of the Program Property licensed by that Epic customer;"

3. Tata America will "require any of Your employees who are given access to the Confidential Information to execute a written agreement . . . requiring non-disclosure of the Confidential Information and limiting the use of the Confidential Information to uses within the scope of the employee's duties conducted pursuant to this Agreement" or "inform all such employees that Your are obligated to keep Confidential Information confidential." ("Confidential Information" is defined as information "concerning the functioning, operation or Code of the Program Property, Epic's training or implementation methodologies or procedures, or Epic's planned products or services");

4. Tata America will "use any Confidential Information only for the purpose of implementing the Program Property on an Epic customer's behalf;"

[3] The court may consider the Tata America Agreement submitted with defendants' motion to dismiss because it is both referenced in Epic's pleadings and central to its claims. *See Geinosky v. City of Chi.*, 675 F.3d 743, 745 (7th Cir. 2012) ("A motion under Rule 12(b)(6) can be based only on the complaint itself, documents attached to the complaint, documents that are critical to the complaint and referred to in it, and information that is subject to proper judicial notice.").

5. Tata America will "[n]otify Epic promptly and fully in writing of any person, corporation or other entity that You know has copied or obtained possession of or access to any of the Program Property without authorization from Epic;" and

6. Tata America will "[n]ot permit any employee while in Your employment who has had access to the Program Property of any Confidential Information relating to the Program Property to participate in any development, enhancement or design of, or to consult, directly or indirectly, with any person concerning any development, enhancement or design of, any software that competes with or is being developed to compete with Epic Program Property[.]"

(*Id.* at ¶ 29; *see also* Robben Decl., Ex. B (dkt. #45-2) pp.2-3.) Shortly after the filing of this law suit, Epic terminated the Tata America Agreement. The confidentiality and use restrictions, however, remain in effect "for the maximum duration and scope allowed by law." (*Id.* at ¶ 30.)

D. Tata's Unauthorized Access and Downloading

As early as 2012, Tata began accessing and downloading information from Epic's UserWeb without authorization. Epic primarily based this allegation on information received from a Tata informant, Philippe Guionnet. Until May 2014, Guionnet was responsible for managing all aspects of Tata's contract with Kaiser, reporting directly to Tata executive management. On multiple occasions, his job responsibilities exposed him to Med Mantra products. He also participated in marketing Med Mantra products to Kaiser and was aware of comparisons between Epic and Med Mantra softwares created by the Med Mantra team.

According to Guionnet, downloaded information included both Program Property and Confidential Information within the meaning of the Tata America Agreement. Once

downloaded, this information was used to benefit Tata's competing Med Mantra software. Guionnet also represents that Tata leaders in the U.S. and India were aware of and complicit in this scheme.

Once aware of the unauthorized downloading, Epic conducted an investigation of its UserWeb, which led to the account of Ramesh Gajaram, a Tata employee, working as a consultant for Kaiser in Portland, Oregon. Gajaram's account revealed that at least 6,477 documents, accounting for 1,687 unique files, had been downloaded, including documents containing Program Property and Confidential Information within the meaning of the Tata America Agreement. Many of these documents were not necessary for Gajaram to perform his job functions for Kaiser. Examples of confidential and/or trade secret documents that Gajaram attained only through his improper customer-level access include Community Connect Install Summary, ADT End-User Proficiency Question Bank, ED Registrar Checklist, and the Physician's Guide to EpicCare Ambulatory zip file.

Furthermore, Epic's investigation revealed that Gajaram's access credentials had been used outside Oregon to download documents from an IP address in India registered to Tata. When confronted, Gajaram admitted to violating the UserWeb Access Agreement by providing his access credentials to two other Tata employees in India -- Aswin Kumar Anandhan and Sankari Gunasekara -- neither of whom needed access to much of the information downloaded from Gajaram's account in order to perform their job functions for Kaiser.

In addition to being misused, Gajaram's UserWeb log-in credentials were also

obtained in a deceptive manner. When Gajaram registered for his UserWeb credentials, he registered as a customer employee, rather than as a consultant and used a Kaiser, rather than a Tata, email address. Rather than the more limited consultant-level access, this allowed Gajaram broader, customer-level access. After Epic suspended Gajaram's access to the UserWeb, Gajaram sent two emails requesting reactivation. The first email request was sent on June 24, 2014, and listed only his Kaiser role in the signature block, with his Tata role deleted. The second email request was sent on June 30, 2014, and included his full signature with his roles for both Kaiser and Tata disclosed. Epic argues the omission of Tata from the June 24 email permits an inference that Gajaram intentionally misrepresented himself to be a Kaiser employee, and that his objective was to obtain unauthorized UserWeb access.

On October 31, 2014, Epic filed a complaint seeking both injunctive relief and monetary damages. On January 5, 2015, Tata filed a motion to dismiss the majority of Epic's claims. In response, Epic filed an amended complaint on January 26, 2015, which resulted in TATA filing its present motion to dismiss.

OPINION

Epic claims Tata violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and Wisconsin's Computer Crimes Act, Wis. Stat. § 943.70. Epic also asserts various other claims under Wisconsin's statutes and common law, including misappropriation of trade secrets, Wis. Stat. § 134.90, breach of contract, breach of the covenant of good faith and fair dealing, fraud, conversion, common law unfair competition, injury to business, Wis. Stat. § 134.01, and property damage or loss, Wis.

Stat. § 865.446. As an alternative to its breach of contract claim, Epic also asserts a claim for unjust enrichment. The court will address each of defendants' challenges to plaintiff's claims in turn below.

I. CFAA Challenges

Defendants assert two core bases for seeking dismissal of plaintiff's CFAA claim: (1) plaintiff's claim does not fall within the main anti-hacking policy objective of the CFAA; and (2) plaintiff fails to plead damage or loss, as required to bring a civil claim under the CFAA.[4]

A. Policy Objective behind CFAA

Defendants assert that the CFAA is meant to target solely hackers and disgruntled employees, neither category of which encompasses defendants. Defendants are correct in asserting that computer hackers were a main target of the CFAA at the time of its enactment. *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) ("Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking . . . ."). What defendants fail to recognize, however, is that the allegations of their conduct contained in plaintiff's Complaint would constitute "hacking" within both the spirit and likely the meaning of the CFAA.

The CFAA "distinguishes between [accessing a computer] 'without authorization' and 'exceeding authorized access,' . . . while making both punishable." *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (quoting 18 U.S.C § 1030(e)(6)

[4] Defendants also argue that plaintiff's CFAA claim is implausible. The court addresses this challenge together with defendants' other plausibility challenges in section II below.

(2015)). Exceeding authorization is defined as "access[ing] a computer with authorization and . . . [then] us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). As the Ninth Circuit explained in *Nosal*, acting "without authorization" within the meaning of the CFAA applies "to *outside hackers* (individuals who have no authorized access to the computer at all)," while "exceeds authorized access" under the CFAA applies "to *inside hackers* (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." 676 F.3d at 858 (emphasis added). In other words, obtaining information by exceeding one's authorized access is committing a form of hacking. Furthermore, courts frequently apply the CFAA to address so-called "inside hacking." *1st Rate Mortg. Corp. v. Vision Mortg. Servs. Corp.*, No. 09-C-471, 2011 WL 666088, at *3 (E.D. Wis. Feb. 14, 2011) ("[C]ourts have noted that the CFAA has frequently been used to remedy 'inside jobs'[.]").

Here, plaintiff's claim that TATA employees sought and obtained files from parts of the UserWeb located beyond their authorization level as consultant employees would, if true, qualify each of those employees as inside hackers. Even assuming defendants' argument that the allegation must fall within the primary policy objective has merit, plaintiff's claim plainly falls within the main anti-hacking policy objective of the CFAA.

B. Damages or Loss

Although the CFAA is a criminal statute, plaintiff may maintain a civil cause of action for economic damages if among other possible alternatives listed in § 1030(c)(4)(A)(i), it suffered "damages or loss" as a result of a CFAA violation that in

the aggregate amount to at least $5,000 within any one-year period. § 1030(c)(4)(A)(i)(I), (g). Defendants represent that the courts are split on whether a plaintiff must show both damages *and* loss, or simply one or the other, in order to bring a civil cause of action under the CFAA. Curiously, however, the only case cited by defendants to support this representation is a case that declares the proper construction of the "damages or loss" language to be its plain meaning. *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009) ("[A] plaintiff alleging violations of sections 1030(a)(2) or (a)(4) need only allege damage *or* loss, not both.") (emphasis added). Regardless, to the extent the distinction is meaningful, this court joins other courts in concluding that a civil action under the CFAA requires a plaintiff to plead -- and eventually prove -- only damages *or* loss. *See, e.g.*, *Pascal Pour Elle, Ltd. v. Jin*, No. 14-C-7943, 2014 WL 6980699, at *7 (N.D. Ill. Dec. 9, 2014) ("Plaintiff need only plead damage or loss to adequately plead a private right of action [under the CFAA]."); *Navistar, Inc. v. New Balt. Garage, Inc.*, No. 11-cv-6269, 2012 WL 4338816, at *6 (N.D. Ill. Sept. 20, 2012) ("Thus, to recoup compensatory damages, a plaintiff must show either damage or loss.") (quoting *U.S. Gypsum Co. v. Lafarge N. Am. Inc.*, 670 F. Supp. 2d 737, 743 (N.D. Ill. Oct. 27, 2009)).[5]

Even if it were required, however, plaintiff alleges both damages *and* loss. (Am. Compl. (dkt. #38) ¶ 74.) Within the CFAA, most courts recognize the term "damages" to require a destructive element. *See First Fin. Bank, N.A. v. Bauknecht*, No. 12-cv-1509,

[5] Indeed, the only place the CFAA utilizes the phrase "damages and loss" is as part of an additional requirement for proving a 1030(a)(5)(C) violation -- a distinctly separate violation from any of those claimed by plaintiff here.

2014 WL 5421241, at *22 (C.D. Ill. Oct. 24, 2014) ("District courts have relied on the CFAA's statutory language to limit CFAA damages to 'destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution in the completeness or usability of the data on a computer system.'") (quoting *Farmers Ins. Exch. v. Auto Club Group*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011)); *but see Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 996 (E.D. Cal. 2007) ("The alleged unauthorized access to the Publication and the disclosure of its information may constitute an impairment to the integrity of data or information even though 'no data was physically changed or erased.'") (quoting *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000)).

As plaintiff claims only that files were copied from unauthorized areas of its UserWeb -- not that any files were altered or erased -- at least under the majority view, plaintiff might not have alleged "damages" under the CFAA. *See, e.g.*, *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009) ("The plain language of the statutory definition [of damages] refers to situations in which data is lost or impaired . . ."); *Navistar*, 2012 WL 4338816, at *6 ("[T]he mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement.") (quoting *Farmers Ins. Exch.*, 823 F. Supp. 2d at 852). Even so, it would be premature to dismiss a claim based on damages without an opportunity to amend.

As for "loss," the CFAA requires that there be a loss in excess of $5,000 within a one-year period. 18 U.S.C. § 1030(c)(4)(A)(i)(I). The CFAA defines loss as "any reasonable cost to any victim," listing two general categories of loss: (1) "the cost of

responding to an offense, conducting a damage assessment . . .” and (2) “any revenue lost, cost incurred, or other consequential damages incurred because of interruption of services.” 18 U.S.C. § 1030(e)(11).

As for the first category, although plaintiff does not expressly allege that it suffered an interruption of services due to defendants’ actions, plaintiff alleges “far more than $5,000 in costs and loss related to investigating defendants’ unauthorized accessing of Epic’s UserWeb.” (Am. Compl. (dkt. #38) ¶ 50.) Relying on a case from the Northern District of Illinois, defendants nevertheless persist in arguing that any loss tied to an investigation must still relate to impairment or interruption of services. *Mintel Int’l Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2010 WL 145786, at *10 (N.D. Ill. Jan. 12, 2010) (“The alleged loss must relate to the investigation or repair of a computer or computer system following a violation that caused impairment or unavailability of data or interruption of service.”). More recent case law rejects this overly narrow position, particularly in instances where the facts align more closely with those presently claimed by plaintiff. *See, e.g.*, *Pascal Pour Elle, Ltd. v. Jin*, 2014 WL 6980699, at *7 (acknowledging a split within the Circuit as to what constitutes loss, but ultimately denying defendant’s motion to dismiss based on the plain meaning of the statutory definition of loss and plaintiff’s plea of $5000 in “investigation and security assessment costs associated with the intrusion”); *1st Rate Mortg.*, 2011 WL 666088, at *2 (finding that the cost of a reasonable employer’s response to a CFAA violation constituted loss even in the absence of damages); *Dental Health Prods. v. Ringo*, No. 08-C-1039, 2011 WL 3793961, at *3 (E.D. Wis. Aug. 24, 2011) (finding that $16,000 spent on a computer

expert to determine the extent of defendants unauthorized access was reasonable and constituted loss under the CFAA).[6] Consistent with the plain language of the statute, the court agrees with the reasoning of other decisions, allowing "loss" associated with the costs of an investigation. Even if this were not so, the court would have allowed for an amended filing. Accordingly, the court will deny defendants' motion to dismiss this claim.

II. Plausibility Challenges

Defendants' plausibility challenges under Rules 8 of the Federal Rules of Civil Procedure are, if anything, even less meritorious. As a preliminary matter, despite a heightened pleading standard after *Twombly* and *Iqbal*, the court still generally operates on a system of notice pleading. *Bissessur v. Ind. Univ. Bd. of Trustees*, 581 F.3d 599, 603 (7th Cir. 2009) (stating that federal courts still operate "on a notice pleading standard; *Twombly* and its progeny do not change this fact"). To be facially plausible, plaintiff's complaint must plead "factual content that allows 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).

Across a number of claims, defendants vaguely contend that plaintiff has failed to adequately plead that the information was obtained by "improper means" or "without authorization." To the contrary, the detailed allegations in plaintiff's complaint are more than adequate to meet both the requirements of Rule 8 and the plausibility requirements

[6] *Mintel* is also distinguishable from the facts alleged in this case. Unlike the plaintiff in *Mintel*, Epic is not simply trying to recoup the cost of paying one of its experts. Rather, it is seeking the cost of responding to an offense committed by the defendants -- a cost which falls within the plain meaning of the CFAA's loss definition.

articulated in *Twombly* and *Iqbal*. (*See, e.g.,* Defs.' Opening Br. (dkt. #44) 26 (failed to adequately plead "without authorization under the CFAA); 28-29 (failed to adequately plead "without authorization under Wisconsin's Computer Crimes Act); 30-31 (failed to adequately allege "misappropriation" for a claim under the UTSA); 37 (failed to adequately allege defendants "wrongfully obtained access" to state a breach of contract claim).) Indeed, the claims plaintiff asserts are not just plausible, but highly compelling.

To the extent defendant's arguments concern whether plaintiff will be able to *prove* its claims -- for example, calling into question TATA informant Philippe Guionnet's credibility -- that challenge is for another day. Today, in contrast, the court will deny defendants' motion to dismiss under Federal Rule of Civil Procedure 8.

III. Other Challenges

Defendants assert a few other challenges, which deserve only brief attention.

A. Fraud

Defendants challenge the sufficiency of plaintiff's fraud claim under Rule 9(b), which requires plaintiff to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). The Seventh Circuit describes the necessary level of particularity as including the "'who, what, when, where, and how' of the fraud." *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 615 (7th Cir. 2011). As plaintiff convincingly details, the allegations of the complaint meet each of those requirements: "the 'who' (the TCS employee, with TCS's knowledge); the 'what' (the TCS employee representing that he was a Kaiser employee, using a 'kp.org' email address, and altering his email signature line); the 'when' (at the time the TCS employee registered, before June 2014); the

'where' (in the registration for credentials and in the emails); and the 'how' (by falsely identifying himself as a Kaiser employee instead of a consultant to gain access offered to customers)." (Pl.'s Opp'n (dkt. #46) 46-47.) In light of this level of particularity, the court will deny defendants' motion to dismiss plaintiff's fraud claim.

B. Pleading Alternative Claims

Next, defendants challenge plaintiff's good faith and fair dealing claim as duplicative of its breach of contract claim. Plaintiff, however, claims good faith and fair dealing as an alternative to its breach of contract claim, which is its right. *See Maryland Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1509 (E.D. Wis. 1996) (finding that despite overlap, common law breach of contract and good faith and fair dealing claims could be pled in the alternative). Accordingly, the court will deny defendants' motion to dismiss plaintiff's good faith and fair dealing claim as well.

Defendants also challenge all of plaintiff's state statutory and tort claims as preempted by the Uniform Trade Secrets Act ("UTSA"). According to defendants, Epic has not yet declared, at least specifically, which information constitutes trade secret and which information constitutes confidential information. Defendants' preemption challenges, however, are similarly premature. *See, e.g.*, *Radiator Exp. Warehouse, Inc. v. Shie*, 708 F. Supp. 2d 762, 770 (E.D. Wis. 2010) ("[D]iscovery could prove that the information at issue in the plaintiff's first cause of action falls short of the statutory definition of 'trade secret' . . . . In short, a claim of abrogation is premature at the motion to dismiss stage."); *Genzyme Corp. v. Bishop*, 463 F. Supp. 2d 946, 949 (W.D. Wis. 2006) ("[S]uch an inquiry [as preemption] is better addressed on summary judgment where

both parties have the opportunity to develop the record and submit evidence to the Court in support of their respective positions."). For these same reasons, the court also rejects any preemption challenges in defendants' motion to dismiss.[7]

Aside from the challenges brought under the CFAA (which despite failing to pose particularly close legal questions, were at least appropriate for a motion to dismiss), the arguments presented in defendants' motion to dismiss were either meritless or inappropriate for the pleading stage.

ORDER

IT IS ORDERED that:

1) defendants Tata Consultancy Services Limited and Tata America International Corporation's motion to dismiss (dkt. #43) is DENIED; and

2) plaintiff Epic System Corporation's unopposed motion for leave to file second amended complaint (dkt. #152) is GRANTED. Plaintiff is directed to refile its second amended complaint (dkt. #154-2) as a stand-alone document. Defendants' answer is due on or before December 2, 2015.

Entered this 18th day of November, 2015.

BY THE COURT:

/s/

_____
WILLIAM M. CONLEY
District Judge

[7] Defendants also challenge plaintiff's conversion claim on the basis that electronic files do not constitute "property." (Defs.' Opening Br. (dkt. #44) 44.) The court rejects this basis as well because: (1) Epic alleges that defendant took Epic's documents and information, not just electronic files; and (2) courts from other jurisdictions have recognized that electronic documents are the proper subject of conversion claims. (Pl.'s Opp'n (dkt. #46) 60.)